federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

6 DICEMBRE 2017

La disciplina del *cyberspace* alla luce della direttiva europea sulla sicurezza delle reti e dell'informazione: contesto normativo nazionale di riferimento, ruolo dell'*intelligence* e prospettive *de iure condendo*

di Luca Vincenzo Maria Salamone
Dirigente presso il Ministero della difesa

La disciplina del *cyberspace* alla luce della direttiva europea sulla sicurezza delle reti e dell'informazione: contesto normativo nazionale di riferimento, ruolo dell'*intelligence* e prospettive *de iure condendo* *

di Luca Vincenzo Maria Salamone
Dirigente presso il Ministero della difesa

Sommario: 1. Innovazione tecnologica e sicurezza cibernetica: rischi latenti e nuove esigenze ordinamentali. **– 2.** La direttiva NIS: *ratio* e fondamento giuridico. **– 3.** La direttiva NIS: uno sguardo d'insieme sulle finalità e l'ambito di applicazione. **– 3.1.** *(Segue):* analisi di dettaglio della direttiva NIS. **– 4.** Contesto giuridico nazionale di riferimento nel settore della tutela dello spazio cibernetico nelle more del recepimento della direttiva NIS. **– 4.1.** *(Segue):* l'attuale architettura amministrativa nazionale nel settore della tutela dello spazio cibernetico, con particolare riferimento al ruolo dell'*intelligence.* **– 5.** Recepimento in ambito nazionale della direttiva NIS: possibili aspetti critici e riflessioni *de iure condendo.*

Abstract [It]: L'Autore esamina la disciplina giuridica dello spazio cibernetico alla luce della direttiva UE n. 2016/1148 sulla sicurezza delle reti e dell'informazione (cd. Direttiva NIS). In particolare, l'Autore, dopo avere messo in rilievo la rilevanza geopolitica e strategica della tutela del *cyberspace* in un'ottica non solo nazionale, bensì europea e globale, sottolinea la ragguardevole importanza della nuova normativa UE, in quanto con essa è disciplinata, per la prima volta, la materia della tutela dello spazio cibernetico. Egli evidenzia, altresì, come la messa a punto di una tale organizzazione difensiva unitaria da parte dell'UE costituisca un fatto di grande rilevanza politica, dal momento che, grazie ad essa, l'Unione si dota di uno strumento giuridico che, con il fine del ravvicinamento delle legislazioni dei singoli Stati europei, consente finalmente di implementare una strategia comune nel campo della *cybersecurity*, gettando le basi per mettere a punto un'organizzazione difensiva completamente integrata e sotto egida europea.
L'Autore, infine, dopo avere esaminato approfonditamente la direttiva NIS – non tralasciando di analizzarne alcune possibili criticità in sede di recepimento della stessa da parte degli Stati membri (come, ad esempio, l'aspetto relativo alla previsione di poteri coercitivi e sanzionatori e dell'individuazione dell'autorità nazionale competente) – e dando anche atto, in alcuni brevi passaggi di analisi comparata, di come si stanno attrezzando altre nazioni (ad es. USA, Israele, Cina, Russia, ecc.) nel campo della *cybersecurity* e dell'*intelligence* di settore, delinea il quadro giuridico-amministrativo nazionale di riferimento nelle more del recepimento della direttiva NIS, sottolineando il ruolo, sempre più rilevante, ricoperto nello specifico settore della tutela dello spazio cibernetico dal comparto *intelligence* nazionale.

Abstract [En]: The author examines the legal framework of cyberspace in the light of EU directive n. 2016/1148 on Network and Information Security (called NIS Directive).
In particular, after highlighting the strategic and geopolitical relevance of cyberspace protection not only from a national, but also European and global perspective, he emphasizes the remarkable importance of EU legislation, as it deals with the protection of the Cyber space for the first time.

* Articolo sottoposto a referaggio. Nell'esercizio della libertà di espressione e di pensiero e nel rispetto dei relativi limiti, il contenuto della presente pubblicazione riflette esclusivamente il pensiero dell'autore e non, necessariamente, quello dell'Istituzione per la quale lo stesso presta servizio ovvero appartiene.

He also highlights how the development of such a European unified defensive organization is a matter of great political significance since it provides the EU with a legal instrument, aimed at the approximation of the individual European states laws. Through this effort, it will be possible to implement a common European cybersecurity strategy, laying the foundations for the development of a fully-integrated defensive organization under the auspices of the EU.
The author, after thoroughly examining the European legislation (including a specific focus on criticalities such as the aspect of the foreseeing of coercive powers and sanctions and the identification of the competent national authority) and carrying out a quick rundown of how other nations (e.g. USA, Israel, China, Russia) are equipped in the field of cybersecurity and intelligence, outlines the Italian legal and administrative reference framework in the transposition of the NIS directive, underlining the role played by the national intelligence services in the specific cyberspace protection sector.

1. Innovazione tecnologica e sicurezza cibernetica: rischi latenti e nuove esigenze ordinamentali

«Non ho idea di quali armi serviranno per combattere la terza guerra mondiale, ma la quarta sarà combattuta con i bastoni e con le pietre ([1])». Questa famosa citazione ci ha spesso indotto a prefigurare una minacciosa evoluzione della terribile arma nucleare attraverso devastanti sistemi di distruzione di massa. Al giorno d'oggi, però, sembrano molto lontani i tempi delle guerre nucleari, ormai possiamo dire di essere nell'epoca dove le guerre si combattono in un universo parallelo, quello digitale. La nuova guerra, infatti, è diventata *cyber* ed è certamente globale; ciò deriva dal fatto che la società moderna è sempre più pervasa e dipendente da sistemi tecnologici complessi e, in particolare, dall'interconnessione tra reti telematiche e informatiche nello spazio cibernetico ([2]).

È innegabile, infatti, che negli ultimi due decenni, le reti e i sistemi informativi – ma più in generale lo spazio cibernetico quale strumento di comunicazione senza confini – hanno avuto un impatto eccezionale, esteso a tutti gli aspetti della nostra società. Il *cyberspace* aperto e libero, infatti, ha promosso anche l'inclusione politica e sociale a livello mondiale e ha abbattuto le barriere tra paesi, comunità e cittadini, rendendo possibili l'interazione e lo scambio di informazioni e di idee in tutto il globo. Esso, a ben vedere, ha finanche creato un *"forum"* di libertà di espressione e di un sempre maggiore esercizio dei diritti fondamentali e ha conferito altresì potere partecipativo ai cittadini nella ricerca di una società più democratica e più giusta, come è stato dimostrato, in modo anche clamoroso, durante la cd. "Primavera araba" ([3]).

Il *cyberspace* è la realtà più complessa e articolata che l'essere umano abbia mai concepito, costituita dall'unione di reti, di dati e dalla stratificazione di *software* che interconnettono cose, uomini e macchine a livello globale. Ne è prova il fatto che le economie dei paesi moderni – ma in misura crescente anche di quelli emergenti – poggiano sempre più sull'utilizzo dello spazio cibernetico e i programmi di trasformazione digitale ([4]) non fanno altro che aumentare questo inscindibile legame. In detto contesto, non può negarsi che le tecnologie dell'informazione e della comunicazione ("*Information and Communications Technology"* - ICT) siano diventate la spina dorsale della crescita di molti paesi e, al

contempo, una risorsa critica da cui dipendono non solo i settori dell'economia mondiale moderna ([5]), ma anche la politica ([6]). Infatti, i sistemi informativi digitali – e in particolare *Internet* ([7]) – mediante la loro interconnessione in tutte le nazioni del pianeta, svolgono un ruolo essenziale nell'agevolare i movimenti transfrontalieri di beni, servizi e persone a tal punto che la nostra vita quotidiana, i diritti fondamentali, le economie (locali, nazionali e sovranazionali) sono strettamente dipendenti dal regolare funzionamento delle tecnologie dell'informazione e dalla comunicazione tra reti. Al giorno d'oggi queste tecnologie sono alla base di sistemi compositi che fanno funzionare le nostre economie in settori fondamentali (*rectius:* vitali), mentre molti modelli di impresa si fondano sulla disponibilità ininterrotta di reti *Internet* e sul corretto funzionamento dei sistemi informativi interconnessi, di talché la mancanza di interconnessione renderebbe impossibile il loro stesso funzionamento. La presenza di reti *wireless,* alle quali si può accedere praticamente ovunque, ha inoltre sempre di più incoraggiato la diffusione capillare di dispositivi in grado di connettersi nel *cyberspace*: dai *"mobile devices"* fino ai più recenti *"wearable devices"*. Detta elevata pervasività delle tecnologie e delle reti informatiche in ogni strato dell'odierno ambito sociale ha perciò completamente trasformato ogni aspetto della nostra società, ivi compresi l'erogazione e gestione dei servizi pubblici e privati, l'accesso alle informazioni, la loro qualità e quantità, nonché l'interazione tra tutti questi elementi e il cittadino. A ben vedere, questo fenomeno globale incide trasversalmente sull'organizzazione sociale, a partire dalla più semplice attività condotta dai comuni cittadini (si pensi ai pagamenti elettronici, agli acquisti *online*[8], ecc.), passando a quelle compiute dai gestori di servizi – su tutti quelli essenziali (in settori critici quali l'energia, i trasporti, il sistema idrico, l'assistenza sanitaria e la finanza), ma altrettanto può dirsi anche per i fornitori di servizi digitali (mercati *online*, motori di ricerca e servizi di *cloud,* cd. *"cloud computing",* o la "comunicazione da macchina a macchina" ([9]) – per finire con le operazioni condotte in ambito militare ([10]) mediante l'uso delle tecnologie avanzate dei moderni campi di battaglia (dalla raccolta delle informazioni, ai sistemi di elaborazione dati, all'utilizzo di satelliti sui campi di combattimento, al crescente sfruttamento di mezzi da combattimento autonomi, del tipo *"unmanned aerial vehicle"* – UAV ([11]), fino alla strumentazione militare in grado di identificare autonomamente gli obiettivi da colpire, ecc.). Operazioni, queste ultime, che richiedono l'utilizzo di apparati più o meno articolati e di *network* di controllo dipendenti dal *cyberspace* e che, pertanto, scontano inevitabilmente l'esigenza di interfacciarsi con sistemi di comunicazione operanti su reti informatiche complesse – e in quanto tali vulnerabili – soggette dunque a rischio di sabotaggio mediante *malware* ([12]).

Collegarsi alla rete, quindi, oltre a permettere l'accesso ad una mole enorme di informazioni, rende anche tutti i sistemi interconnessi potenzialmente vulnerabili e con essi i loro contenuti. Detto rischio, invero, riguarda sia i singoli individui, sia gli Stati (rispetto ai quali l'attività degli "attori ostili" è prevalentemente finalizzata, sul piano strategico, alla raccolta di informazioni tese a comprendere il posizionamento di un

determinato paese *target* su eventi geopolitici di interesse per l'attore statuale ostile), sia, infine, le grandi realtà aziendali e industriali (banche, società energetiche, società che operano nel settore della difesa, strutture sanitarie, ecc.) che usano la rete per scambiare informazioni, organizzare la fornitura dei servizi da essi erogati, coordinare le relative attività. In quest'ultimo caso, quindi, l'attacco *cyber* può essere indirizzato – ed è questo un altro aspetto sensibile – anche ad acquisire informazioni industriali, commerciali o relative al *know-how*: la vulnerabilità dei sistemi informatici consente, difatti, di accedere in pochi secondi a segreti industriali, militari, brevetti e progetti ad alto contenuto di innovazione tecnologica (per usi militari, civili ovvero duali) che magari hanno richiesto anni di ricerca e, spesso, anche cospicui investimenti finanziari (privati e pubblici). Il crimine informatico ([13]) può, pertanto, decretare il fallimento di aziende (per le imprese che puntano sull'innovazione tecnologica come elemento di sviluppo, il danno potenziale può essere infatti enorme ([14]), il sabotaggio di impianti industriali (anche di quelli rientranti nel novero delle infrastrutture critiche[15]) e di apparati governativi ([16]), causando danni smisurati e non solo sul piano economico ([17]) ma anche organizzativo e d'immagine.

In questa cornice generale è pertanto evidente che non sono a rischio solo gli individui e le aziende ma, più nel complesso, lo stesso bene comune della sicurezza nazionale può potenzialmente essere considerato in serio pericolo. Si pensi alle drammatiche conseguenze che potrebbero derivare dall'alterazione dei sistemi che regolano le grandi linee di trasporto o le reti energetiche ([18]) – impattando in maniera significativa sulla sfera economica di un paese, colpendone duramente i suoi interessi nazionali – o addirittura dalla manomissione dei moderni sistemi di comando e controllo militari di difesa ([19]) e di sicurezza governativa ([20]).

Anche per detta ragione la tutela del *cyberspace,* sia in ambito europeo che in quello dell'Alleanza atlantica ([21]), è oramai divenuta – anche per numerosi servizi di *intelligence* ([22]) – una priorità sotto molteplici aspetti: giuridici ([23]), economici, industriali, tecnologici, nonché di spionaggio ([24]) e difesa militare. Anzi, con particolare riferimento a detto ultimo aspetto, è appena il caso di evidenziare che, nell'immediato futuro, un ruolo chiave nello specifico settore sarà giocato, da un lato, dall'implementazione della *«Joint Declaration»* tra NATO e UE del 6 dicembre 2016, che mira ad ampliare e approfondire la collaborazione tra i due organismi in modo sostanziale, individuando nelle aree di cooperazione anche la *«cybersecurity and defence»* e, dall'altro, dall'avvio della *«Permanent Structured Cooperation on security and defence»* (PeSCo), in attuazione degli articoli 42, paragrafo 6 e 46 nonché del protocollo 10 del Trattato sull'Unione europea (TUE), alla quale il 13 novembre 2017 hanno aderito 23 paesi dell'UE, con l'obiettivo comune di mettere a sistema specifiche capacità militari nonché contribuire allo sviluppo di nuove tecnologie (anche nel settore della *cybersecurity*) e sistemi d'arma utilizzando non solo le risorse dei propri bilanci nazionali ma anche, per la prima volta, le specifiche risorse finanziare europee dedicate a progetti militari e raggruppate

all'interno dell'*«European Defence Fund»* (concernente **«***Research»* e *«Development and acquisition»* e discendente dall'*«European Defence Action Plan»* del 30 novembre 2016). In tal senso, sarebbe quindi auspicabile che mediante i programmi – ivi inclusi quelli di ricerca e innovazione tecnologica – che discenderanno della PeSCo si possano sviluppare *standard* tecnologici di *cybersecurity* europea che possano comportare, tra l'altro, la possibilità di aumentare la sicurezza del mercato interno di componenti strategici per le industrie della difesa.

Occorre peraltro evidenziare un ulteriore, ma non meno significativo, profilo che non può essere trascurato: tali sistemi, oltre a diventare bersaglio per azioni intenzionalmente tese a danneggiare o interrompere il funzionamento degli stessi, possono anche essere "semplicemente" oggetto di incidenti informatici. Entrambe le ipotesi predette presentano, tuttavia, aspetti in gran parte sovrapponibili, in quanto sia le azioni di attacco, cui si è fatto riferimento sinora, sia gli incidenti di tipo non doloso possono impedire, o gravemente turbare, in misura pressoché similare, l'esercizio delle attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia.

In definitiva, appare manifesto come al giorno d'oggi nessuno possa dirsi immune dal rischio di intrusioni o danni, che possono avere effetti devastanti tanto sulla vita personale quanto sull'economica di un intero paese: si tratta oramai di pericoli reali che non possono più essere sottovalutati ([25]). L'accesso al *cyberspace,* infatti, se da una parte ci apre al mondo, dall'altra rende le persone, le aziende e le istituzioni governative potenzialmente esposte a rischi di truffa, furto di informazioni (anche a scopo di spionaggio) o sabotaggio. Ne consegue che la sicurezza delle reti e dei sistemi informativi è, quindi, essenziale per l'armonioso funzionamento dei mercati globali, anche perché, in considerazione della dimensione transnazionale dello spazio cibernetico, le perturbazioni di tali sistemi in un singolo paese, intenzionali o meno e indipendentemente dal luogo in cui si verificano, sono in grado di diffondersi attraverso singoli Stati e provocare conseguenze in tutto il mondo: per questo motivo, in futuro, la correlazione tra la prosperità economica di un dato paese e la qualità, in termini di difesa e resilienza, delle sue infrastrutture cibernetiche sarà sempre più stretta ed ogni nazione che voglia pensare di sopravvivere dovrà pertanto puntare, sempre più, su alti *standard* di *cybersecurity* ([26]) nella società, nel sistema industriale e, non ultimo, negli apparati governativi.

Alla luce di quanto detto, appare di tutta evidenza che sviluppare nuove capacità e nuovi strumenti – non solo tecnologici, ma anche giuridici ed amministrativi – per migliorare la sicurezza *cyber* delle reti rappresenti una sfida di grande importanza per la crescita, il benessere e la sicurezza dei cittadini e che la stessa non possa certamente essere rimandata. È questa la ragione per la quale i governi di tutto il mondo hanno iniziato a sviluppare strategie unitarie in materia di *cybersecurity* e a considerare il *cyberspace* come una questione internazionale connotata dai caratteri dell'urgenza. Ben si comprende, allora, perché, oltre ai

singoli Stati membri ([27]), anche l'Unione europea (UE) abbia ravvisato la necessità di avere una legislazione solida ed efficace per affrontare la minaccia nei confronti dello spazio cibernetico ([28]), ritenendo improcrastinabile dotarsi, per la prima volta, di uno strumento giuridico che, con il fine del ravvicinamento delle legislazioni dei singoli Stati europei, consentisse di implementare una strategia comune europea nel campo della *cybersecurity* ([29]).

È in questo quadro di iniziative – tendenti a costituire un nuovo assetto ordinamentale di disciplina e riferimento per le attività finalizzate al miglioramento della preparazione e della reazione alle minacce cibernetiche – che il 6 luglio 2016 il Parlamento Europeo ha adottato, *ex* art. 288 del Trattato sul funzionamento dell'UE, la direttiva n. 2016/1148 sulla sicurezza dei sistemi delle reti e dell'informazione (*«Network and Information Security»,* cd. "Direttiva NIS"[30]), che stabilisce i requisiti minimi di sicurezza informatica per gli operatori di servizi essenziali ([31]) e servizi digitali – che spesso costituiscono infrastrutture critiche ([32]) per le quali è stato fatto ancora relativamente poco dal punto di vista della *cybersecurity* – e soprattutto rappresenta il primo organico insieme di regole sulla sicurezza informatica in ambito UE. Nelle intenzioni del legislatore europeo, peraltro, la direttiva sulla sicurezza delle reti e dell'informazione dovrebbe prioritariamente assolvere la funzione di intensificazione della cooperazione tra gli Stati membri su una questione vitale qual è quella della sicurezza del *cyberspace.*

2. La direttiva NIS: *ratio* e fondamento giuridico

Considerati i pericoli evidenziati, connessi ad eventuali attacchi cibernetici, la resilienza e la stabilità delle reti e dei sistemi informativi sono, quindi, ritenute sempre più essenziali dall'UE, anche per l'armonioso funzionamento del mercato interno. Ciò anche in considerazione del fatto che, nell'ultimo ventennio, l'Europa ha liberalizzato il mercato delle infrastrutture critiche, comprese le *public utilities* (energia, acqua e gas), affidandole alla gestione/proprietà di soggetti privati, i quali spesso hanno migliorato il servizio procedendo ad una digitalizzazione della gestione di esso, ma d'altro canto non hanno fatto seguire contestuali investimenti nella sicurezza informatica. Le capacità esistenti, infatti, non bastavano a garantire un grado elevato di sicurezza delle reti e dei sistemi informativi nell'UE, anche perché i livelli di preparazione negli Stati membri risultavano molto diversi tra loro, il che comportava una frammentazione degli approcci nel contesto dei paesi dell'Unione. Ne derivava un livello disomogeneo di protezione dei consumatori e delle imprese che comprometteva il livello globale di sicurezza delle reti e dei sistemi informativi nell'UE, aggravato dal fatto che i dispositivi e le capacità tecnologiche esistenti in questo settore erano semplicemente insufficienti per far fronte alla rapida evoluzione delle possibili minacce alla sicurezza e per assicurare un livello elevato comune di protezione in tutti gli Stati membri. Inoltre, la mancanza di obblighi comuni(tari) imposti agli operatori di servizi essenziali e ai fornitori di servizi digitali

rendeva impossibile la creazione di un meccanismo globale ed efficace di cooperazione a livello dell'Unione. Un approccio esclusivamente facoltativo aveva fatto sì che la cooperazione funzionasse solo tra una minoranza di Stati membri che avessero avuto un livello elevato di capacità. È evidente come questa situazione ostacolasse anche la creazione di quel clima di fiducia tra pari, indispensabile per la collaborazione e lo scambio di informazioni nel *cyberspace,* in quanto la cooperazione operava solo tra quella minoranza di Stati membri che avevano un elevato livello di capacità di difesa e resilienza. Nel descritto contesto, infatti, le disparità derivanti da capacità disuguali dei singoli Stati membri in materia di regolamentazione della sicurezza delle reti e dell'informazione, ma soprattutto in termini di politiche e di livello di protezione, aveva anche creato barriere nel mercato interno (soprattutto per quelle imprese che desideravano operare in vari paesi e per il conseguimento di economie di scala globali) che giustificavano, in maniera ormai ineludibile, un'azione a livello europeo. Dette disorganicità normative, in virtù della nota interconnessione tra le reti e i predetti sistemi, comportavano inoltre che la sicurezza generale delle reti informatiche dell'UE risultasse fortemente indebolita dai (non pochi) Stati membri che adottavano a loro interno un livello insufficiente di protezione. Il tutto risultava aggravato dalla scarsa capacità di generare deterrenza e difesa che, unita all'incapacità di coordinare ruoli, competenze e risposte alle minacce cibernetiche, contribuiva a creare in ambito europeo uno scenario complessivo evidentemente inquietante in cui la resilienza e la stabilità delle reti e dei sistemi informativi diventavano essenziali per il completamento del mercato unico digitale, oltre che per l'armonioso funzionamento del mercato europeo. Al fine di poter contenere e minimizzare le ripercussioni negative degli incidenti informatici occorreva, quindi, che le misure in materia di sicurezza delle reti e dell'informazione adottate dalle amministrazioni nazionali fossero quantomeno coerenti tra loro, obiettivo, questo, che nelle intenzioni del legislatore europeo, grazie alla direttiva in esame, dovrebbe essere raggiunto. In mancanza di quest'ultima, invero, sarebbe stata destinata a perdurare una situazione in cui ogni Stato avrebbe continuato ad agire da solo, senza tener conto delle interdipendenze tra le reti e i sistemi informativi in tutta l'Unione e attraverso strategie incoerenti e norme divergenti, con la naturale conseguenza – anche in considerazione della natura transnazionale della sicurezza delle reti e dell'informazione e conseguentemente degli incidenti e dei rischi a carico delle stesse – di una protezione insufficiente dello spazio cibernetico nell'UE.

D'altro canto, nel corso dell'ultimo decennio si era anche presa sempre più coscienza che l'eventuale imposizione di obblighi agli Stati membri sulla gestione dello spazio cibernetico avrebbe garantito un adeguato livello di preparazione a livello nazionale e avrebbe, altresì, contribuito a creare quel clima di affidamento reciproco che costituisce un prerequisito per l'effettiva collaborazione a livello dell'UE. Inoltre, l'imposizione alle amministrazioni pubbliche ed ai principali operatori privati di obblighi in

materia di gestione dei rischi a carico della sicurezza delle reti e dell'informazione (SRI) avrebbe certamente costituito un forte incentivo alla gestione efficace dei rischi di sicurezza. L'obbligo di segnalare gli incidenti SRI aventi un impatto significativo avrebbe rafforzato, ad esempio, le capacità di risposta agli incidenti stessi e la trasparenza. Mettendo pertanto ordine al suo interno, l'Unione avrebbe potuto imporsi a livello internazionale e diventare un *partner* ancora più credibile per la collaborazione a livello bilaterale e multilaterale, acquisendo così la capacità di promuovere con più forza i diritti e i valori fondamentali dell'UE al suo esterno. Consapevole di tutte le suddette ragioni, l'UE ha ritenuto essenziale coinvolgere tutti gli Stati membri nella gestione sinergica dello spazio cibernetico e, per fare ciò, il presupposto necessario era che tutti disponessero del livello minimo di capacità occorrente. Per una risposta efficace alle sfide in materia di sicurezza delle reti e dei sistemi informativi, era infatti necessario un approccio condiviso a livello di Unione, che contemplasse la creazione di una capacità minima comune e la previsione di disposizioni normative minime in materia di autorità competenti, pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali. Solo un coordinamento adeguato tra gli Stati membri, invero, poteva tentare di garantire la corretta gestione dei rischi a livello della sicurezza delle reti e dell'informazione nel loro contesto transfrontaliero, creando parità di condizioni e ovviando alle lacune legislative esistenti attraverso l'introduzione di opportuni obblighi giuridici funzionali al raggiungimento di tale scopo. Alla luce del quadro generale appena descritto e al fine di garantire un sistema giuridico uniforme, l'UE non poteva che intervenire con un atto normativo che consentisse di delineare un *framework* di riferimento in materia di *cybersecurity*. Sotto questo aspetto, la direttiva ([33]) NIS rappresenta, dunque, il primo e univoco insieme di regole sulla sicurezza informatica a livello dell'Unione ([34]), rientrando tra gli obiettivi della strategia ([35]) da essa adottata in relazione alla *cybersecurity* (un ciberspazio aperto e sicuro[36], riguardo al quale il Consiglio ha adottato conclusioni il 25 giugno 2013[37]), tesa a prevenire e rispondere alle perturbazioni e agli attacchi che colpiscono i sistemi di telecomunicazione in Europa. La strategia, infatti, prevedeva una prima proposta recante la comunicazione della Commissione e dell'Alto rappresentante dell'UE per gli affari esteri e la politica di sicurezza che delineasse una strategia dell'UE per la sicurezza cibernetica; detta comunicazione avrebbe dovuto essere poi supportata dal secondo elemento della strategia stessa, ovvero una seconda proposta recante, appunto, la direttiva sulla sicurezza delle reti e dell'informazione in esame.

Sul piano dei principi giuridici generali, il ricorso all'atto normativo europeo in parola è espressione del principio di sussidiarietà sancito dall'articolo 5 del TUE ([38]); la direttiva, nel rispetto altresì del principio di proporzionalità ([39]), ha quindi il fine di procedere ad un ravvicinamento delle normative (laddove esistenti) dei singoli Stati facenti parti dell'UE. Come è noto, infatti, l'UE ha il potere di adottare misure

destinate all'instaurazione o al funzionamento del mercato interno, conformemente alle disposizioni pertinenti dei trattati (art. 26 del Trattato sul funzionamento dell'Unione europea - TFUE) e, in particolare, a norma dell'articolo 114 TFUE, può adottare «[…] le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione o il funzionamento del mercato interno».

Rifacendosi al modello della direttiva quadro sulle comunicazioni elettroniche, la direttiva NIS mira a garantire lo sviluppo di una cultura della gestione dei rischi e dello scambio di informazioni tra i settori pubblico e privato. Alle imprese attive nei settori specifici (quali, ad esempio, quello delle infrastrutture critiche ovvero quello della fornitura dei servizi essenziali per il funzionamento della nostra società) e alle pubbliche amministrazioni sarà, infatti, chiesto di valutare i rischi che corrono e conseguentemente di adottare misure adeguate e proporzionate per garantire la sicurezza delle reti e dell'informazione (i predetti soggetti, per esempio, dovranno segnalare alle autorità competenti gli incidenti suscettibili di compromettere gravemente le loro reti e sistemi informativi, aventi un impatto significativo sulla continuità di servizi critici e sulla fornitura di beni).

3. La direttiva NIS: uno sguardo d'insieme sulle finalità e l'ambito di applicazione

Si è ampiamente detto che i sistemi informativi digitali, quali strumenti di comunicazione senza confini, sono interconnessi in tutti gli Stati membri e svolgono un ruolo essenziale nel facilitare i movimenti di beni, servizi e persone. In particolare, con lo sviluppo del mercato interno dell'UE, molti sistemi di rete e informativi hanno assunto una dimensione transfrontaliera; molte imprese e amministrazioni in tutta l'UE si affidano, infatti, alle reti e alle infrastrutture digitali per fornire i loro servizi essenziali. Si è, altresì, evidenziato che i sistemi ICT odierni possono essere vittime di incidenti di sicurezza – siano essi guasti tecnici o *virus* – e che un incidente a carico della sicurezza delle reti e dell'informazione (SRI) verificatosi in un paese può avere ripercussioni in altri Stati membri o persino in tutta l'Unione.

Questo tipo di incidenti, denominati "incidenti SRI", stanno diventando più frequenti e più difficili da gestire; quando si verifica un incidente a carico della SRI, infatti, l'impatto può essere considerevole, poiché i servizi transnazionali vengono compromessi e le imprese non possono lavorare secondo i previsti canoni di produzione. Oltre a ciò, gli incidenti SRI indeboliscono la fiducia dei consumatori nei sistemi di pagamento *online* e nelle reti informatiche, con evidenti ricadute sulla libera circolazione di beni e servizi nel mercato interno. Proprio in ragione dell'evidente transnazionalità del fenomeno *cyber,* una delle prescrizioni più significative delle nuove norme europee riguarda gli obblighi di sicurezza e di notifica degli incidenti per gli operatori di servizi essenziali e delle infrastrutture critiche. Introducendo,

infatti, misure di gestione del rischio più coerenti e la segnalazione sistematica degli incidenti, la direttiva NIS aiuta i settori che dipendono dai sistemi ICT ad essere più affidabili e stabili.

Prima di procedere ad un esame dettagliato delle singole disposizioni della direttiva NIS, può senz'altro anticiparsi che le indicazioni da essa espresse, per quanto ancora generali, sono in linea con l'impostazione attuale della gestione della sicurezza come strumento di mitigazione del rischio. Inoltre, una disamina di carattere generale ci consente di affermare che i punti chiave della direttiva NIS possono sintetizzarsi nell'obbligare gli Stati ad adottare una strategia nazionale (per un esame dettagliato v. *infra* par. 3.1) in materia di sicurezza della rete e dei sistemi informativi, nel migliorare le capacità di *cybersecurity* dei singoli Stati dell'UE, nell'aumentare il livello di cooperazione tra gli Stati membri dell'Unione, nell'obbligare gli operatori di servizi essenziali e i fornitori di servizi digitali alla gestione dei rischi ed a riferire gli incidenti di una certa entità. In una prospettiva sinergica, infatti, la cooperazione tra i vari enti dei singoli Stati membri è un punto veramente fondamentale della direttiva in parola. A questo scopo, come vedremo innanzi nel dettaglio, la direttiva chiede agli Stati membri di designare una o più autorità nazionali, di elaborare una strategia per affrontare le minacce relative alla *cybersecurity*, nonché di aumentare il loro grado di preparazione e di migliorare la collaborazione reciproca.

L'ultimo dei punti chiave della direttiva riguarda gli operatori dei servizi essenziali per i singoli Stati membri e i fornitori di servizi digitali. Al riguardo, la direttiva NIS elenca una serie di settori critici in cui sono attivi gli operatori di servizi essenziali, quali l'energia, i trasporti, la finanza e la sanità. Come si vedrà innanzi più nel dettaglio, in questi settori gli Stati membri, sulla base di criteri precisi stabiliti nella direttiva, avranno il dovere di identificare gli operatori che forniscono i cd. «servizi essenziali»; la direttiva sul punto si limita a indicare i criteri che dovranno essere applicati a livello nazionale, con l'auspicio che ciò avvenga ovunque in modo coerente e che, laddove un operatore eroghi servizi in diversi Stati membri, un accordo fra gli stessi regoli la loro definizione ai sensi della direttiva, al fine di evitare un approccio differenziato in ambito UE. Gli obblighi e la supervisione saranno maggiori per questi operatori rispetto ai fornitori di «servizi digitali», atteso il livello di rischio che eventuali perturbazioni di detta tipologia di servizi possono determinare per il mantenimento di attività sociali e/o economiche fondamentali, quelle che comunemente vengono chiamate "infrastrutture critiche". La direttiva NIS perciò obbliga i gestori di tali servizi ([40]) a dotarsi di misure di sicurezza appropriate ([41]) e di notificare all'autorità nazionale competente gravi incidenti di sicurezza, secondo parametri di numero di utenti coinvolti, durata dell'incidente e diffusione geografica. Oltre alle misure già previste per gli operatori di servizi essenziali, le misure di sicurezza relative ai fornitori di servizi digitali prevedono alcuni fattori specifici, come ad esempio la sicurezza dei sistemi e degli impianti, la gestione della continuità operativa, il monitoraggio e i *test* e la conformità a norme internazionali. Per quanto riguarda i parametri per la valutazione di un incidente

rilevante che va segnalato, vi sono, oltre a quelli sopra elencati, anche l'entità dell'interruzione del servizio e l'impatto sulle attività economiche e sociali.

In questa cornice descrittiva generale, giova rilevare, infine, che la pubblica amministrazione non è espressamente compresa nell'ambito di applicazione della direttiva NIS (benché lo sia certamente quale soggetto garante dell'intera architettura istituzionale che dovrà essere definitiva in attuazione della direttiva NIS, sul quale v. *infra* par. 4.1 e 5), nondimeno gli Stati membri hanno la possibilità di estendere il raggio d'azione della stessa, e quindi applicarne le regole, in termini di requisiti di sicurezza e obblighi di notifica, anche a settori da essa non direttamente disciplinati (qual è quello pubblico), laddove l'amministrazione eroghi servizi essenziali.

3.1 *(Segue):* analisi di dettaglio della direttiva NIS

Quanto appena descritto illustra i principi giuridici cardine su cui si regge l'intero sistema normativo introdotto dalla direttiva NIS; vediamo adesso, nel dettaglio, le singole disposizioni della direttiva al fine di verificarne potenzialità e relative criticità anche in ottica *de iure condendo.*

La direttiva NIS è suddivisa in sette capi ed è composta da ventisette articoli e tre allegati. L'art. 1 definisce gli obiettivi della direttiva, individuati nella finalità di conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi ([42]) nell'UE, così da migliorare il funzionamento del mercato interno. A tal fine, la direttiva fa obbligo a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi che definisca gli obiettivi e le priorità strategiche, le politiche adeguate e le misure di regolamentazione per affrontare le questioni di *cybersecurity.* All'uopo la direttiva NIS istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi. Essa, inoltre, crea una rete nazionale di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT» - *«Computer Security Incident Response Team»*) per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace (v. *infra,* art. 12), che diventano il cardine delle attività di analisi e contrasto, anche attraverso una rete di cooperazione (cd. *"Cooperation Network"*). L'art. 1 prevede, altresì, una sorta di clausola di salvaguardia finale relativa allo scambio di informazioni riservate ai sensi della normativa dell'Unione e nazionale, quale quella sulla riservatezza degli affari; in tal senso, è disposto che, fatto salvo quanto previsto dall'articolo 346 TFUE ([43]), le predette informazioni siano scambiate con la Commissione e con altre autorità competenti solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione della direttiva stessa e che le informazioni scambiate siano limitate alle informazioni pertinenti e commisurate allo scopo. Lo scambio di informazioni, pertanto, tutela la riservatezza dei dati e protegge la sicurezza e gli interessi commerciali degli operatori di servizi essenziali

e dei fornitori di servizi digitali. Un'importante disposizione di chiusura è contenuta nell'ultimo comma dell'art. 1, in cui è disposto che, qualora un atto giuridico settoriale dell'UE faccia obbligo agli operatori di servizi essenziali o ai fornitori di servizi digitali di assicurare la sicurezza delle loro reti e dei loro sistemi informativi o di notificare gli incidenti, nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui alla presente direttiva, si applicheranno le disposizioni di detto atto giuridico settoriale dell'Unione.

L'art. 2 della direttiva disciplina il trattamento di dati personali, stabilendo che lo stesso è effettuato ai sensi della direttiva 95/46/CE.

Di particolare rilievo è l'art. 3, il quale sancisce il principio di "armonizzazione minima", disponendo che, fatto salvo l'articolo 16, par. 10, e gli obblighi loro imposti dal diritto dell'Unione, gli Stati membri possono adottare o mantenere in vigore disposizioni atte a conseguire un livello di sicurezza più elevato della rete e dei sistemi informativi.

L'art. 4 della direttiva in esame, la cui collocazione più opportuna sul piano del *drafting* normativo sarebbe stata ragionevolmente all'art. 1, reca una serie di definizioni utili ai fini di una migliore comprensione degli aspetti tecnici e procedurali della direttiva NIS.

Una norma di particolare rilievo è certamente l'art. 5, il quale stabilisce che, entro il 9 novembre 2018, gli Stati membri identifichino, per ciascun settore e sotto-settore di cui all'allegato II (energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile e infrastrutture digitali), gli operatori (che ai sensi dell'art. 4, punto 4 della direttiva sono soggetti pubblici[44] o privati) di servizi essenziali (analoga norma non è invece prevista per i fornitori di servizi digitali) con una sede nel loro territorio, fissando altresì i criteri per l'identificazione degli operatori di servizi essenziali nei seguenti: a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio. Qualora un soggetto fornisca un servizio ritenuto essenziale per il mantenimento di attività sociali e/o economiche fondamentali in due o più Stati membri, questi ultimi avviano consultazioni reciproche che si svolgono comunque prima che sia presa una decisione sull'identificazione. Nel processo di identificazione degli operatori di servizi essenziali ([45]), gli Stati membri dovranno valutare, almeno per ciascun sotto-settore di intervento della direttiva, quali servizi debbano essere considerati essenziali per il mantenimento di attività sociali ed economiche fondamentali e se i soggetti elencati nei settori e sotto-settori di cui alla direttiva, che forniscono tali servizi, rispettino i criteri per l'identificazione degli operatori. Nel valutare se un soggetto fornisce un servizio essenziale per il mantenimento di attività sociali ed economiche fondamentali, sarà sufficiente esaminare se il soggetto fornisce un servizio incluso nell'elenco di servizi

essenziali. Si dovrebbe, inoltre, dimostrare che la fornitura del servizio essenziale dipende dalle reti e dai sistemi informativi. Inoltre, nel valutare se un incidente possa avere un effetto negativo significativo sulla fornitura del servizio, gli Stati membri dovrebbero tenere conto di una serie di fattori intersettoriali, nonché, ove opportuno, di fattori settoriali. Detto contesto è di tale complessità che, per la sola classificazione di detti servizi essenziali, la direttiva prevede un ulteriore periodo di sei mesi rispetto al termine di recepimento della stessa (quindi entro il 9 novembre 2018). Giova evidenziare che, in seguito al processo di identificazione, gli Stati membri dovrebbero, poi, adottare misure nazionali dirette a determinare i soggetti cui si applicano gli obblighi in materia di sicurezza delle reti e dei sistemi informativi. Tale risultato potrebbe essere raggiunto adottando un elenco di tutti gli operatori di servizi essenziali, oppure adottando misure nazionali comprendenti criteri oggettivi quantificabili (quali la produzione dell'operatore o il numero di utenti) che rendano possibile determinare a quali soggetti si applichino i predetti obblighi in materia di sicurezza delle reti e dei sistemi informativi. Infine, le misure nazionali, siano esse già esistenti o adottate nel contesto della direttiva NIS, dovrebbero includere tutte le misure giuridiche, amministrative e le prassi che rendano possibile l'identificazione degli operatori di servizi essenziali ai sensi della direttiva stessa. Per il processo in parola, in una prospettiva *de iure condendo,* stanti le differenze fondamentali tra gli operatori di servizi essenziali (in particolare per il loro collegamento diretto con le infrastrutture fisiche) e i fornitori di servizi digitali (in particolare per la loro natura transnazionale), il recepimento della direttiva NIS potrebbe adottare un approccio differenziato rispetto ai due gruppi di soggetti; in particolare, per gli operatori di servizi essenziali, gli Stati membri dovrebbero poter identificare gli agenti operatori e imporre requisiti, se del caso, anche più rigorosi di quelli previsti dalla direttiva. Gli Stati membri non dovrebbero, invece, identificare i fornitori di servizi digitali, in quanto la direttiva dovrebbe applicarsi a tutti i fornitori di servizi digitali rientranti nel campo di applicazione della stessa. Inoltre, la direttiva in esame e i discendenti provvedimenti di attuazione da parte dei singoli Stati membri dovrebbero assicurare un elevato livello di armonizzazione per i fornitori di servizi digitali con riguardo agli obblighi di notifica e di sicurezza. Ciò dovrebbe consentire che i fornitori di servizi digitali siano trattati in modo uniforme in tutta l'UE, in modo proporzionato alla loro natura e al grado di rischio cui potrebbero essere esposti.

L'art. 6 della direttiva *de qua* disciplina gli effetti negativi rilevanti di cui all'articolo 5, par. 2, lettera c). A tal fine, nella determinazione della rilevanza dei predetti effetti negativi, gli Stati membri dovranno tenere conto dei seguenti fattori intersettoriali: a) il numero di utenti che dipendono dal servizio fornito dal soggetto interessato; b) la dipendenza di altri settori di cui all'allegato II dal servizio fornito da tale soggetto; c) l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza; d) la quota di mercato del soggetto coinvolto; e) la

diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente; f) l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura del servizio stesso. Il medesimo articolo, con un'apposita norma di chiusura (co. 2), stabilisce, altresì, che, al fine di determinare se un incidente ha effetti negativi rilevanti sulla fornitura di un servizio essenziale, gli Stati membri, in aggiunta ai fattori intersettoriali, dovranno tener conto anche di fattori settoriali.

Detti fattori potrebbero comprendere: per i fornitori di energia, il volume o la quota di energia nazionale prodotta; per i fornitori di petrolio, il volume su base giornaliera; per il trasporto aereo, inclusi aeroporti e vettori aerei, il trasporto ferroviario e i porti marittimi ([46]), la quota di volume di traffico nazionale e il numero di passeggeri o di operazioni di trasporto merci su base annua; per il settore bancario o le infrastrutture dei mercati finanziari, la loro importanza sistemica in base alle attività totali o al rapporto tra tali attività totali e il PIL; per il settore sanitario, il numero di pazienti assistiti dal fornitore su base annua; per la produzione, il trattamento e la fornitura di acqua, il volume e il numero e i tipi di utenti riforniti, inclusi, ad esempio, ospedali, servizi pubblici, organizzazioni o persone fisiche, nonché l'esistenza di fonti idriche alternative per servire la stessa area geografica.

A parere dello scrivente, una delle disposizioni cardine della direttiva in esame è l'art. 7, a mente del quale ogni Stato membro adotta una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi che definisce gli obiettivi strategici e le opportune misure strategiche e regolamentari al fine di conseguire e mantenere un livello elevato di *cybersecurity*, che contempli almeno i settori di cui all'allegato II (energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile e infrastrutture digitali) e i servizi di cui all'allegato III (mercato *online,* motore di ricerca *online* e servizi nella nuvola - *cloud computing*). Ai sensi della disposizione in esame, la strategia nazionale del singolo Stato membro in materia di sicurezza delle reti e dei sistemi informativi deve affrontare in particolare i seguenti aspetti: a) gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi; b) un quadro di *governance* per conseguire gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi, inclusi i ruoli e le responsabilità degli organismi pubblici ([47]) e degli altri attori pertinenti; c) l'individuazione delle misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato; d) un'indicazione di programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi; e) un'indicazione di piani di ricerca e sviluppo relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi; f) un piano di valutazione per individuare i rischi; g) un elenco dei vari attori coinvolti nell'attuazione della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi. Una volta proceduto

all'adozione delle strategie nazionali in materia di sicurezza della rete e dei sistemi informativi, gli Stati membri dovranno comunicare dette strategie alla Commissione entro tre mesi dalla loro adozione; a tal fine, gli Stati membri possono escludere elementi della strategia riguardanti la sicurezza nazionale.

Altra norma di fondamentale importanza è l'art. 8 della direttiva NIS, che concerne, invece, l'architettura istituzionale di cui ogni singolo Stato membro dovrà dotarsi, imponendo agli stessi la designazione di una o più autorità nazionali competenti in materia di sicurezza delle reti e dei sistemi informativi (cd. «Autorità competente»), con il compito di occuparsi almeno dei settori di cui all'allegato II (energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile e infrastrutture digitali) e dei servizi di cui all'allegato III (mercato *online,* motore di ricerca *online* e servizi nella nuvola-*cloud computing*), prevedendo tuttavia che gli Stati membri possano affidare questo ruolo a una o più autorità esistenti. Di fondamentale importanza è il ruolo delle autorità nazionali competenti che verranno individuate e che avranno il (non semplice) compito di controllare l'applicazione della direttiva NIS a livello nazionale. A tal fine, ogni Stato membro dovrà designare un punto di contatto unico nazionale in materia di sicurezza delle reti e dei sistemi informativi (cd. «Punto di contatto unico», sul quale v. anche *infra* art. 14); anche in questo caso gli Stati membri possono affidare questo ruolo a un'autorità già esistente. La disposizione precisa che se uno Stato membro designa soltanto un'autorità competente, quest'ultima è anche il punto di contatto unico. Quest'ultimo svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità degli Stati membri con le autorità competenti negli altri Stati membri e con il gruppo di cooperazione di cui all'art. 11 e la rete di CSIRT di cui all'art. 12 della direttiva medesima. Ogni Stato membro dovrà comunque comunicare alla Commissione la designazione dell'autorità competente e del punto di contatto unico, i loro compiti e qualsiasi variazione dei medesimi.

Di peculiare rilievo, anche in termini di previsione di compiti operativi, è l'art. 9 della direttiva NIS. Infatti, sul presupposto che gli Stati membri siano dotati delle capacità tecniche e organizzative necessarie a prevenire, individuare, rispondere e attenuare i rischi e gli incidenti a carico delle reti e dei sistemi informativi, la direttiva fa obbligo agli Stati membri di designare uno o più gruppi di intervento per la sicurezza informatica in caso di incidente (cd. «CSIRT»), anche noti come squadre di pronto intervento informatico («CERT»[48]). Tali soggetti devono essere conformi ai requisiti di cui all'allegato I, punto 1, della direttiva in esame, occuparsi almeno dei settori di cui all'allegato II (energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile e infrastrutture digitali) e dei servizi di cui all'allegato III (mercato *online,* motore di ricerca *online* e servizi nella nuvola-*cloud computing*) e devono adempiere non solo compiti connessi alla sicurezza della rete e dei sistemi informativi ed essere ben funzionanti e rispondenti a determinati requisiti essenziali (in modo da

garantire l'esistenza di capacità effettive e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello di Unione), ma devono svolgere altresì il compito di trattare gli incidenti e i rischi secondo una procedura ben definita e l'accesso a un'infrastruttura di informazione e comunicazione appropriata, sicura e resiliente a livello nazionale. Al riguardo, la direttiva prevede che un CSIRT possa essere creato anche all'interno dell'autorità competente; esso, in base a quanto previsto dall'allegato I della direttiva NIS, dovrà comunque essere responsabile del monitoraggio degli incidenti a livello nazionale, fornendo allarmi tempestivi, avvisi ed annunci con lo scopo di diffondere informazioni su rischi e incidenti per promuovere la cooperazione operativa. Dovrà, inoltre, fornire analisi sui rischi e sugli incidenti e aumentare il grado di consapevolezza, nonché garantire la cooperazione internazionale e *l'"information sharing"*. Data l'importanza della cooperazione internazionale in materia di sicurezza cibernetica, i CSIRT dovrebbero poter anche partecipare a reti di cooperazione internazionale, oltre alla rete di CSIRT istituita dalla direttiva in esame. Una volta istituiti, gli Stati membri hanno l'obbligo di comunicare alla Commissione il mandato dei loro CSIRT e gli elementi principali della procedura di trattamento degli incidenti loro affidata.

L'art. 10 della direttiva NIS, in attuazione del principio della cooperazione a livello nazionale, prevede che se l'autorità competente all'uopo individuata, il punto di contatto unico e i CSIRT dello stesso Stato membro sono separati, gli stessi devono comunque collaborare per quanto concerne l'adempimento degli obblighi scaturenti dalla direttiva. A tal fine, gli Stati membri dovranno garantire che le autorità competenti oppure i CSIRT ricevano le notifiche di incidenti trasmesse ai sensi della direttiva e che ove uno Stato membro decida che i CSIRT non ricevano le notifiche, questi ultimi abbiano accesso, nella misura necessaria per l'esecuzione dei loro compiti, ai dati sugli incidenti notificati dagli operatori di servizi essenziali ai sensi dell'art. 14, paragrafi 3 e 5, o dai fornitori di servizi digitali ai sensi dell'art. 16, paragrafi 3 e 6. Gli Stati membri dovranno, altresì, garantire che le autorità competenti o i CSIRT informino i punti di contatto unici in merito alle notifiche di incidenti trasmesse ai sensi della direttiva in esame. Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni, di sviluppare la fiducia, anche nell'ottica di conseguire un livello comune elevato di sicurezza delle reti e dei servizi informativi nell'UE e fra Stati membri, l'art. 11 dispone, altresì, che sia istituito un gruppo di cooperazione. Quest'ultimo dovrà essere composto da rappresentati degli Stati membri, dalla Commissione e dall'ENISA (*«European Union for Network and Information Security Agency»*[49]). Le quattro aree di lavoro del gruppo dovranno essere quelle di pianificazione, guida, segnalazione e condivisione. Un singolo punto di contatto dovrà inoltre essere designato da ognuno degli Stati membri, con il compito di assicurare la cooperazione internazionale e di collegarsi con gli altri Stati attraverso meccanismi di cooperazione identificati dalla direttiva stessa.

L'art. 12 della direttiva NIS dispone che, al fine di contribuire allo sviluppo della fiducia fra gli Stati membri e di promuovere una cooperazione operativa rapida ed efficace, debba essere istituita una rete di CSIRT. Questa è composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE (la Commissione partecipa alla rete dei CSIRT in qualità di osservatore) e ha numerosi e rilevanti compiti tra i quali, di maggior rilievo, lo scambio di informazioni sui servizi, sulle operazioni e sulle capacità di cooperazione; il sostegno agli Stati membri nel far fronte a incidenti transfrontalieri, sulla base dell'assistenza reciproca volontaria; la discussione, l'esame e l'individuazione di ulteriori forme di cooperazione operativa; infine, il compito di formulare orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni in materia di cooperazione operativa.

Sempre in tema di cooperazione, assume rilievo l'art. 13 della direttiva, che reca disposizioni in materia di cooperazione internazionale, prevedendo che l'UE possa concludere accordi internazionali ([50]) ai sensi dell'articolo 218 TFUE con paesi terzi o organizzazioni internazionali che consentano e organizzino la loro partecipazione a talune delle attività del gruppo di cooperazione. Detti accordi dovranno tenere conto della necessità di garantire la protezione adeguata dei dati. A tal fine, sarebbe auspicabile che nel prossimo futuro si possa giungere a stipulare accordi politici tra Stati che, omogeneizzando le differenze (in alcuni casi carenze) normative, legislative, organizzative e culturali, favoriscano lo scambio di informazioni e *best practices* per la *cybersecurity* ([51]).

L'art. 14 della direttiva in rassegna disciplina gli obblighi in materia di sicurezza e notifica degli incidenti per gli operatori di servizi essenziali ([52]). Tuttavia, come visto, gli obblighi di sicurezza e di notifica, ai sensi dell'art. 1, par. 3 della direttiva, non si applicano alle imprese che sono soggette agli obblighi di cui agli articoli 13 *bis* e 13 *ter* della direttiva 2002/21/CE, né ai prestatori di servizi fiduciari che sono soggetti agli obblighi di cui all'articolo 19 del regolamento (UE) n. 910/2014. In particolare, in riferimento agli operatori di servizi essenziali, gli obblighi sono riconducibili a due ambiti specifici: obblighi di sicurezza e obblighi di notifica. A tal fine, la disposizione in esame prevede che gli Stati membri provvedano affinché gli operatori di servizi essenziali adottino misure tecniche e organizzative idonee e proporzionate alla gestione dei rischi incidenti sulla sicurezza delle reti e dei sistemi informativi usati nelle loro operazioni: le misure adottate dovranno contemplare un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente. Inoltre, gli Stati membri dovranno provvedere affinché gli operatori di servizi essenziali adottino misure atte a prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi; gli stessi dovranno altresì provvedere affinché gli operatori di tali servizi notifichino senza ritardo all'autorità competente individuata dal singolo Stato membro o al CSIRT

gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati e le notifiche dovranno includere le informazioni che consentono all'autorità competente o al CSIRT di determinare qualsiasi impatto transfrontaliero dell'incidente. Queste notifiche saranno poi utilizzate dalle autorità competenti e/o dai CSIRT, anche nell'ambito di un quadro nazionale ed europeo, nella prevenzione di incidenti analoghi e, laddove opportuno e sentiti gli operatori coinvolti, per informare eventualmente il pubblico dell'incidente in corso. Di particolare interesse è la disposizione di cui all'art. 14, co. 4, nella parte in cui prevede che per determinare la rilevanza dell'impatto di un incidente si debba tenere conto, in particolare, dei seguenti parametri: a) il numero di utenti interessati dalla perturbazione del servizio essenziale; b) la durata dell'incidente; c) la diffusione geografica relativamente all'area interessata dall'incidente. In virtù delle informazioni fornite nella notifica da parte dell'operatore di servizi essenziali, l'autorità competente o il CSIRT dovrà informare l'altro o gli altri Stati membri interessati se l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali in quello Stato membro. A tal fine, l'autorità competente o il CSIRT dovrà preservare, conformemente al diritto dell'UE o alla legislazione nazionale conforme al diritto dell'Unione, la sicurezza e gli interessi commerciali dell'operatore di servizi essenziali, nonché la riservatezza delle informazioni fornite nella sua notifica. Ove le circostanze lo consentano, la disposizione in esame prevede che l'autorità competente o il CSIRT dovrà altresì fornire all'operatore di servizi essenziali che effettua la notifica di incidente le pertinenti informazioni relative al seguito della notifica stessa, come quelle che possano facilitare un trattamento efficace dell'incidente. Su richiesta dell'autorità competente o del CSIRT, il punto di contatto unico di cui all'art. 8 della direttiva dovrà trasmettere le notifiche degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati ai punti di contatto unici degli altri Stati membri interessati. Dopo aver consultato l'operatore notificante dei servizi essenziali, l'autorità competente o il CSIRT, qualora sia necessaria la sensibilizzazione del pubblico per evitare un incidente o gestirne uno in corso, potrà informare il pubblico in merito ai singoli incidenti.

L'art. 15 della direttiva NIS – altra norma di rilevante importanza nell'ottica del funzionamento complessivo del sistema di sicurezza dello spazio cibernetico – reca disposizioni in tema di attuazione e controllo e dispone che gli Stati membri provvedano affinché le autorità competenti individuate siano dotate dei poteri e dei mezzi necessari per valutare la conformità degli operatori di servizi essenziali agli obblighi loro imposti dall'articolo 14 e i relativi effetti sulla sicurezza della rete e dei sistemi informativi. A tal fine, con una disposizione che si presenta tra le più delicate nella prospettiva *de iure condendo,* la direttiva dispone che gli Stati membri provvedano affinché le autorità competenti siano dotate dei poteri (non si capisce bene di che tipo, ma sembra ovvio che si debba fare riferimento a quelli di accertamento, verifica, controllo) e dei mezzi (anch'essi non definiti: sanzionatori e repressivi ai sensi dell'art. 21? Ad

esempio, per quanto riguarda l'Italia, così sembrerebbe doversi procedere ai sensi dell'obiettivo operativo 6.3 del «Piano nazionale per la protezione cibernetica e la sicurezza informatica» 2017) per richiedere agli operatori di servizi essenziali di fornire: a) le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza; b) la prova dell'effettiva attuazione delle politiche di sicurezza, come i risultati di un *audit* sulla sicurezza svolto dall'autorità competente o da un revisore abilitato e, in quest'ultimo caso, mettere a disposizione dell'autorità competente i risultati, inclusi gli elementi di prova. Quando richiede tali informazioni o prove, l'autorità competente indica lo scopo della stessa specificando il tipo di informazioni da fornire. Successivamente alla valutazione delle informazioni o dei risultati degli *audit* sulla sicurezza, l'autorità competente potrà emanare istruzioni vincolanti per gli operatori di servizi essenziali al fine di porre rimedio alle carenze individuate.

L'art. 16 disciplina invece gli obblighi in materia di sicurezza e notifica degli incidenti per i fornitori di servizi digitali ([53]). Anche in questo caso, a similitudine di quanto previsto all'art. 14 per gli operatori di servizi essenziali, per espresso richiamo dell'art. 1, par. 3 della direttiva, gli obblighi di sicurezza e di notifica non si applicano alle imprese che sono soggette agli obblighi di cui agli articoli 13 *bis* e 13 *ter* della direttiva 2002/21/CE, né ai prestatori di servizi fiduciari che sono soggetti agli obblighi di cui all'art. 19 del regolamento (UE) n. 910/2014. Nello specifico, la disposizione in esame prevede che gli Stati membri provvedano affinché i fornitori di servizi digitali identifichino e adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dell'offerta di servizi digitali all'interno dell'UE. Tali misure dovranno assicurare un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente e dovranno tenere conto dei seguenti elementi: a) sicurezza dei sistemi e degli impianti; b) trattamento degli incidenti; c) gestione della continuità operativa; d) monitoraggio, *audit* e *test*; e) conformità con le norme internazionali. Di notevole importanza è la disposizione dell'art. 16 – anch'essa tra le più delicate nella prospettiva *de iure condendo* – finalizzata a fare in modo che gli Stati membri provvedano affinché i fornitori di servizi digitali adottino (e se fossero reticenti nel farlo?) misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi del fornitore di servizi digitali con riferimento ai medesimi servizi offerti all'interno dell'Unione e al fine di assicurare la continuità degli stessi. Gli Stati membri dovranno provvedere affinché i fornitori di servizi digitali notifichino (e se fossero reticenti nel farlo?) senza indebito ritardo all'autorità competente o al CSIRT qualsiasi incidente avente un impatto rilevante sulla fornitura di un servizio digitale che essi offrono all'interno dell'Unione. Le notifiche dovranno includere, altresì, le informazioni che consentono all'autorità competente o al CSIRT di determinare la rilevanza di qualsiasi impatto transfrontaliero. Al fine di determinare se l'impatto di un

incidente sia sostanziale, dovranno essere tenuti in considerazione, in particolare, i seguenti parametri: a) il numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi; b) la durata dell'incidente; c) la diffusione geografica relativamente all'area interessata dall'incidente; d) la portata della perturbazione del funzionamento del servizio; e) la portata dell'impatto sulle attività economiche e sociali. È da notare che la direttiva prevede che l'obbligo di notificare un incidente si applichi soltanto qualora il fornitore di servizi digitali abbia accesso alle informazioni necessarie per valutare l'impatto di un incidente. Inoltre, qualora un operatore di servizi essenziali dipenda da una terza parte fornitrice di servizi digitali per la fornitura di un servizio indispensabile per il mantenimento di attività economiche e sociali fondamentali, l'operatore stesso dovrà notificare (e se fosse reticente nel farlo?) qualsiasi impatto rilevante per la continuità di servizi (essenziali) dovuto ad un incidente a carico di tale operatore. Se del caso, e, in particolare, se l'incidente avente un impatto rilevante sulla fornitura di un servizio digitale riguarda due o più Stati membri, l'autorità competente o il CSIRT informa gli altri Stati membri coinvolti. A tal fine, le autorità competenti, i CSIRT e i punti di contatto unici dovranno tutelare, nel rispetto del diritto dell'Unione o della legislazione nazionale conforme al diritto dell'Unione, la sicurezza e gli interessi commerciali del fornitore del servizio digitale, nonché la riservatezza delle informazioni fornite. Anche in questo caso, analogamente a quanto previsto dall'art. 14 per gli operatori di servizi essenziali, dopo aver consultato il fornitore di servizi digitali interessato, l'autorità competente o il CSIRT e, se del caso, le autorità o i CSIRT degli altri Stati membri interessati, potranno informare il pubblico riguardo ai singoli incidenti o chiedere al fornitore di servizi digitali di provvedervi, qualora sia necessaria la sensibilizzazione del pubblico per evitare un incidente o gestirne uno in corso o qualora la divulgazione dell'incidente sia altrimenti nell'interesse pubblico.

L'art. 17 della direttiva in esame reca disposizioni relative all'attuazione e al controllo, prevedendo, con una disposizione che non brilla certo per chiarezza, che gli Stati membri dovranno provvedere affinché le autorità competenti all'uopo individuate adottino provvedimenti, se necessario, mediante misure di vigilanza *ex post,* quando ottengono la prova che un fornitore di servizi digitali non rispetta gli obblighi di cui all'articolo 16. Tale prova potrà essere presentata dall'autorità competente di un altro Stato membro in cui è fornito il servizio. Ai fini dell'adozione delle misure di vigilanza *ex post*, ancora una volta con una disposizione che si presenta tra le più delicate nella prospettiva *de iure condendo,* la norma dispone che le autorità competenti dovranno essere dotate dei poteri (non si capisce bene di che tipo ma sembra ovvio che si debba fare riferimento a quelli di accertamento, verifica, controllo) e dei mezzi (anch'essi non definiti: sanzionatori e repressivi ai sensi dell'art. 21? Ad esempio, per quanto riguarda l'Italia, così sembrerebbe doversi procedere ai sensi dell'obiettivo operativo 6.3 del «Piano nazionale per la protezione cibernetica e la sicurezza informatica» 2017) necessari per imporre ai prestatori di servizi digitali di: a)

fornire le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza; b) rimediare a qualsiasi mancato adempimento degli obblighi di cui all'articolo 16. È altresì previsto che se un fornitore di servizi digitali ha lo stabilimento principale o un rappresentante in uno Stato membro, ma la sua rete o i suoi sistemi informativi sono ubicati in uno o più altri Stati membri, l'autorità competente dello Stato membro dello stabilimento principale o del rappresentante e le autorità competenti dei suddetti altri Stati membri dovranno cooperare e assistersi reciprocamente in funzione delle necessità. Detta assistenza e cooperazione potrà comprendere scambi di informazioni tra le autorità competenti interessate e richieste di adozione delle misure di vigilanza.

L'art. 18 della direttiva NIS reca disposizioni in tema di giurisdizione e territorialità, prevedendo che, ai fini della direttiva stessa, un fornitore di servizi digitali è considerato soggetto alla giurisdizione dello Stato membro in cui ha lo stabilimento principale e che esso è considerato avere il suo stabilimento principale in uno Stato membro quando ha la sua sede sociale in tale Stato membro. Un fornitore di servizi digitali che non è stabilito nell'Unione, ma offre servizi digitali all'interno dell'Unione, dovrà comunque designare un rappresentante nell'Unione. Il rappresentante dovrà essere stabilito in uno di quegli Stati membri in cui sono offerti i servizi e il fornitore di servizi digitali dovrà essere considerato soggetto alla giurisdizione dello Stato membro in cui è stabilito il suo rappresentante. La norma, forse per mera dimenticanza, non dispone nulla, invece, per quanto concerne gli operatori di servizi essenziali per i quali, a parere di chi scrive, la sede territoriale di erogazione del servizio determina anche la giurisdizione dello Stato membro.

Sul piano dell'attività di normazione, in una prospettiva *de iure condendo,* l'art. 19 stabilisce che, per promuovere l'attuazione convergente degli obblighi in materia di sicurezza e notifica degli incidenti (di cui agli artt. 14 e 16, rispettivamente per servizi essenziali e digitali), gli Stati membri, senza fare imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, dovranno incoraggiare l'applicazione di norme e specifiche europee e/o accettate a livello internazionale, relative alla sicurezza della rete e dei sistemi informativi. In tal senso, un ruolo fondamentale sarà svolto dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) che, in collaborazione con gli Stati membri, avrà il compito di redigere pareri e linee guida riguardanti tanto i settori tecnici da prendere in considerazione, quanto le norme già esistenti, comprese le norme nazionali degli Stati membri, che potrebbero essere applicate a tali settori.

Nel contesto così tratteggiato non poteva ovviamente mancare una norma recante disposizioni in merito al quadro sanzionatorio: all'uopo, l'art. 21 della direttiva NIS dispone che gli Stati membri dovranno stabilire norme relative alle sanzioni da irrogare ([54]) in caso di violazione delle disposizioni nazionali di attuazione della direttiva medesima e dovranno altresì adottare tutti i provvedimenti necessari per la loro

applicazione. Al riguardo, nella prospettiva *de iure condendo*, di particolare interesse sarà verificare quale sarà l'autorità nazionale prescelta e di quali poteri la stessa sarà eventualmente dotata. Le sanzioni previste dovranno essere effettive, proporzionate e dissuasive e dovranno essere notificate alla Commissione entro il 9 maggio 2018. Sul punto, giova evidenziare come la direttiva europea si sia, giustamente, solo limitata a prevedere che gli Stati debbano adottare sanzioni, non precisando la natura (amministrativa o penale) delle stesse ([55]).

L'art. 22 della direttiva dispone che la Commissione è assistita dal comitato per la sicurezza delle reti e dei sistemi informativi ai sensi del regolamento (UE) n. 182/2011. In tal senso, sarà interessante capire, all'atto del recepimento della direttiva NIS sul piano nazionale, a quale autorità sarà affidato questo importante e delicato compito.

L'art. 23 prevede che, entro il 9 maggio 2019 (quindi ad un anno di distanza dal termine ultimo di recepimento della direttiva in esame, previsto per il 9 maggio 2018), la Commissione presenti al Parlamento europeo e al Consiglio una relazione di valutazione della coerenza dell'approccio adottato dagli Stati membri nell'identificazione degli operatori di servizi essenziali ai sensi dell'art. 5 della direttiva.

L'art. 24 reca, invece, misure transitorie, prevedendo che, al fine di fornire agli Stati membri ulteriori possibilità di un'adeguata cooperazione durante il periodo di recepimento, il gruppo di cooperazione e la rete di CSIRT inizino a svolgere i compiti di cui all'articolo 11, par. 3, e all'articolo 12, par. 3, entro il 9 febbraio 2017. Per il periodo compreso tra il 9 febbraio 2017 e il 9 novembre 2018 e al fine di sostenere gli Stati membri nell'adozione di un approccio coerente nel processo di identificazione degli operatori di servizi essenziali, il gruppo di cooperazione dovrà invece esaminare la procedura, la sostanza e il tipo delle misure nazionali che consentano l'identificazione degli operatori di servizi essenziali in un settore specifico, conformemente ai criteri di cui agli articoli 5 e 6. Il gruppo di cooperazione dovrà esaminare altresì, su richiesta di uno Stato membro, specifici progetti di misure nazionali di tale Stato membro volte a consentire l'identificazione degli operatori di servizi essenziali in un settore specifico, conformemente ai criteri di cui agli artt. 5 e 6 della direttiva medesima. Entro il 9 febbraio 2017 ed ai fini della disposizione in esame, gli Stati membri avrebbero dovuto quindi assicurare un'adeguata rappresentanza in seno al gruppo di cooperazione e alla rete di CSIRT.

In questo quadro ordinamentale, l'art. 25 reca disposizioni in tema di tempistiche di recepimento della direttiva in esame prevedendo, all'uopo, che gli Stati membri debbano adottare e pubblicare, entro il 9 maggio 2018, le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla direttiva NIS e di esse dovranno informare immediatamente la Commissione.

Nella prospettiva *de iure condendo*, le modalità (strumenti normativi a monte e amministrativi a valle, ecc.) di recepimento della direttiva in esame saranno ovviamente stabilite dai singoli Stati membri. Tuttavia,

sono previsti diversi passaggi e scadenze fondamentali da rispettare per il pieno recepimento della direttiva *de qua*. In particolare, ad agosto 2017, i fornitori di servizi digitali avrebbero dovuto già adottare i requisiti minimi di sicurezza e di notifica degli incidenti. Il passaggio più importante è tuttavia quello di maggio 2018: il recepimento della direttiva NIS all'interno degli ordinamenti nazionali. A novembre dello stesso anno ogni Stato membro dovrà, poi, identificare ai sensi dell'art. 5 gli operatori di servizi essenziali. Infine, nel 2019 la Commissione europea valuterà la coerenza dell'identificazione degli operatori di servizi essenziali da parte degli Stati membri e nel 2021 verrà esaminato il funzionamento complessivo della direttiva NIS, con particolare attenzione alla cooperazione strategica e operativa degli Stati e all'applicazione della stessa da parte dei gestori di servizi essenziali e dei fornitori di servizi digitali.

In conclusione, è evidente che la direttiva NIS, una volta recepita, è destinata ad incidere su diversi soggetti; in *primis*, si può certamente affermare che essa avrà un impatto significativo su tutte le imprese che forniscono servizi essenziali e su quelle che gestiscono le infrastrutture critiche in diversi settori, tra cui energia, sanità, trasporti, banche e servizi digitali. Essa, infatti, insieme al regolamento generale per la protezione dei dati del 27 aprile 2016 (*«General Data Protection Regulation»* - GDPR - Regolamento UE 2016/679), destinato anch'esso ad entrare in vigore a maggio 2018, sarà l'asse normativo portante della politica europea sulla sicurezza informatica, in quanto stabilisce norme comuni in detto settore e mira a intensificare la cooperazione tra gli Stati dell'UE e i fornitori di servizi essenziali e digitali.

La direttiva in esame, inoltre, è di rilevante importanza, non solo per il dato normativo, ma soprattutto perché, come autorevolmente evidenziato, grazie ad essa «[…] il legittimo, necessario, direi dovuto anelito verso la ricerca, individuazione e realizzazione di una struttura di difesa unitaria in ambito europeo, è oggi molto più facilmente ed opportunamente realizzabile dando vita ad una organizzazione di difesa e contrasto unitaria, nei confronti della minaccia cibernetica, la quale, tra l'altro, costituisce oggi e in prospettiva, minaccia ben più pericolosa per la società europea e per il sistema Europa, nel suo complesso» ([56]). Essa costituisce quindi la pietra miliare della strategia europea in tema di *cyber* sicurezza, la sua attuazione da parte degli Stati membri deve avvenire sulla base di un approccio armonizzato, ad evitare disallineamenti e frammentazioni tali da compromettere gli sforzi finora dispiegati, come del resto ribadito anche nella comunicazione congiunta *«Resilience, Deterrence and Defence: Building strong cybersecurity for the EU»* JOIN(2017) 450 *final* del 13 settembre 2017. La direttiva NIS assume, inoltre, il ruolo di "linea guida" in un settore – quello della *cybersecurity* – che, da questo punto di vista, risultava ancora carente di un *framework* sovranazionale; in tal senso, la direttiva rappresenta, pertanto, una fondamentale opportunità di crescita economica, oltre che un'importante difesa da minacce sempre più presenti nella vita quotidiana dei cittadini e delle imprese europee.

Giova, infine, precisare che le disposizioni della direttiva NIS lasciano impregiudicate le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare quelle di tutela della sicurezza nazionale – comprese le misure volte a tutelare le informazioni, la cui divulgazione sia dagli Stati membri considerata contraria agli interessi essenziali della loro sicurezza – e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati.

4. Contesto giuridico nazionale di riferimento nel settore della tutela dello spazio cibernetico nelle more del recepimento della direttiva NIS

Creato il *framework* sovranazionale grazie alla direttiva NIS, la reale efficacia delle misure di sicurezza delle reti e dell'informazione dipenderà da come la stessa verrà recepita dagli Stati membri nell'ambito degli ordinamenti interni, nonché da quanto questa implementazione sarà in linea con gli obiettivi originali della direttiva ([57]). Difatti, la direttiva in esame, non rientrando nel novero delle fonti normative cosiddette a effetti diretti ([58]) o comunque *"self executing"*, necessiterà di un'ulteriore attività legislativa supplementare da parte dei singoli Stati membri, con particolare riferimento alla forma e ai mezzi necessari al raggiungimento delle finalità dalla medesima prefissate. In tal senso, quindi, la valutazione sulla bontà della stessa non potrà che passare, inevitabilmente, dal corretto recepimento che di essa faranno i singoli Stati membri e, soprattutto, dal modo in cui successivamente ogni Nazione implementerà la stessa sul piano amministrativo.

Con particolare riferimento all'Italia giova evidenziare che la tematica *cyber* è di grande attualità politica ([59]) e operativa ([60]), sebbene ancora oggi le istituzioni italiane ([61]), ma in generale anche l'industria dell'alta tecnologia e il settore privato, siano ancora lontane da un approccio sistemico e coordinato, volto ad assicurare una protezione nazionale dello spazio cibernetico. Nondimeno, sul piano giuridico interno, diverse normative, provvedimenti, direttive e *standard* sono già stati introdotti da prima dell'adozione della direttiva NIS. Al riguardo, sul piano normativo primario e secondario, si richiamano le seguenti fonti:

- il decreto legge 27 luglio 2005, n. 144 ([62]), recante «Misure urgenti per il contrasto del terrorismo internazionale», convertito con legge 31 luglio 2005, n. 155, che all'art. 7-*bis* («Sicurezza telematica»), che dispone, ferme restando le competenze dei servizi informativi e di sicurezza, che l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (Servizio di polizia postale e delle comunicazioni) assicuri i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno;
- la legge 3 agosto 2007, n. 124 ([63]), recante il «Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto», e, in particolare, gli artt. 1, 4, 38, come modificati

successivamente alle modifiche operate dalla legge 7 agosto 2012, n. 133, con i quali sono state rafforzate le attività dell'*intelligence* ([64]) nel settore *cyber;*

- il decreto del Ministero dell'interno 9 gennaio 2008 ([65]), che ha proceduto all'individuazione delle infrastrutture critiche informatizzate di interesse nazionale ai sensi e per gli effetti del citato art. 7-*bis* del decreto legge 27 luglio 2005, n. 144;
- il decreto legge 30 ottobre 2015, n. 174 ([66]), recante «Proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione», che, all'art. 7-*bis* («Disposizioni in materia di *intelligence*»), co. 5, ha attribuito al Comitato interministeriale per la sicurezza della Repubblica (CISR) compiti di deliberazione, consulenza e proposta a supporto del Presidente del Consiglio dei ministri in caso di situazioni di crisi (ad esempio cibernetica) che coinvolgono la sicurezza nazionale;
- la legge 28 dicembre 2015, n. 208, recante «Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato» (cd. legge di stabilità 2016[67]), che, all' art. 1, co. 965 e ss., ha stanziato 150 milioni di euro per il rafforzamento della sicurezza informatica nazionale ([68]);
- il decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017 ([69]), recante gli «Indirizzi per la protezione cibernetica e la sicurezza informatica nazionale», approvato dal Comitato interministeriale per la sicurezza della Repubblica (CISR) il 17 febbraio 2017, che ha sostituito il precedente decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013 ([70]).

In particolare, è ai sopracitati atti che va fatta risalire la prima vera svolta nella storia della trattazione italiana della delicata tematica della *cybersecurity,* contribuendo in maniera significativa allo sviluppo della materia e al rafforzamento del ruolo dei servizi di *intelligence* nello specifico settore. Con essi, infatti, sono stati individuati i principali organi di governo incaricati di gestire la sicurezza informatica in Italia, nonché una strategia appositamente dedicata.

Sul piano delle azioni amministrative, si vedano invece:

- l'istituzione, nell'aprile 2013, del "Tavolo tecnico *cyber*", istituito dal Dipartimento per le informazioni e la sicurezza della Repubblica (DIS) per il coordinamento interministeriale, che ha operato, sotto la guida del Comitato interministeriale per la sicurezza della Repubblica (CISR – Tecnico), quale principale sede di coordinamento interministeriale per lo sviluppo dell'architettura nazionale;

- l'istituzione, nel novembre 2013, del "Tavolo tecnico imprese" per la *partnership* pubblico-privato quale sede per avviare forme di collaborazione nel campo della *cybersecurity* con enti e società di rilevanza strategica per la sicurezza nazionale;
- l'istituzione, nel dicembre 2013, del *«Computer Emergency Response Team»* della pubblica amministrazione (CERT-PA), gestito dall'Agenzia per l'Italia Digitale (AgID);
- il «Quadro strategico nazionale per la sicurezza dello spazio cibernetico» (QSN[71]) del 27 gennaio 2014, elaborato dal "Tavolo tecnico *cyber";*
- il «Piano nazionale per la protezione cibernetica e la sicurezza informatica» (PN) del 27 gennaio 2014 ([72]), di recente sostituito dal «Piano nazionale per la protezione cibernetica e la sicurezza informatica» (PN) del 31 marzo 2017 ([73]), adottato ai sensi dell'art. 3 del citato d.P.C.M. 17 febbraio 2017, che prevedono vari livelli di indirizzi (strategici e operativi[74]);
- l'accordo di collaborazione che il DIS ha firmato con il Consorzio interuniversitario nazionale per l'informatica (CINI) nell'ottobre 2014, finalizzato allo svolgimento di attività di ricerca e sviluppo ed alla realizzazione di iniziative formative nel settore della sicurezza cibernetica;
- l'istituzione del *«Computer Emergency Response Team»* nazionale, presso il Ministero dello sviluppo economico (Mise), divenuto operativo nel novembre 2014;
- la direttiva del Presidente del Consiglio dei ministri del 1 agosto 2015 di coordinamento interministeriale, volta a rafforzare l'architettura nazionale di *cybersecurity,* così da giungere ad un rapido allineamento degli assetti difensivi *cyber* del Paese a quelli dei principali *partner* internazionali ([75]);
- con specifico riferimento al settore della difesa, di particolare rilievo è il «Libro bianco per la sicurezza internazionale e la difesa 2015» ([76]), che indica nella *cyber defence* e nell'estensione delle operazioni militari al dominio cibernetico una delle priorità strategiche e, conseguentemente, uno dei più importanti programmi di investimento futuri e la recente costituzione del «Comando interforze per le operazioni cibernetiche» (CIOC ([77]);
- con specifico riferimento al settore più generale delle Pubbliche amministrazioni, rileva la Circolare 7 marzo 2017, n. 1/2017 ([78]) dell'Agenzia per l'Italia Digitale (AgID), recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni», che ha fornito alle stesse una serie di istruzioni circa gli adempimenti richiesti al fine di contrastare le minacce che incombono sui sistemi informativi; le amministrazioni dovranno ora adeguarsi alla serie di controlli di natura tecnologica, organizzativa e procedurale descritti dalla circolare entro il 31 dicembre 2017. A tale processo si aggiungerà presto quello di predisposizione e attuazione dei piani di adeguamento

alle regole tecniche per la sicurezza ICT, previste dal «Piano Triennale per l'informatica nelle pubbliche amministrazioni», approvato dal Presidente del Consiglio dei Ministri il 31 maggio 2017;

- infine, di particolare interesse è il nuovo «Protocollo d'intenti sulla protezione dei dati personali nelle attività di sicurezza cibernetica» firmato il 6 ottobre 2017 dal presidente dell'Autorità Garante per la Protezione dei dati personali e dal direttore generale del DIS. Il documento tiene conto del «Piano nazionale per la protezione cibernetica e la sicurezza informatica» (PN) del 31 marzo 2017 e si propone di mettere a sistema e rendere più efficaci le verifiche del Garante, già previste dalla normativa vigente, in una complessiva logica di responsabilità del Comparto *intelligence* rispetto alla sua attività e di adesione alle istanze del controllo. Le verifiche del Garante completano, così, la cornice di garanzie a presidio dei trattamenti dei dati personali effettuati dagli Organismi di informazione per la sicurezza.

Inoltre, a dimostrazione dell'importanza di una strategia sinergica sul tema, anche il mondo della ricerca ha posto in essere iniziative che possono considerarsi di riferimento nello specifico settore della *cybersecurity*; tra di esse, assumono particolare importanza:

- il *«Framework Nazionale per la Cyber Security 2015»* che rappresenta uno strumento (ad adozione volontaria) di auto-analisi di una organizzazione nel settore della *cybersecurity* ([79]);
- l'*«Italian Cybersecurity Report - Controlli Essenziali di Cybersecurity 2016»* ([80]);
- la costituzione, in data 21 febbraio 2017, del Comitato nazionale per la ricerca in *cybersecurity* ([81]).

4.1 ***(Segue):*** **l'attuale architettura amministrativa nazionale nel settore della tutela dello spazio cibernetico, con particolare riferimento al ruolo dell'*intelligence***

In Italia, la tutela del *cyberspace,* soprattutto in questo delicato momento ([82]), è diventata una priorità sotto molteplici aspetti ([83]) e, in *primis,* quelli di difesa e sicurezza della Repubblica ([84]). Con particolare riferimento a detto ultimo aspetto, di assoluto rilievo è il ruolo assunto dai servizi di *intelligence* nazionali ([85]) nel settore della sicurezza delle reti e dell'informazione ([86]).

Nell'attuale struttura nazionale del settore della *cybersecurity,* il Dipartimento per le informazioni e la sicurezza della Repubblica (DIS) e le due agenzie di informazione, esterna (AISE) e interna (AISI), svolgono un ruolo fondamentale nell'ambito del sistema di informazione per la sicurezza della Repubblica, avvalendosi di strumenti, modalità e procedure stabilite dalla già citata legge n. 124 del 3 agosto 2007 ([87]). Infatti, già da tempo, nei loro rispettivi ambiti di attribuzione, le due agenzie conducono tutte le attività di ricerca ed elaborazione informativa per la protezione cibernetica e la sicurezza

informatica nazionale; il DIS, d'altro canto, ha il compito di definire le linee di azione che dovranno portare ad assicurare i necessari livelli di sicurezza dei sistemi e delle reti di interesse strategico, sia pubblici che privati, verificandone ed eliminandone le vulnerabilità, provvedendo alla trasmissione di informazioni rilevanti ai fini della *cybersecurity* alle Pubbliche amministrazioni e agli altri soggetti interessati, anche privati. Nondimeno, in attesa di dare attuazione alla direttiva NIS, anche l'architettura istituzionale-amministrativa nazionale ([88]) deve cominciare a conformarsi ai contenuti della stessa. Al riguardo, come anticipato, si è già mosso il Governo che, il 17 febbraio 2017, durante la riunione del Comitato interministeriale per la sicurezza della Repubblica (CISR), ha adottato il già citato d.P.C.M. 17 febbraio 2017, che, nel superare i contenuti del d.P.C.M. 24 gennaio 2013, ha anche comportato il conseguente adeguamento del «Piano nazionale per la protezione cibernetica e la sicurezza informatica» (PN), nella sua nuova versione del marzo 2017 ([89]), il quale individua – dando in tal senso attuazione, seppur a legislazione invariata, all'art. 7 della direttiva NIS, a mente del quale ogni Stato membro adotta una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi – gli indirizzi operativi, gli obiettivi da conseguire e le linee d'azione da porre in essere per dare concreta attuazione al «Quadro strategico nazionale per la sicurezza dello spazio cibernetico» (QSN[90]) del 27 gennaio 2014.

Nelle more del recepimento della direttiva europea NIS (il cui termine ultimo è previsto nel maggio 2018, ad eccezione di alcune specifiche scadenze temporalmente successive), il d.P.C.M. 17 febbraio 2017 ha quindi proceduto, a legislazione invariata, ad un aggiornamento della strategia sulla *cybersecurity* sulla base delle seguenti direttrici:

1. definizione, in un contesto unitario e integrato, dell'architettura istituzionale deputata alla tutela della sicurezza nazionale, relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicandone all'uopo i compiti affidati a ciascuna componente e i meccanismi e le procedure da seguire ai fini della riduzione delle vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi;
2. significativo incremento delle competenze del DIS nel settore in esame, prevedendo al riguardo che il Direttore Generale dovrà definire linee di azione di interesse generale che dovranno portare ad assicurare i necessari livelli di sicurezza dei sistemi e delle reti di interesse strategico, sia pubblici che privati, verificandone ed eliminandone le vulnerabilità;
3. rafforzamento del ruolo del CISR, che emanerà direttive con l'obiettivo di innalzare il livello della sicurezza informatica del Paese e si avvarrà, in questa attività, del supporto da parte del coordinamento interministeriale delle amministrazioni CISR (cd. CISR Tecnico) e del DIS ([91]);

4. semplificazione della catena di comando mediante la ristrutturazione dell'architettura istituzionale delle procedure di coordinamento tra i diversi soggetti che la compongono, soprattutto in situazioni di emergenza;
5. disponibilità e affidabilità delle tecnologie da autorizzare per le infrastrutture di interesse strategico;
6. infine, raccordo e costante osmosi informativa tra tutte le strutture dei Ministeri competenti in materia di *cybersecurity*.

L'intervento previsto è imperniato, da un lato, sull'affermazione del ruolo strategico del Comitato interministeriale per la sicurezza della Repubblica (CISR) nelle crisi di sicurezza nazionale e, dall'altro, sulla semplificazione e razionalizzazione della catena di comando per la risposta alle minacce cibernetiche. In tal senso, il provvedimento rafforza il ruolo stesso del CISR che è chiamato adesso ad emanare direttive con l'obiettivo di innalzare il livello della sicurezza informatica del Paese e si avvale, nello svolgimento di questa attività, del supporto e del coordinamento interministeriale del cosiddetto CISR tecnico e del DIS. A parere di chi scrive, di particolare rilievo è la previsione del nuovo d.P.C.M. sulla *cybersecurity*, che attribuisce al Direttore Generale del DIS ([92]) il compito di definire linee di azione che dovranno assicurare i necessari livelli di sicurezza dei sistemi e delle reti di interesse strategico, sia pubblici che privati, verificandone ed eliminandone le vulnerabilità; l'aver identificato nel DIS un attore unico di riferimento semplifica la comunicazione in caso di attacchi, rafforza la gestione operativa – e quindi quella dei CERT – e permette di mettere in piedi un'attività di prevenzione che, in molti casi, fa la differenza quando si parla di *cybersecurity*. Per la realizzazione di queste iniziative è, tra l'altro, previsto il coinvolgimento del mondo accademico e della ricerca, con la possibilità di avvalersi di risorse di eccellenza, così come una diffusa collaborazione con le imprese operanti nel settore della *cyber*. Con detto provvedimento, la tematica della *cybersecurity* è, quindi, accentrata in capo al predetto organo di coordinamento dei servizi di *intelligence* nazionale, aprendo così le porte a un maggiore coordinamento centrale della difesa cibernetica a livello di "Sistema-Paese" ([93]), il tutto, tra l'altro, in linea con la normativa vigente, che prevede che il comparto *intelligence* sia l'unico deputato a gestire segreti di Stato anche sul versante elettronico (la l. n. 124/2007 stabilisce che i servizi di informazione siano i soli a potersi occupare di attività d'*intelligence* in materia *cyber,* salvo intervento legislativo).

Detta previsione è da considerarsi come un grande passo in avanti. Al riguardo, non può negarsi infatti che, fino ad oggi, l'assenza di una *governance* centrale e unitaria è stata la madre di tutti i problemi per la *cybersecurity* italiana. Risolvere questo nodo gordiano è stato un primo passaggio propedeutico per affrontare, per la prima volta, il problema in modo più maturo anche in Italia e per consentire, nell'ottica

dell'ormai prossimo recepimento della direttiva NIS, una più agevole implementazione della stessa. Come evidenziato dagli analisti, con l'adozione del provvedimento in esame, «finalmente si assiste a un incardinamento istituzionale di tutte le attività riguardanti la *cybersecurity*. In pratica, si sa a chi fare riferimento, quali sono gli organismi che se ne occupano, quali sono i compiti e le procedure» ([94]): difatti, «il vero elemento di novità introdotto dal nuovo Decreto risiede nel ruolo sempre più centrale e preponderante che il Dipartimento delle informazioni per la sicurezza (DIS) acquisisce nel settore della sicurezza cibernetica, da oggi in poi vero e proprio braccio operativo sul piano strategico del Presidente del Consiglio, nonché il collante tra il CISR e l'intera pubblica amministrazione e il settore privato» ([95]).

Tra le altre novità non meno significative del d.P.C.M. 17 febbraio 2017, si segnala quella che riconduce il «Nucleo sicurezza cibernetica» (NSC[96]) all'interno del DIS (precedentemente era sotto il controllo dell'Ufficio del Consigliere militare della Presidenza del Consiglio dei ministri), con il compito di assicurare la risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale in raccordo con tutte le strutture dei diversi Ministeri coinvolti in materia, nel rispetto delle competenze attribuite dalla legge a ciascuna di esse. Il NSC può, inoltre, avvalersi, ad esempio in caso di risposta ad una crisi, del supporto di tutti i CERT previsti nel quadro strategico nazionale. Detto Nucleo – che a prima vista sembrerebbe assimilabile, almeno in base alle competenze e funzioni che dovrà esercitare, al «punto di contatto unico» previsto dall'art. 8 della direttiva NIS – tra le innumerevoli funzioni (nel campo della prevenzione e della preparazione ad eventuali situazioni di crisi cibernetica e dell'attivazione delle azioni di risposta e ripristino rispetto alle predette situazioni) avrà quella di riferire direttamente al direttore generale del DIS, per la successiva informazione al Presidente del Consiglio dei ministri e al Comitato interministeriale per la sicurezza della Repubblica (CISR). Nel modello organizzativo-funzionale delineato è prevista, inoltre, una forte integrazione con le attività dell'Agenzia per l'Italia digitale (AgID), del Dipartimento della funzione pubblica, del Ministero dello sviluppo economico, del Ministero dell'interno, del Ministero della difesa e del Ministero dell'economia e delle finanze.

Altri punti qualificanti del decreto sono costituiti dall'introduzione di meccanismi di certificazione della sicurezza e dallo sviluppo di tecnologie nazionali, in modo da accrescere l'affidabilità delle reti e dei sistemi utilizzati per funzioni di interesse strategico. Ulteriore aspetto qualificante del provvedimento in questione è anche il pieno coinvolgimento degli operatori privati titolari di infrastrutture critiche nell'attuazione delle politiche di sicurezza informatica.

In conclusione, giova evidenziare che lo sforzo compiuto dal Governo con l'adozione del decreto in argomento costituisce solo il punto di partenza della nuova architettura istituzionale di cui si dovrà dotare il Paese nel settore *cyber*. Infatti, il nuovo assetto introdotto dal provvedimento in parola dovrà essere, verosimilmente, rivisitato, rafforzato e messo a sistema dal punto di vista normativo con la legge di

recepimento della direttiva NIS, magari novellando e ampliando il raggio di azione della l. n. 124/2007. Nondimeno, in vista del recepimento della direttiva NIS, tra l'altro espressamente citata nelle premesse del provvedimento *de quo*, lo stesso tiene già conto di alcune delle principali indicazioni scaturenti dalla medesima (si pensi, ad esempio, al concetto di individuazione di un'unica Autorità nazionale competente introdotto dall'art. 8 della direttiva europea, che in questo caso sembrerebbe rinvenirsi nel DIS) e va nella direzione di dare una risposta sempre più coordinata ed efficace alle minacce cibernetiche rilevanti per la sicurezza nazionale, confermando l'assoluta necessità della collaborazione pubblico-privato come base per ogni azione di rafforzamento della *cybersecurity* nazionale, nonché l'importanza del coinvolgimento dei centri di ricerca accademici per far fronte al naturale, incessante, sopravvenire di nuove tecnologie e alle modalità di utilizzo di reti e sistemi che possano generare minacce sempre più sofisticate.

All'uopo, volendo un po' anticipare il futuro, non sembra possa essere messo in dubbio che, nella prospettiva *de iure condendo*, tutte le articolazioni pubbliche competenti per la *cybersecurity* nazionale saranno impegnate sotto il coordinamento del DIS (anche al fine di evitare inutili duplicazioni dei costi, facilitare lo scambio di informazioni e velocizzare i tempi di realizzazione) nella permanente ricerca di misure adeguate in un contesto coordinato di scambio di informazioni ed esperienze per consentire la messa a punto di tecnologie nazionali al servizio della sicurezza nazionale e, quindi, dell'intera comunità. In merito a detto ultimo aspetto, tra l'altro, non può non evidenziarsi come sia necessario aumentare la consapevolezza sulla necessità (oramai irrinunciabile) di dotarsi di tecnologie sviluppate ([97]), prodotte e controllate in ambito nazionale, almeno per quanto riguarda gli utilizzi in ambito di infrastrutture critiche, enti governativi e pubblica amministrazione, applicando magari lo stesso criterio già in essere per la ricerca ([98]) e le tecnologie militari. Difatti, solo in questo modo si può garantire lo sviluppo e l'evoluzione di competenze *cyber* di alto livello, sia in ambito scientifico che in quello industriale e soprattutto un maggior livello di sicurezza dello spazio cibernetico a tutela del "Sistema-Paese". Il tutto, a sommesso parere di chi scrive, non potrà che avvenire con il coinvolgimento delle aziende italiane ([99]). Occorre, pertanto, strutturare solide *partnership* tenendo a mente principalmente il reale ed altissimo valore economico e militare di questo settore. All'uopo sarà fondamentale sviluppare "tecnologie sovrane" che possano rappresentare un vantaggio tecnologico e geopolitico per il "Sistema-Paese" ([100]) per non dipendere da "variabili esterne" che nella realtà complessa odierna potrebbero rappresentare un sostanziale svantaggio in questo specifico settore. A tale ultimo riguardo, a sommesso avviso di chi scrive, sul piano amministrativo, e nell'ottica "Sistema-Paese", manca un tassello fondamentale in questo delicato settore; in tal senso sarebbe infatti auspicabile l'istituzione di una cd. "cabina di regia *cyber*" nazionale permanente (tra l'altro ciò sarebbe anche in linea con il citato PN del 31 marzo 2017, in particolar modo con gli indirizzi operativi n. 2 e 8 concernenti in termini generali il coordinamento e lo sviluppo tecnologico

nazionale) tesa al rafforzamento della cooperazione pubblico-privato in tema di *cybersecurity* al fine di sviluppare, in ambito nazionale, tecnologie *cyber* utili alla sicurezza interna, e d'indirizzare (*rectius:* guidare) nello specifico settore *de quo* non solo il mondo industriale ma anche quello accademico e della ricerca in generale. Al riguardo, infatti, non può sottacersi che in ambito nazionale, almeno ad oggi, per ciò che riguarda la *cybersecurity* esistono forti carenze di dialogo sia all'interno del settore pubblico sia tra quest'ultimo e quello privato. All'uopo, l'istituzione di una "cabina di regia *cyber*" nazionale permanente, tesa a garantire idonei *standard* di sicurezza e linee strategiche condivise, da un lato potrebbe consentire alle istituzioni nazionali di avviare un dialogo virtuoso nell'ottica della condivisione di strategie e sistemi *cyber* comuni; dall'altro consentirebbe alle aziende italiane, nell'ambito della suddetta auspicata "cabina di regia" nazionale, di rivolgersi alle istituzioni pubbliche prospettando lo sviluppo di determinate tecnologie *cyber* basate su attività di ricerca condotte esclusivamente in ambito nazionale che, se ritenute valide in termini di sicurezza e affidabilità complessiva, potrebbero poi essere acquisite dalle istituzioni previo avvio di percorsi di ricerca che includano il mondo accademico, quello industriale e quello pubblico ([101]). Ma ben potrebbe accadere l'inverso, ossia che l'amministrazione pubblica (si pensi ad esempio alla difesa) necessiti di una determinata tecnologica (ad esempio necessaria a garantire l'operatività di un sistema d'arma ovvero di un sistema di sistemi nel dominio cibernetico) e si rivolga, seppur sempre in ambito nazionale, all'esterno (industria, accademia, ecc.) per avviare attività di ricerca e successivo sviluppo capacitivo di soluzioni atte a garantire alti *standard* tecnologici di *cybersecurity* evitando, al contempo, di fare ricorso a mercati esteri che (in ipotesi, ma non solo…) potrebbero non garantire lo stesso livello di sicurezza.

5. Recepimento in ambito nazionale della direttiva NIS: possibili aspetti critici e riflessioni *de iure condendo*

Come evidenziato, allo stato attuale, la maggior parte delle amministrazioni pubbliche e delle infrastrutture critiche sono ancora in ritardo nell'adozione di un modello condiviso di *cybersecurity* nazionale. Ciò in quanto, seppur tutte le normative e gli atti amministrativi citati hanno indicato una strategia ([102]) da seguire, mancano ancora dei regolamenti tecnici o di auto-disciplina che consentano di uniformare le aspettative e le necessità in materia di *cybersecurity* nazionale. Analogamente dicasi per lo scambio informativo sugli incidenti subiti e sulle tecniche di risposta, che risultano ancora attuati a singhiozzo e comunque solo in alcuni ambiti/settori (per l'amministrazione pubblica attraverso il CERT-PA ovvero il CERT nazionale ([103]), attraverso convenzioni ed accordi *ad-hoc*). Invero, almeno sino ad oggi, alla base dei principali problemi dell'infrastruttura di sicurezza nazionale sotto il profilo *cyber*, vi sono stati una modesta capacità di condivisione delle informazioni in ambito nazionale e soprattutto con altri

Stati, lo scarso coinvolgimento del cittadino e la conseguente assenza di una consapevolezza della minaccia cibernetica del sistema Italia e, non ultimo, la citata scarsa collaborazione tra attori privati e istituzioni per la salvaguardia del patrimonio informativo nazionale; tutte lacune, queste, che, a seguito del recepimento della direttiva NIS, dovranno essere, invece, auspicabilmente (*rectius:* necessariamente) colmate. Inoltre, molte organizzazioni pubbliche e private non hanno ancora maturato una sensibilità (*rectius:* cultura) specifica sull'effettiva necessità di contribuire attivamente alla *cybersecurity* nazionale, non essendo, tra l'altro, almeno fino ad oggi, obbligati nel concreto a farlo. Infine, un capitolo a parte meriterebbe la questione degli investimenti nel settore *cyber*, che differiscono sensibilmente da soggetto a soggetto e questo non facilita il raggiungimento di un livello di sicurezza omogeneo all'interno del *cyberspace*.

Nell'imminenza del recepimento della direttiva NIS, pertanto, il risultato è una protezione ancora poco efficace dal punto di vista nazionale e fortemente dipendente dalla capacità dei singoli (istituzioni, organizzazioni, aziende, privati, ecc.) di rendere sicura la loro porzione di *cyberspace*. Fino a qualche tempo addietro, ciò che è emerso nel dibattito italiano è, da un lato, la mancanza di una riflessione strutturata – in ottica evolutiva – finalizzata a veicolare una vera e propria politica di *cybersecurity* nazionale, la quale, peraltro, risulta ancora oggi priva di alcuni pilastri normativi imprescindibili (come, ad esempio, una definizione di sicurezza nazionale, nel cui alveo deve necessariamente essere ricompresa gran parte della tematica della sicurezza dello spazio cibernetico[104]); dall'altro lato, invece, emerge oggi con forza la necessità che in questo settore gli attori istituzionali italiani cambino l'approccio strategico da meramente difensivo (ovvero di semplice gestione di eventuali crisi, di prevenzione degli attacchi informatici e di riduzione dei loro danni) a proattivo, finalizzato, quindi, a prevedere e anticipare le tendenze e i mutamenti futuri di questo settore per pianificarne in tempo le opportune azioni e strategie ([105]).

In questa cornice generale, nella prospettiva *de iure condendo*, il recepimento della direttiva NIS in ambito nazionale dovrebbe pertanto consentire, in primo luogo, di arrivare all'adozione di un *framework* giuridico nazionale di *cyber defence* che possa, da un lato, uniformare le capacità richieste dai CERT e, dall'altro, favorire il coordinamento tra attori pubblici e privati con innegabili vantaggi, tra i quali maggiore fiducia tra gli operatori, migliore capacità di deterrenza e prevenzione, migliore capacità di reazione, contributo alla *"situational awareness"* nazionale, *"baseline"* di protezione e maggiore competitività in ambito internazionale.

La direttiva NIS, pertanto, seppur non coglie l'Italia del tutto impreparata per un recepimento in linea con i suoi contenuti, introduce la necessità di operare qualche aggiustamento dell'attuale architettura normativa-istituzionale – in tal senso un primo importante passo, che indubbiamente non può ancora bastare, è stato compiuto con l'adozione del citato d.P.C.M. 17 febbraio 2017 (sul quale v. *supra*) – e può

rappresentare, per il Paese, un'occasione da non perdere per fare un salto in avanti deciso, proponendosi come mercato all'avanguardia in quanto a *standard* e politiche per la sicurezza IT. Sulla base di tali ordini di considerazioni, non può sottacersi che gran parte della partita si giocherà sul come la direttiva in rassegna verrà recepita sul piano giuridico ([106]) e da quanto l'attuazione, anche sul piano amministrativo (ad esempio mediante l'istituzione dell'auspicata "cabina di regia *cyber*" di cui si è detto), sarà in linea con gli obiettivi originali della medesima. *De iure condito,* occorrerà quindi valutare se il recepimento della stessa sul piano del diritto interno – inutile nascondere che per quel che riguarda l'Italia il problema è di grande attualità, richiedendo interventi normativi non più procrastinabili ([107]) – si limiterà ad un mero recepimento formale (ad esempio ricalcando di fatto per grandi linee quanto previsto dalla direttiva) oppure andrà ad impattare – come sarebbe opportuno – sui gangli del sistema nazionale di *cybersecurity,* rimodulando l'intera architettura degli apparati amministrativi esistenti, riallocandone le funzioni ([108]), modificando le strutture organizzative (individuando pertanto la o le Autorità nazionali competenti in materia di sicurezza delle reti e dei sistemi informativi, designando il punto di contatto unico nazionale in materia di sicurezza delle reti e dei sistemi informativi nonché uno o più CSIRT che si occupino almeno dei settori e dei servizi identificati come essenziali e abbiano il compito di trattare gli incidenti e i rischi secondo una procedura ben definita[109]), nonché rivedendo le procedure tecnico-amministrative attualmente in vigore e che già disciplinano, magari in modo non organico, la materia *de qua*, verosimilmente introducendo anche severe norme sanzionatorie laddove necessario. In tal senso, consapevole dell'importanza di detto passaggio legislativo, anche il «Piano nazionale per la protezione cibernetica e la sicurezza informatica 2017» (PN) indica, all'obiettivo operativo 6.2, la necessità di «individuare, alla luce del contesto normativo dell'Unione europea e internazionale di riferimento, la disciplina giuridica nazionale atta a regolamentare – in una logica di anticipazione dei presìdi – le attività di sicurezza in materia *cyber*, incluse le operazioni cibernetiche» e, all'obiettivo operativo 6.3, la necessità di «elaborare un quadro legale ed una metodologia di riferimento al fine di identificare gli strumenti tecnici, inclusi quelli relativi all'indirizzamento, necessari all'attribuzione di responsabilità in caso di violazioni di sicurezza (e delle relative sanzioni) da parte di amministratori ed utenti delle reti di interesse». Rispetto al primo dei due profili da ultimo evocati, ad esempio, un aspetto di grande rilievo, nell'ottica del recepimento della direttiva europea, sarà certamente quello della corretta individuazione dei servizi essenziali e della relativa emanazione degli obblighi in materia di sicurezza nei riguardi degli operatori di tali servizi, ivi comprese le preventive analisi del rischio e la notifica degli incidenti subiti. Infatti, come messo in evidenza, una delle prescrizioni più significative delle nuove norme previste dalla direttiva NIS sono gli obblighi di sicurezza e di notifica degli incidenti per gli operatori di servizi essenziali e delle infrastrutture critiche. Ne consegue, quindi, che, sulla base di come l'Italia deciderà di definire i fornitori

di servizi essenziali, ovvero (con le opportune modifiche al d.M. del Ministero dell'interno 9 gennaio 2008) quelli che gestiscono le infrastrutture critiche nazionali, potrebbe misurarsi l'efficacia della strategia governativa complessiva. Il legislatore, ad esempio, potrebbe orientarsi sull'obbligo di notifica degli attacchi soltanto per i grandi *players* aziendali e industriali di carattere nazionale oppure – scelta da non escludere *a priori* – potrebbe prevedere un medesimo obbligo anche per realtà più piccole, ma che magari contano su un ampio numero di utenti e il cui contributo su scala nazionale potrebbe quindi essere ugualmente significativo; ovvero ancora potrebbe ricomprendere, o meno, nell'ambito di applicazione del suddetto obbligo, anche la pubblica amministrazione, infatti nonostante la stessa non sia espressamente compresa nell'ambito di applicazione della direttiva NIS (benché, come detto, lo sia certamente quale soggetto garante dell'intera architettura istituzionale che dovrà essere definitiva in attuazione della direttiva NIS), nondimeno gli Stati membri hanno la possibilità di estendere il raggio d'azione della stessa, e quindi applicarne le regole, in termini di requisiti di sicurezza e obblighi di notifica, anche a settori da essa non direttamente disciplinati (qual è quello pubblico), laddove l'amministrazione eroghi servizi essenziali. Inoltre, gli operatori di servizi essenziali e i fornitori di servizi digitali dovrebbero essere incoraggiati ad adottare piattaforme comuni interoperabili come STIX per la condivisione delle informazioni di *cyber intelligence*, o acquisire competenze critiche come il *"Middlebox Security Protocol"* per gestire le crescenti sfide del traffico criptato.

Altrettanto rilievo avrà, ad esempio, l'implementazione dei meccanismi che consentiranno la cooperazione operativa rapida ed efficace mediante la rete di cooperazione (cd. *"Cooperation network"*). Su questo aspetto, l'Italia è già ben indirizzata, almeno da un punto di vista normativo, grazie all'istituzione del CERT nazionale e all'adozione del già citato «Quadro Strategico nazionale per la sicurezza dello spazio cibernetico 2014» (QSN) che verosimilmente andrà comunque rivisto in ottica *de iure condendo*. A tale specifico riguardo, l'implementazione del CERT europeo e dei processi europei di *"incident notification and responding"* potrebbe valorizzare il ruolo chiave del CERT nazionale italiano, come potenziale centro prioritario di raccoglimento e dispacciamento delle principali informazioni sia di carattere preventivo (*"information sharing"*) che reattivo (*"incident notification"*). Tale ruolo, tra l'altro, gioverebbe non poco alla razionalizzazione della rete dei CERT italiani (nazionale, pubbliche amministrazioni, difesa, etc.), in termini sia di semplificazione sia di velocizzazione dei flussi informativi e decisionali.

Last but not least, ulteriore e non meno significativo aspetto che in prospettiva *de iure condendo* non potrà essere sottovalutato dal legislatore, al fine di non vanificare l'intero assetto normativo e regolamentare *de iure condito*, sarà quello concernente l'autorità nazionale prescelta per vigilare sulla corretta attuazione della normativa interna di recepimento (al riguardo, se si pone mente al concetto di individuazione di un'unica autorità nazionale competente[110] introdotto dall'art. 8 della direttiva NIS, detta autorità sembrerebbe –

ma il condizionale è d'obbligo – potersi verosimilmente rinvenire nella Presidenza del Consiglio dei Ministri: DIS?), e di quali poteri (di vigilanza, di accertamento e di coercizione, se del caso definendo un adeguato regime sanzionatorio da applicarsi in caso di inadempienza da parte dei soggetti obbligati) la stessa sarà eventualmente dotata e, soprattutto, se la scelta di attribuire detti poteri ad una determinata autorità nazionale sia ontologicamente in linea con l'esercizio delle funzioni cui la stessa è istituzionalmente preposta.

Infine, occorre soggiungere che, risalendo al piano sovranazionale, altrettanto importante sarà l'esame dei mezzi e delle modalità con le quali l'UE intenderà gestire questo nuovo ruolo di indirizzo e attribuzione di chiare e trasparenti responsabilità tra tutti i soggetti coinvolti nella tutela e sicurezza del *cyberspace*. Sfida, quest'ultima, che non si presenta certamente come una delle più semplici anche alla luce della contestuale implementazione che l'Unione dovrà dare alla *«Joint Declaration»* tra NATO e UE del 6 dicembre 2016 e alla *«Permanent Structured Cooperation on security and defence»* (PeSCo) del 13 novembre 2017 – entrambe, come evidenziato ([111]), destinate ad incidere pesantemente anche nel settore della *cybersecurity and defence,* seppur limitatamente allo specifico ambito militare della difesa – il cui impatto richiederà un'irrinunciabile opera di raccordo tra le strategie di *cybersecurity* per la protezione delle infrastrutture critiche ad uso civile e quelle per la protezione delle infrastrutture di comando e controllo ad uso militare, anche al fine di sviluppare una complessiva architettura cibernetica che sia sicura e, in ipotesi, anche in grado di collegare le infrastrutture militari europee a quelle dei singoli Stati membri, stabilendo protocolli di sicurezza condivisi e destinati a garantire le comunicazioni criptate e le capacità di difesa *cyber* anche per le attività militari.

Note di chiusura

([1]) A. EINSTEIN.

([2]) Un'interessante definizione di spazio cibernetico si rinviene, già diversi anni addietro, nel *White House, The National strategy to secure cyberspace,* 2003, p. IX, nel quale esso viene definito come «Il sistema nervoso del Paese […] composto da centinaia di migliaia di *computer, server, router* e fibre ottiche tra loro interconnessi e che permettono alle infrastrutture critiche di essere operative». A ben vedere, lo *United States Department of Defense* (*DoD*) è stato il soggetto che più ha riconosciuto il *cyberspace* come nuovo e rilevante dominio verso cui indirizzare le proprie attività. Ad esempio, già nel 2006, grazie al *Chairman* del *Joint Chiefs of Staff* (Generale P. PACE), il Dipartimento di Difesa americano ha approvato un documento che ha sancito la necessità di sviluppare una strategia militare nazionale per le operazioni nello spazio cibernetico, al riguardo definito come «[…] un dominio caratterizzato dall'uso di sistemi elettronici per immagazzinare, modificare e scambiare informazioni attraverso sistemi interconnessi e strutture fisiche», dal *Chairman of the Joint Chiefs of Staff, Department of Defense, The National Military Strategy for Cyberspace Operations,* 2003, *Washington DC,* p. 8. Nell'edizione 2015 del *«The department of defense cyber strategy»* è stata altresì stabilita una *cyber-strategy* che poggia su tre pilastri fondamentali: *«The Defense Department has three primary cyber missions. First, DoD must defend its own networks, systems, and information* [...]. *For its second mission, DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence* [...]. *Third, if directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans».* In particolare, riguardo la predetta seconda missione, di recente, la *Defense Department Science Board's Task Force on Cyber Deterrence* ha pubblicato un importante *report* che evidenzia quali siano, per il futuro, le tre sfide essenziali per la deterrenza nel *cyberspace*, individuandole nelle seguenti: *«First, major powers (Russia and China) have a significant and*

growing ability to hold U.S. critical infrastructure at risk via cyber-attack, and an increasing potential to also use cyber to thwart U.S. military responses to any such attacks. This emerging situation threatens to place the United States in an untenable strategic position. […]. *Second, regional powers (such as Iran and North Korea) have a growing potential to use indigenous or purchased cyber tools to conduct catastrophic attacks on U.S. critical infrastructure. The U.S. Government must work with the private sector to intensify efforts to defend and boost the cyber resilience of U.S. critical infrastructure in order to avoid allowing extensive vulnerability to these nations.* […]. *Third, a range of state and non-state actors have the capacity for persistent cyber-attacks and costly cyber intrusions against the United States, which individually may be inconsequential (or be only one element of a broader campaign) but which cumulatively subject the Nation to a "death by 1,000 hacks". To address these challenges, bolstering the U.S. cyber deterrence posture must be an urgent priority. The DoD and the Nation should pursue three broad sets of initiatives to bolster deterrence of the most important cyber threats and related challenges to the United States»,* in *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence on February 23, 2017*. Per approfondimenti sulle armi cibernetiche, sulle potenze cibernetiche e sulle operazioni militari nello spazio cibernetico di Cina e Russia, v. G. CUSCITO, *La rete degli spiriti che "difende"* Internet *in Cina,* in *Limes - A che servono i servizi,* n. 7/2014, p. 147, G. GIACOMELLO, *Geopolitica delle armi autonome,* in *Limes - Chi comanda il mondo. Autonomia dei poteri invisibili nel nuovo disordine mondiale. I quattro sfidanti dell'impero USA,* n. 2/2017, pp. 253 – 260 e ancora v. D. DENNING, *How the Chinese cyberthreat has evolved,* in *http://fifthdomain.com,* 9 ottobre 2017. Sul punto giova soggiungere che mentre in Occidente il *cyberspace* è visto come qualcosa che può essere sfruttato a vantaggio dello spionaggio, del sabotaggio e delle distorsioni di vario genere, nei regimi autocratici, invece, come Cina e Russia, il *cyberspace* è uno strumento per il controllo politico generalizzato. In tal senso, *Russia e Cina hanno un approccio totalmente differente*, per loro lo spazio cibernetico s*ignifica controllo nel processo di produzione ma anche di informazione. T*ra l'altro, di recente la Cina ha annunciato che creerà un *database* nazionale di dati per immagazzinare le informazioni sugli attacchi informatici. All'uopo, il Ministero dell'Industria e della Tecnologia dell'Informazione (MIIT) cinese ha dichiarato che compagnie private ed enti governativi dovranno condividere informazioni riguardanti, tra gli altri, gli incidenti, i *malware* e le vulnerabilità *hardware,* prevedendo, per chi non rispetterà tali regole, multe e altre sanzioni amministrative. La nuova misura si inquadra nella serie di misure intraprese dalle autorità di Pechino (da ultimo si veda la nuova legge sulla *cybersecurity*) volte a proteggere le infrastrutture critiche e i settori pubblico e privato contro gli attacchi informatici su vasta scala. Invece, sulle specifiche capacità militari della Russia nel settore cibernetico, v. R.C. MANESS, B. VALERIANO, *Russia's Coercitive Diplomacy: energy, cyber, and marittime policy as new sources of power,* Bashingstoke 2015, v. D. DENNING, *Tracing the sources of today's Russian cyberthreat,* in *http://fifthdomain.com,* 17 agosto 2017, v. P. MASTROLILLI, *Kaspersky era il Cavallo di Troia degli hacker russi negli Stati Uniti*, in *La stampa*, 12 ottobre 2017 (inchiesta dalla quale emergerebbe che l'*intelligence* israeliana avrebbe scoperto che la Russia usava gli antivirus per spiare gli USA), v. A. F. RASMUSSEN, *Ecco perché la Russia preoccupa la Nato (anche) nel* cyber *spazio,* in *www.cyberaffairs.it, 14 ottobre 2017,* e, con particolare riferimento alla capacità dei servizi di *intelligence* russi di dirottare i segnali satellitari per lanciare attacchi informatici (l'utilizzo attivo e passivo della tecnologia satellitare per comandare a distanza i computer, danneggiando i dispositivi *target*, è stato pubblicamente dimostrato nel 2015), v. *La Russia è in grado di sfruttare segnali satellitari per lanciare* cyber *attacchi?* in *www.analisidifesa.it,* 6 agosto 2017 e M. SPAGNULO, *Internet su satelliti a prova di* hacker, in *www.cyberaffairs.it, 14 ottobre 2017*. Per dette ragioni gli Stati Uniti cercano sempre più insistentemente *partner* per affrontare tali nuove impegnative sfide in ambito cibernetico, per approfondimenti v. anche *US seeks stronger international cyber defense partnerships,* in *http://fifthdomain.com,* 14 giugno 2017. Alcuni analisti aggiungono anche altri due Stati dai quali gli USA devono guardarsi nel settore *cyber,* ossia Iran e Corea del Nord, v. M. POMERLEAU, *America's top 4 cyberspace foes,* in *http://fifthdomain.com,* 16 agosto 2017 (sulla pericolosità della Corea del Nord, da ultimo v. anche*, South Korean lawmaker says North Korea hacked war plans,* in *http://fifthdomain.com,* 10 ottobre 2017 e v. *Perché il* cyber *esercito della Corea del Nord dovrebbe preoccuparci tutti*, in *cyberaffairs.it*, 21 ottobre 2017). In particolare, nel 2014 diverse agenzie di *intelligence* hanno rilevato che il Governo di Pyongyang stava investendo in maniera significativa nell'incremento delle sue capacità *cyber*, per questo obiettivo il numero di *hackers* operanti nelle file dell'esercito nazionale fu raddoppiato; infatti già nel 2011, immagini satellitari in possesso dell'*intelligence* americana rivelarono l'esistenza del *"North Korea's 'No. 91 Office"*, un'unità speciale di *hacking* collocata nel distretto di Mangkyungdae nella città di Pyongyang (per approfondimenti v. P. PAGANINI, *Cyber war, perché arriva dalla Corea del Nord il vero pericolo,* in *www.agendadigitale.ue*). Inoltre alcuni analisti hanno rilevato come *hackers,* che si ritiene siano legati al governo iraniano, hanno colpito imprese aerospaziali e petrolchimiche saudite ed occidentali, segnando un aumento dell'abilità di Teheran nel *cyber* spionaggio. Il gruppo soprannominato *"Hacker APT33"* avrebbe avviato la sua attività a partire dal 2013, quando sono emersi diversi suoi tentativi di rubare segreti militari e del settore

dell'aviazione, mentre nel frattempo si preparava a lanciare attacchi che avrebbero potuto paralizzare intere reti di *computer*.

([3]) In tal senso, v. il quadro strategico dell'UE in materia di *cyber*-difesa [*Consilium* 15585/14] e la comunicazione congiunta «*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*», *(JOIN(2013)1),* 7 *February* 2013.

([4]) Come «Industria 4.0», espressione collegata alla cosiddetta "quarta rivoluzione industriale". Questa nuova rivoluzione industriale, resa possibile dalla disponibilità di sensori e di connessioni *wireless* a basso costo, si associa a un impiego sempre più pervasivo di dati e informazioni, di tecnologie computazionali e di analisi dei dati, di nuovi materiali, componenti e sistemi totalmente digitalizzati e connessi (*"internet of things and machines"*). «Industria 4.0» richiede soluzioni tecnologiche per ottimizzare i processi produttivi, supportare i processi di automazione industriale, favorire la collaborazione produttiva tra imprese attraverso tecniche avanzate di pianificazione distribuita, gestione integrata della logistica in rete e interoperabilità dei sistemi informativi. In detto contesto di cd. *"digital transformation"*, i nuovi processi produttivi si basano in particolare su tecnologie di produzione di prodotti realizzati con nuovi materiali, meccatronica, robotica, utilizzo di tecnologie ICT avanzate per la virtualizzazione dei processi di trasformazione e sistemi per la valorizzazione delle persone nelle fabbriche. Al riguardo, i principali paesi industrializzati si sono già attivati a supporto dei settori industriali nazionali in modo da cogliere appieno le opportunità offerte da «Industria 4.0». L'Italia, ad esempio, ha sviluppato un «Piano nazionale Industria 4.0, 2017-2020», che prevede misure concrete in base a tre principali linee guida: operare in una logica di neutralità tecnologica; intervenire con azioni orizzontali e non verticali o settoriali; agire su fattori abilitanti. Le direttrici strategiche sono quattro: investimenti innovativi; infrastrutture abilitanti; competenze e ricerca; *awareness* e *governance.* Con particolare riferimento al rapporto tra «Industria 4.0» e *cybersecurity,* v. *Industry* 4.0: come cambia la *cyber* sicurezza dei *robot* industriali, v. *www.cyberaffairs.it, 17 giugno 2017*.

([5]) A carattere generale, occorre evidenziare che il rischio di *cyber attack* è strettamente correlato al livello di dipendenza di ogni singolo Stato dalla *Information and Communication Technology* (ICT). Si pensi, ad esempio, agli Stati Uniti, che hanno una dipendenza dall'ICT ancora più marcata dell'Europa e nei quali la sicurezza delle reti informatiche è ormai diventata una *"top priority"*, al punto che il precedente Presidente degli USA, Obama, era giunto a dichiarare che le infrastrutture digitali sono un assetto strategico nazionale e la loro difesa è una priorità della sicurezza nazionale, in *White House, National Security Strategy,* maggio 2010, p. 27. Ciò, peraltro, si raccorda perfettamente con la proposta di finanziamento per il 2017 che il Pentagono ha formulato agli inizi del 2016. Solo per il settore della *cybersecurity,* infatti, la richiesta è stata di 7 miliardi di dollari (circa un miliardo in più rispetto alle richieste per il 2016) e di 35 miliardi di dollari per i prossimi 5 anni, da destinare alla protezione delle infrastrutture militari, ma anche – si legge esplicitamente nella richiesta – per accelerare lo sviluppo delle capacità offensive nel/attraverso il *cyber*-spazio. A questa richiesta, d'altra parte, ha fatto da eco la Casa Bianca attraverso il suo *«Cyber security National Action Plan»,* del febbraio 2016, un documento strategico teso a potenziare le capacità e soprattutto la solidità in materia di sicurezza informatica del governo federale e di tutto il Paese attraverso specifiche azioni di breve e di medio-lungo periodo. Le principali direttrici su cui si muove il "Piano", infatti, vanno da un'ampia riorganizzazione a un maggiore coordinamento centrale delle attività federali in materia di sicurezza informatica e *privacy*. Per l'attuazione di questo *"Action Plan",* prima del temine del suo mandato, il Presidente Obama ha richiesto, per il 2017, un finanziamento di ben 19 miliardi di dollari, incrementando così del 35%, rispetto a quanto previsto, il *budget* per la *cybersecurity*. Ma, a ben vedere, anche l'amministrazione Trump sta puntando fortemente sul settore *cyber*. In tal senso, la prima proposta di *budget* federale presentata dal neopresidente degli Stati Uniti prevede 1,5 miliardi di dollari per il *Department of Homeland Security (DHS)* per proteggere le reti nazionali e le infrastrutture critiche da attacchi informatici. La richiesta di bilancio aumenta gli stanziamenti al DHS del 6,8 %, mentre riduce fortemente i contributi ad altre agenzie e dipartimenti e richiede anche una maggiore cooperazione tra il governo e il settore privato sulla sicurezza cibernetica. Uno dei consiglieri della Casa Bianca, Tom Bossert, *advisor* sui temi della sicurezza nazionale e del contrasto al terrorismo, ha ribadito che l'amministrazione Trump darà priorità alla *cybersecurity,* richiedendo ai dipartimenti e alle agenzie di attuare un quadro di sicurezza informatica federale e di sviluppare sistemi che mostrino i loro progressi. Al riguardo, un primo importante segnale è stato il prolungamento dell'emergenza nazionale dichiarata l'1 aprile del 2015 dal Presidente Obama per ciò che concerne le *cyber* minacce di derivazione straniera (nell'aprile del 2015, infatti, Obama firmò un *executive order* che consentiva al governo di congelare i beni di chiunque fosse stato scoperto a condurre attività di *hacking* che minacciassero la sicurezza nazionale. A dicembre del 2016, poi, il Presidente uscente siglò un nuovo *executive order* che modificava il primo, aggiungendovi la possibilità di congelare anche gli *asset* di chi conduce azioni di pirateria informatica per interferire nelle elezioni). Detta decisione, comunicata con il *«Message to the Congress regarding the Continuation of the National*

Emergency with Respect to Significant Malicious Cyber-Enabled Activities», scaturisce dal presupposto che significative e dannose attività *cyber* originate o dirette da persone situate in *toto* o in grossa parte fuori dagli Stati Uniti continuano a rappresentare una minaccia insolita e straordinaria per la sicurezza nazionale, la politica estera e l'economia degli USA. La nuova amministrazione statunitense, pertanto, ha deciso di prolungare l'emergenza nazionale dichiarata nell'*executive order* n. 13694, con riferimento a significative e dannose attività *cyber,* al di là dell'1 aprile 2017. E ancora, tra le novità del *budget* per l'anno fiscale 2018, c'è anche un forte aumento dei fondi (+10% circa) destinati al Dipartimento della Difesa americano, in parte volto a migliorare le operazioni e le difese informatiche delle Forze Armate statunitensi. Per approfondimenti su detti temi, v. *Government procurement under Trump could offer incentives to boost cyber solutions,* secondo il quale *«The Trump administration is expected to incentivize cybersecurity companies to collaborate on interoperable software that boosts security of the overall ecosystem, according to a technology industry leader and former government IT security compliance official»* e, ancora, *Trump budget request boosts DHS activities for securing federal data, sharing cyber-threat info,* entrambi in *www.insideCybersecurity.com*, 17 marzo 2017. È evidente che interventi così decisi da parte della Casa Bianca sono il frutto dei numerosi incidenti informatici occorsi proprio ai sistemi della pubblica amministrazione americana durante il 2015 (primo fra tutti, ad esempio, l'attacco all'*Office of Personnel Management*) e il 2016 (violazioni ai danni dei dipendenti del *Department of Homeland Security* e del *Federal Bureau of Investigation - FBI*). Per approfondimenti sul piano d'azione americano v. S. MELE, *Cyber Strategy & Policy Brief,* Volume 02 – Febbraio 2016 (p. 9), v. M. POMERLEAU, *DoD still doesn't have cyber deterrence, redline policies, but says they're working on it*, in *http://fifthdomain.com,* 20 ottobre 2017 e v. M. POMERLEAU, *DoD is outpacing itself on cyber,* in *http://fifthdomain.com,* 8 novembre 2017. Da ultimo, di particolare interesse nella materia sono anche: la *«Presidential Policy Directive»* del luglio 2016, denominata *"PPD-41 - United States Cyber Incident Coordination",* che tende a riorganizzare in maniera chiara e coerente la macchina di gestione degli incidenti informatici nell'ambito del governo federale, in cui un ruolo centrale è assunto dai servizi di *intelligence,* mediante l'*Office of the Director of National Intelligence* e il suo *Cyber Threat Intelligence Integration Center;* l'*executive order* n. 13800 dell'11 maggio 2017*,* recante *«Strengthening the cybersecurity of federal networks and critical Infrastructure»,* redatto con l'obiettivo di rafforzare la sicurezza cibernetica dei *network* federali e delle infrastrutture critiche, prevedendo un cambio nelle metodologie con cui le agenzie federali americane investiranno nel prossimo futuro le risorse destinate alla difesa dalle minacce informatiche, indicando loro di redigere appositi *report* da consegnare direttamente al Presidente e al suo *team* entro periodi temporali che variano dai 60 ai 240 giorni ovvero predisporre un piano di fattibilità per accorpare le infrastrutture delle diverse agenzie federali e la richiesta, per quest'ultime, di adottare il *framework* sviluppato dal *National Institute of Standards and Technology* (per approfondimenti, v. *www.cyberaffairs.it, 20 maggio 2017 e* T. HUBBARD, G. L. WEBER and J. C. STEINHOFF, 12 *ways to defend the nation against cyberattack,* in *http://fifthdomain.com,* 2 novembre 2017); la *«National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework»* dell'agosto 2017 dell'*U.S. Department of Commerce,* consultabile su *https://doi.org/10.6028/NIST.SP.800-181,* per un esame della quale si rinvia a R. KALINYAK, *New guidelines help strengthen cybersecurity workforce,* in *http://fifthdomain.com,* 1 agosto 2017; la dichiarazione del 18 agosto 2017 del Presidente USA di elevare il Comando *cyber* americano allo *status* di un comando combattente unificato, una delle dieci strutture militari che possono effettuare missioni all'estero, sulla quale v. A. MEHTA *and* L. SHANE III, *Trump elevates Cyber Command; split with NSA still an option,* in *http://fifthdomain.com,* 19 agosto 2017. Detto ultimo piano di elevare la struttura è stato inserito nella legge di finanziamento del comparto difesa: il *«National Defence Authorization Act for Fiscal Year 2017 (NDAA)»*. La proposta di passare da comando sotto-unificato a un livello superiore era stata presentata da alcun senatori al Congresso, affinché fosse riconosciuto che «il cyberspazio è di fatto il campo di battaglia del 21° secolo». Di conseguenza è necessario che ci sia un comando che possa rispondere direttamente alle minacce organizzando sia la difesa sia possibili offensive. Fino a questo momento, invece, la struttura doveva necessariamente appoggiarsi ad altre. Ciò a seconda del tipo di azione che intendeva effettuare, soprattutto se al di fuori degli Stati Uniti. Inoltre, la struttura era guidata dal Direttore della *National Security Agency (NSA)* che aveva un doppio cappello. Secondo gli analisti la designazione di comando combattente e la maturazione continua dell'organismo gli conferirà una posizione di privilegio per richiedere future risorse e perseguire in autonomia lo sviluppo di tecnologie innovative, da ultimo sul tema v. M. POMERLEAU, *DoD still working toward CYBERCOM elevation,* in *http://fifthdomain.com,* 16 ottobre 2017 e M. POMERLEAU, *Does organizing cyberspace actually ratchet up potential for conflict?,* in *http://fifthdomain.com,* 10 novembre 2017.

(6) In tal senso, si pensi al cd. *"Russiagate",* ossia alle accuse sulle presunte *cyber*-intrusioni nelle elezioni americane 2016 da parte della Russia e dello stesso Cremlino, i cui *hackers* avrebbero violato il *server* del Comitato Nazionale dei Democratici, consegnando a *Wikileaks* lo scambio di *e-mail* fra il capo della campagna dei democratici John Podesta e la candidata Hillary Clinton per sabotarne l'elezione e favorire il candidato Donald Trump che con la Russia dichiarava di voler dialogare.

(7) *Internet* è una rete ad accesso pubblico che connette vari dispositivi in tutto il mondo. Dalla sua nascita rappresenta il principale mezzo di comunicazione di massa, che offre all'utente una vasta serie di contenuti potenzialmente informativi e di servizi. Dal punto di vista tecnico, si tratta di un'interconnessione globale tra reti informatiche di natura e di estensione diversa, resa possibile da una *suite* di protocolli di rete comune chiamata "TCP/IP" dal nome dei due protocolli principali, il *«Transmission Control Protocol»* (TCP) e l'*«Internet Protocol»* (IP), che costituiscono la "lingua" comune con cui i computer collegati a *Internet* (i cc.dd. *"host"*) sono interconnessi e comunicano tra loro a un livello superiore, indipendentemente dalla loro sottostante architettura *hardware* e *software*, garantendo così l'interoperabilità tra sistemi e sotto-reti fisiche diverse. Per le sue qualità di strumento di comunicazione senza confini e multistrato, *Internet* è diventato uno degli strumenti più potenti di progresso planetario, non soggetto a sorveglianza o regolamentazione statale.

(8) È significativo come un'indagine di qualche anno addietro (indagine speciale Eurobarometro del 2012 sulla cibersicurezza) abbia dimostrato che quasi un terzo dei cittadini europei non si fidi di usare *Internet* per operazioni bancarie o acquisti. La stragrande maggioranza degli intervistati ha anche affermato di evitare di rendere pubblici i propri dati personali *online* per questioni di sicurezza; al riguardo, si consideri che, a livello dell'Unione, più di un internauta su dieci è già stato vittima di frodi *online.*

(9) Si definisce «servizio digitale» un sevizio ai sensi dell'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (ossia qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi) di un tipo elencato nell'allegato III della direttiva NIS.

(10) Sul tema dell'incidenza della dimensione *cyber* nel campo delle tecnologie militari, con particolare riferimento all'Italia, v. C. BETTINI, *Il contributo della Difesa alla tutela degli interessi nazionali nell'ambito del dominio cibernetico,* in *Informazioni della Difesa*, 5, 2012, p. 295 e altresì v. *Nasce il Comando Interforze per le Operazioni Cibernetiche. Intervista al Capo di Stato Maggiore della Difesa, Generale Claudio Graziano,* in *Informazioni della difesa,* n. 3/2017, 8 e v. altresì SMD-G-032 «Direttiva di *Policy* Interforze sull'ambiente cibernetico» – Stato Maggiore della Difesa – III Reparto – Centro Innovazione della Difesa (Ed. 2012), nonché CAPSTONE CONCEPT CC – 001, «Implicazioni militari dell'ambiente operativo futuro» – Stato Maggiore della Difesa – III Reparto – Centro Innovazione della Difesa (Ed. 2012). In generale, l'uso dello spazio cibernetico nel campo militare è in realtà noto da tempo, sul tema v. D. BELLIN, G. CHAPMAN (a cura di), Computer *in guerra: funzioneranno? I rischi e le potenzialità delle nuove tecnologie militari,* Milano 1989. Sulle armi cibernetiche e sulle operazioni militari nello spazio cibernetico, v. G. GIACOMELLO, *Geopolitica delle armi autonome, op. cit.* (in nota 2). Al riguardo, fin dal 2004, negli USA, gli organismi preposti alla sicurezza nazionale hanno rilevato la portata del cambiamento e qualificato quello cibernetico come un rivoluzionario dominio operativo militare. Ad esempio, nel documento del 2004 redatto dal *Joint Chiefs of Staff* americano e intitolato *«National Military Strategy»,* si legge che le Forze Armate devono avere la capacità di operare nei domini dell'aria, della terra, del mare, dello spazio e in quello cibernetico. Nel 2006, invece, nel *«Quadrennial Defense Review»* (QDR), si evidenzia come il Dipartimento di Difesa americano «[…] tratterà lo spazio cibernetico come un nuovo dominio di guerra». Ma è dal 2010, ossia dall'anno in cui l'allora Segretario della Difesa americano William J. Lynn III ha qualificato pubblicamente il *cyberspace* come il "quinto dominio della conflittualità" dopo terra, mare, aria e spazio, che è diventata una necessità quanto mai prioritaria l'esigenza di avere norme utili – soprattutto sotto il profilo del diritto internazionale – a regolamentare con chiarezza gli aspetti che governano questo genere di azioni, cfr. W. J. LYNN III, *Defending a New Domain: The Pentagon's Cyberstrategy,* in *Foreign Affairs,* 2010, pp. 97-108; *The threat from the internet: Cyberwar,* in *Economist,* 2010. In tal senso, il crescente utilizzo del *cyberspace* anche per il supporto alle operazioni militari e l'incremento costante del numero e della qualità degli attacchi informatici – sempre più orientati non solo a colpire le infrastrutture critiche, ma anche gli strumenti di difesa (e in alcuni casi di attacco, v. *infra* note 15 e 16) di una nazione – rende ancora più improcrastinabile un approccio strategico il più possibile globale e condiviso da tutti i governi e le organizzazioni internazionali. Al riguardo, lo scorso 23 febbraio 2017, nel corso della conferenza AFCEA di San Diego, l'*Adm.* Michael Rogers, *Commander of U.S. Cyber Command and director of the National Security Agency Cyber,* ha affermato che *«I would argue that we should view cyber as one element of a broader deterrence campaign* […]. *Cyberspace is an operational domain in which the military does a variety of missions and functions, many of which are traditional».* Ha inoltre ribadito che *«the military executes reconnaissance and fire and maneuver activities in cyberspace much like the branches do in the physical world. Don't be intimated by the technical aspects of cyber. Don't make this thing so specialized, so unique, so different that it just gets pushed to the side. That will sub-optimize our ability to execute cyber operations, and quite frankly it will minimize or at least negatively impact, in my view, the operational outcomes, which is the whole reason we're doing this in the first place* […]. *What is stopping the military right now from pushing cyber down to the tactical level is not the classification, the super-secret stuff, which has little if anything to do with it, but rather it's getting correct the*

authorities and rules of engagement to be able to employ it». Nella medesima occasione, il *Vice Adm.* Michael Gilday, *Commander of the Navy's 10 th Fleet and Fleet Cyber Command,* ha affermato che *«If you're going to use automation in the defensive, you're sure as heck going to use it in the offensive»,* ma sul tema *cyber* in ambito Forze Armate americane v. anche v. M. POMERLEAU, *4 areas where military cyber forces should focus in* cyberspace, in *http://fifthdomain.com,* 10 ottobre 2017. Sullo specifico punto, preme evidenziare che, di recente, il 14 giugno 2016, i Ministri della difesa dei paesi appartenenti alla NATO hanno approvato il riconoscimento del *cyberspace* come quinto dominio della conflittualità, dopo terra, mare, aria e spazio. Riconoscimento, poi, ufficializzato durante il ventisettesimo incontro dei capi di Stato e di governo della NATO tenutosi nel luglio 2016 a Varsavia. Ne consegue che oggi gli attacchi perpetrati nello spazio cibernetico sono a tutti gli effetti paragonabili agli attacchi effettuati con armi cinetiche, in quanto i primi come i secondi possono avere forti ripercussioni politiche. In tale delicato settore, quindi, il principale obiettivo della NATO è quello di difendere i propri sistemi informatici e di aiutare gli Stati membri a sviluppare le più idonee capacità di *cyber-defence;* adesso il riconoscimento del *cyberspace* come dominio per le operazioni militari comporterà – già nel breve periodo – una necessaria evoluzione di questa postura, al fine di integrare al più presto lo spazio cibernetico nel campo della difesa collettiva. Detto riconoscimento, inoltre, non potrà non avere riflessi globali soprattutto alla luce dell'estensione anche al *cyberspace* della "clausola di difesa collettiva", che, come è noto, dal settembre del 2014, prevede che gli Stati appartenenti alla NATO si forniscano reciproca assistenza anche in caso di aggressione attraverso attacchi cibernetici, da ultimo sul tema v. M. POMERLEAU*, Here's how NATO is preparing for cyber operations,* in *http://fifthdomain.com,* 19 novembre 2017.

([11]) Gli stessi UAV – realtà in forte espansione, caratterizzata dallo sviluppo di una tecnologia duale – possono essere soggetti passivi di attacchi cibernetici, operando, essi, grazie ad un *data link* elettronico e interagendo con l'ambiente esterno tramite l'elettronica e lo spettro elettromagnetico, così raccogliendo, processando e scambiando una grande quantità di dati e informazioni che viaggiano nel *cyber* spazio e tra le infrastrutture fisiche e di rete a loro dedicate. Questa caratteristica li rende, quindi, potenzialmente vulnerabili ad attacchi esterni di carattere informatico. Le tipologie di attacco sono svariate e possono dimostrarsi estremamente pericolose, potendo riguardare sia la presa di possesso della memoria del velivolo, cancellando, sostituendo o molto più semplicemente sottraendo immagini o altre informazioni raccolte, sia l'acquisizione diretta del controllo del mezzo per compiere qualunque tipo di interferenza illecita, anche a fini di spionaggio, se non addirittura di natura terroristica. Sulla tematica tra l'atro, da ultimo, v. *Esercito Usa vieta l'uso di droni della cinese DJI per vulnerabilità* cyber, in *www.cyberaffairs.it, 12 agosto 2017.*

([12]) Contrazione di *"malicious software",* ossia di un programma inserito in una rete o sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo. I *software* malevoli sono divenuti, nel tempo, sempre più sofisticati; non solo sono adattabili a qualsiasi tipologia di obiettivo, ma sono anche in grado di sfruttare vulnerabilità non ancora note (cd. "0-*day*") per infettare le risorse informatiche dei *target.* Ciò consente a detti *software* di non essere rilevati da molti dei principali sistemi antivirus e di infiltrarsi senza trovare ostacoli. Essi, inoltre, sono in grado di celarsi nell'ambito del sistema-obiettivo, di spostarsi al suo interno, così da poterne effettuare una mappatura e propagare l'infezione. Infine, grazie agli stessi, le informazioni di potenziale interesse, prima di essere sottratte, vengono compresse e criptate per celarne l'esfiltrazione con il traffico di rete generato dall'ordinaria attività lavorativa del *target.* Per un'elencazione dei *software* malevoli anche in grado di entrare e penetrare nelle strutture e nei sistemi difensivi al fine di distruggerli, v. *http://securityaffairs.co/wordpress/3896/intelligence/cyber-weapons.html.*

([13]) Il reato cibernetico o cibercrimine si riferisce comunemente a un'ampia gamma di attività criminali, in cui i sistemi informativi e i sistemi informatici costituiscono l'arma primaria o il bersaglio primario. Il cibercrimine comprende reati tradizionali (ad es. frode, contraffazione o furto di identità), reati connessi ai contenuti (ad es., distribuzione in linea di materiale pedopornografico o incitamento all'odio razziale) e reati peculiari ai sistemi informatici e ai sistemi informativi (ad es., attacchi contro i sistemi informativi, rifiuto di servizio o *malware*). Sul tema cfr. anche la Convenzione di Budapest 23 novembre 2001 del Consiglio d'Europa sulla criminalità informatica, ratificata dall'Italia con legge 18 marzo 2008, n. 48.

([14]) Sul punto, v. J.A. LEWIS and S. BAKER, *The Economic Impact of Cybercrime and Cyber Espionage, Santa Clara, McAfee,* July 2013, p. 5, in *http://csis.org/node/45446* e v. AA.VV., *Tech companies targeted by sophisticated malware attack,* in *http://fifthdomain.com,* 25 settembre 2017. Per un'interessante lettura sul tema, v. *Guerre di rete,* C. FREDIANI, Bari, 2017.

([15]) In tal senso, si rileva come nel 2010 l'impiego del *malware "Stuxnet"* (*software* malevolo ad alto livello di complessità e di danno di verosimile realizzazione congiunta statunitense e israeliana), a cui sono seguiti *"Duqu"* e

"Flame", per attaccare alcuni impianti iraniani di arricchimento dell'uranio, ha segnato un punto di svolta netto nel dibattito circa la possibilità, fino ad allora meramente teorica, di danneggiare fisicamente l'infrastruttura critica di un paese sfruttando i sistemi informatici che la governano. Il *malware "Stuxnet"* ha avuto come obiettivo i sistemi informatici industriali costruiti da una noto colosso industriale tedesco e impiegati dal governo iraniano in alcune delle sue centrali di arricchimento dell'uranio; esso è noto per essere stato in assoluto il primo *software* malevolo – pubblicamente conosciuto – appositamente progettato con l'intenzione di spiare, sabotare, riprogrammare e soprattutto provare a danneggiare fisicamente il suo bersaglio in maniera del tutto autonoma e automatica. Detto *malware* ha richiesto mesi, se non anni di sviluppo, e ha necessitato di una tale mole di dati che non può non far dubitare che la sua provenienza fosse del tutto scevra dall'intervento di altri governi o agenzie di *intelligence* (numerose le ipotesi fatte al riguardo: Usa, Israele, Russia? In particolare, per la presunta attribuzione dell'attacco tramite *"Stuxnet"* ad opera dei servizi segreti israeliani, con particolare riferimento al *"Mossad"*, v. A. RAPAPORT, *La metemorfosi dell'intelligence israeliana,* in *Limes - A che servono i servizi,* n. 7/2014, p. 126, per approfondimenti v. anche *infra* nota 100). Esso era programmato per "attivarsi" solo nel caso in cui fosse arrivato ad infettare un sistema *"Supervisory Control And Data Acquisition"* (cd. SCADA, ossia quei sistemi informatici deputati al monitoraggio e controllo elettronico di sistemi fisici; si tratta, in particolare, di mezzi sviluppati per la gestione e il controllo di impianti come centrali, quadri elettrici, impianti industriali, gallerie o edifici, in sintesi, delle infrastrutture critiche di ogni Stato), equipaggiato con WinCC, PCS7 o STEP7, e ha avuto come obiettivo primario quello di arrivare alla PLC (*"Programmable Logic Controller",* ossia *computer* deputati all'esecuzione di un programma per l'elaborazione dei segnali digitali ed analogici provenienti da sensori e diretti agli attuatori presenti in un impianto industriale) dei sistemi informatici SCADA degli impianti nucleari di arricchimento dell'uranio di Natanz e Basher, e infettare quindi l'applicazione "*Step*-7" utilizzata per la loro programmazione e riprogrammare la velocità di rotazione delle turbine, allo scopo di danneggiare fisicamente le stesse, manomettendo irrimediabilmente gran parte delle centrifughe e delle ventole di raffreddamento di detti impianti e bloccando per circa due anni l'arricchimento dell'uranio in quella parte dell'Iran, ritardando in tal modo lo sviluppo del famigerato programma atomico governativo (al di là del caso *"Stuxnet",* nel 2016 si era anche diffusa la notizia che gli USA avevano in corso uno studio per un attacco informatico su larga scala ai sistemi iraniani di controllo dello spazio aereo, a quelli delle comunicazioni ed ai sistemi deputati all'erogazione dell'energia elettrica. Il nome in codice del piano di attacco sarebbe stato *"Nitro Zeus",* che sarebbe stato poi accantonato a seguito dell'accordo raggiunto sul programma nucleare iraniano; sul tema, vds. S. MELE, *Cyber Strategy & Policy Brief,* Volume 02 – Febbraio 2016). Per una disamina approfondita degli aspetti, anche tecnici, del *malware "Stuxnet",* si rinvia a L. MILEVSKI, *Stuxnet and Strategy: a Space Operation in Cyberspace?* in *JFQ (Joint Force Quarterly), issue* 63, 4th *quarter* 2011, M. DE FALCO, *Stuxnet Facts Report - A Technical and Strategic Analysis, NATO CCD COE Publications,* 2012 e a S. MELE, *Cyber-ware: aspetti giuridici e strategici,* ed. *Istituto Italiano di Studi Strategici "Niccolò Machiavelli",* 2013; ma vds. anche P. WOODWARD, *Iran confirms Stuxnet found at Bushehr nuclear power plant,* 2010, in *http://warincontext.org/2010/09/26/iran-confirms-stuxnet-found-at-bushehr-nuclear-power-plant/* e ancora J.P. FARWELL & R. ROHOZINSKI, *Stuxnet and the Future of Cyber War,* in *Survival: Global Politics and Strategy,* vol. 53, no. 1, February–March 2011. Autorevole dottrina (S. MELE, *cit.*) ha rilevato come l'attacco tramite il *malware "Stuxnet"* sia stato un tipico esempio di «convergenza tra azioni tipiche di *cybercrime* e interessi statali. Attraverso *"Stuxnet",* infatti, sembra aver preso forma "tangibile" quella linea dottrinale, ormai sempre più consolidata, che vede i Governi internazionali impegnati a capitalizzare il più possibile gli investimenti in materia di ricerca tecnica, tecnologica e di *know-how* sulla sicurezza informatica portati avanti principalmente da gruppi di ricercatori indipendenti e, sempre più spesso, anche da gruppi di criminali informatici […]». È questo il caso, ad esempio, dell'operazione di spionaggio elettronico denominata "*Red October*", avente come obiettivi privilegiati i sistemi informatici e le informazioni riservate/classificate in essi contenute di governi, ambasciate, centri di ricerca e società operanti nel settore energetico, petrolifero e del gas di ben 69 paesi in tutto il mondo. Stanti gli elementi finora analizzati dal *Kaspersky Lab*, che per primo ha posto sotto i riflettori questa impressionante rete di spionaggio elettronico, non sembra che questa operazione sia il frutto di un'attività sponsorizzata da uno Stato; molto più credibile, infatti, è l'attribuzione di questa operazione ad un gruppo criminale organizzato di matrice russa, avente come scopo quello di sottrarre informazioni classificate da rivendere sul mercato al miglior offerente. Per approfondimenti, si rinvia a *Securelist, The Red October Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies,* in *http://www.securelist.com,* 2013 ed a S. MELE, *I misteri di* Red October, in *http://www.formiche.net, 2013.* Per una recente introduzione al tema delle possibili reazioni alle attività di *cyber*-spionaggio, tra gli altri, Z.K. GOLDMAN, *Washington's Secret Weapon Against Chinese Hackers,* 2013 e *Global Research&Analysis Team (GReAT) - Kaspersky Lab, The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies,* 2013, in *http://www.securelist.com/en/blog/785/*. Detti episodi non sono

certo rimasti isolati. Nei mesi addietro ha fatto scalpore l'attacco globale avvenuto mediante il *virus "Petya"* (*"NotPetya"* secondo alcuni o *"GoldenEye"*), l'ultimo *ransomware* (il *virus* disattiva i *computer,* rendendone inaccessibili i file e chiede un riscatto di 300 dollari in *"Bitcoin"*) a propagarsi su scala globale (sul quale v. R. SATTER, *New cyberattack wreaking havoc globally*, in *http://fifthdomain.com,* 27 giugno 2017), e precedentemente mediante il *ransomware* denominato *"WannaCry"* – una variante del *"Wanna Decryptor"*, che ha sfruttato una vulnerabilità interna ai sistemi *Windows* – che il 15 maggio 2017 ha colpito 74 paesi, tra cui Italia, Regno Unito, Spagna, Russia, India, Cina, Ucraina, Taiwan ed Egitto. *"WannaCry"* è stato il primo *"computer worm"* ad essere abbinato a un *ransomware,* crittografando i dati sui pc delle vittime e richiedendo un riscatto per ripristinarne l'accesso. Diversi esperti di sicurezza informatica indicano la possibilità che dietro tale attacco *hacker* globale potrebbe esserci la Corea del Nord, cfr. *www.cyberaffairs.it, 20 maggio 2017*. Secondo le ricostruzioni, per infettare i pc in questione sarebbe stata utilizzata una vulnerabilità conosciuta come *"EternalBlue/DoublePulsar",* un sistema *exploit* che si ipotizza sia stato sviluppato dalla *National Security Agency (Nsa)* americana e che rientri tra i codici sottratti all'agenzia di *intelligence* americana da un gruppo di pirati informatici che si fa chiamare *"Shadow Brokers"*; per approfondimenti v. B. D. WILLIAMS, *Is NSA to blame for global WannaCry cyberattack?,* in *http://fifthdomain.com,* 22 maggio 2017. Di contro la NSA ha ricondotto la creazione di *"WannaCry"* al governo nordcoreano. Sul caso in questione e più in generale sugli attacchi informatici in Italia, v. *Audizione davanti alle Commissioni riunite Affari costituzionali e Difesa del Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS),* A. PANSA, con analisi delle problematiche legate alla difesa e alla sicurezza nello spazio cibernetico. Un analogo *virus* è stato appositamente utilizzato ad esempio nel dicembre del 2015, quando un attacco informatico ha lasciato una parte dell'Ucraina senza energia elettrica per diverse ore con ricadute, non banali, sulla popolazione; per approfondimenti si rinvia a S. ADL-TABATABAI, *FBI War of Cyber Attack on Electrical Grid,* April 11, 2016, in *http://yournewswire.com/fbi-warn-of-cyber-attack-on-electricalgrid/*. Al 2014 (ma le conseguenze sembrano essere più che mai attuali, alla luce del crescente clima di tensione in cui versano i rapporti tra i due governi mentre si scrive) viene fatto risalire il via al programma per sabotare con attacchi informatici ed elettronici i test missilistici della Corea del Nord, influendo così sui fallimenti negli ultimi lanci. Secondo le informazioni trapelate, sembra che l'amministrazione Obama abbia scelto tale strategia per far fronte ai progressi del programma nucleare e missilistico di Pyongyang. L'informazione, basata su fonti dell'amministrazione Obama e di quella Trump, oltre che su documenti connessi al programma, lega gli attacchi ai recenti fallimenti di diversi *test* missilistici nordcoreani. Il programma mirerebbe a sabotare i lanci con mezzi informatici ed elettronici prima che i missili siano collocati sulla loro piattaforma o nei primi secondi dopo il lancio. L'ex presidente Obama, affermano le fonti, aveva informato il successore Trump del programma e gli aveva detto che la questione sarebbe probabilmente stata la "più urgente" da affrontare. Anche se gli esperti restano divisi sull'efficacia di questi *cyber* attacchi (infatti, se nei primi mesi una serie di lanci falliti sembrava indicare il successo delle operazioni americane, diversi successi negli ultimi mesi hanno insinuato il dubbio), secondo alcuni di essi, i lanci falliti sono da attribuire soprattutto a problemi di fabbricazione e all'incompetenza dei nordcoreani, che hanno poi corretto gli errori riuscendo con successo ad effettuare tre lanci di missili di media portata negli ultimi otto mesi. Al riguardo, il dittatore nordcoreano Kim Jong-un ha affermato a gennaio 2017 che il suo Paese era ormai nella "ultima fase dei preparativi" per il primo *test* di un missile intercontinentale in grado di trasportare un'arma nucleare che può colpire gli Usa. Facendo riferimento a fonti delle amministrazioni Obama e Trump e alle conclusioni dei rapporti ufficiali, le informazioni sembrerebbero concludere che gli Stati Uniti non dispongano attualmente delle capacità per contrastare efficacemente i programmi nucleari e di missili balistici della Corea del Nord, fonte *New York Times* del 4 marzo 2017. Un'ulteriore ipotesi, rimasta poi solo tale, è quella che nel 2011 ha visto il Governo americano, in occasione della predisposizione dei piani di attacco contro la Libia, valutare in maniera molto concreta la possibilità di colpire e disabilitare attraverso un *cyber* attacco alcuni obiettivi sensibili e i sistemi di difesa aerea del Governo libico, commissionando uno specifico studio sulle infrastrutture tecnologiche libiche ad un gruppo di ventuno esperti del settore a livello internazionale. Ma, ancor prima, un utilizzo di *virus* malevoli su vasta scala si verificò durante la crisi tra Mosca e Tallinn nel 2007, quando un attacco condotto da *server* situati in Russia paralizzò per un mese le reti informatiche estoni che gestivano Governo, Parlamento, banche, ministeri, giornali e radio-televisioni; un *black-out* che Mosca mise in atto aggirando le deboli difese delle reti informatiche dell'Estonia e replicò l'anno successivo anche contro la Georgia, dove gli attacchi presero la forma, come del resto per l'Estonia, di *"Distributed Denial of Service"* (DDoS), letteralmente "negazione diffusa di servizio". Nella fattispecie, si trattò di attacco relativamente semplice e dai costi contenuti, a fronte del notevole impatto e delle ottime probabilità di riuscita, che andò a paralizzare i siti governativi, es. quello del Presidente e della Banca nazionale georgiana e d'informazione; su tali eventi si rinvia a *Estonia Hit by "Moscow Cyber War", BBC News, May* 17, 2007 e D. HOLLIS, *Cyberwar Case Study: Georgia 2008,* in *Small Wars Journal, January* 6, 2011 (l'Estonia, a seguito

di tali attacchi, ha acquisito grande consapevolezza della minaccia e, per fronteggiare la stessa, ha rafforzato i propri legami anche con gli USA; in tal senso è recente la notizia che il *«US Secret Service trains Estonia to handle cyber threats* […]. *Estonia has teamed up with the U.S. Secret Service ahead of its first European Union presidency to train local officials to handle cyber threats — the greatest of which comes from Russia, according to the nation's foreign intelligence service.* […]. *Separately, the head of Estonia's foreign intelligence service, Mikk Marran, said Wednesday that Russia was the greatest source of a threat to Estonia in cyberspace because Estonia is a member of both the EU and NATO»,* in *defensenews.com,* 8 febbraio 2017). Sempre nel 2007, Israele, in occasione dell'attacco sferrato con missili al fine di distruggere la centrale nucleare di Kibar in Siria, prima di procedere con i bombardamenti, secondo alcuni analisti sembra abbia fatto ricorso, ancora una volta, ad un *malware* per disabilitare i sistemi informatici di Damasco per il controllo dello spazio areo. L'obiettivo dell'azione israeliana non era solamente quello di penetrare all'interno delle stazioni *radar* dell'intero reparto difensivo siriano – cosa che avrebbe probabilmente destato sospetti e messo in allarme il personale e gli stessi sistemi predisposti alla sicurezza – ma soprattutto di ingannare i sistemi operativi e impedire, per un lasso di tempo circoscritto ma sufficiente ai fini dell'attacco, che gli operatori individuassero velivoli in avvicinamento, precludendo, quindi, la gestione a terra delle operazioni. Risalendo ancora nel tempo, non può dimenticarsi quanto accaduto nel 1982 lungo il gasdotto transiberiano, dove un'imponente esplosione, alla base della quale, secondo gli analisti, vi sarebbe stata la regia della *Central Intelligence Agency (CIA),* non venne provocata dall'arresto fortuito dei sistemi, ma dal deliberato sovraccarico dell'impianto, attraverso la manipolazione delle valvole di controllo della pressione mediante *malware* e tramite lo sfruttamento dei sistemi operativi in dotazione alla struttura.

([16]) Nel 2016, ad esempio, un misterioso gruppo di *hackers*, chiamato *"Shadow Brokers"*, è riuscito a entrare nell'arsenale dell'*Equation Group,* legato alla *National Security Agency (NSA).* A seguito dell'attacco, sono stati rubati diversi strumenti sofisticati di difesa e attacco *cyber.* Gli *hackers* hanno poi provato a metterli in vendita all'asta nel *Dark Web*, ma non sono riusciti a venderli. Da allora il gruppo è scomparso.

([17]) I *cyber* attacchi possono causare non solo danni economici o informatici, ma anche mettere in pericolo vite umane. Basti pensare ai danni che potrebbero verificarsi se un terrorista assumesse il controllo dei semafori o del sistema ferroviario o portuale oppure a quelli potenziali se una *botnet* attaccasse il sistema telefonico nazionale oppure se un *ransomware* fosse capace di bloccare una centrale per il trattamento delle acque potabili o, peggio ancora, se un *malware* mandasse in *tilt* le torri aeroportuali civili. Senza pensare ai satelliti spaziali, che devono essere costantemente aggiornati in remoto e che gestiscono i sistemi di navigazione (vedi il GPS americano o il GLONASS russo).

([18]) Grazie alle nuove tecnologie e alla digitalizzazione, la rete elettrica sta evolvendo, diventando sempre più interdipendente con la rete informatica. I benefici sono molti, a partire dall'avvento di impianti, reti e servizi sempre più efficienti e *smart.* Tuttavia, vi sono anche aspetti da non sottovalutare in termini di pericoli intrinseci: aumentano i rischi di attacchi informatici da parte di *hackers* sempre più esperti, con tutte le conseguenze che ne possono derivare: dalla totale interruzione dei servizi agli attacchi terroristici. I rischi concreti vanno dai *black out,* anche molto estesi, a disastri più gravi, visto che ormai le *smart grid* connettono tra loro in maniera integrata, per la gestione delle informazioni e del controllo della rete elettrica, anche centrali nucleari, oleodotti, gasdotti e sistemi di ri-gassificazione, oltre alle tecnologie di produzione di energia da fonte rinnovabile. In detto specifico settore, gli obiettivi di un *hacker* possono essere vari: rubare informazioni e compromettere i dispositivi di controllo delle reti per estorcere denaro, rivendere brevetti alle aziende concorrenti o minacciare la sicurezza di una nazione. Gli *hackers*, poi, possono inserire dati di traffico contradditori per indurre decisioni sbagliate nei sistemi di risposta e sabotare il sistema di comunicazione ed elaborazione dei dati per ritardarlo o mandarlo in *tilt.* Una recente simulazione ha stimato che, in caso di attacco alla rete elettrica, un *black-out* energetico che duri qualche settimana determinerebbe un collasso totale dell'intero "Sistema-Paese", producendo danni, anche in termini di vite umane, paragonabile a quello di un'aggressione militare su larga scala. Questo è quanto emerge dal nuovo *«Report Cyber Security in the Energy Sector»*, commissionato dalla Direzione generale energia della Commissione Europea alla piattaforma europea degli esperti energetici della sicurezza informatica nell'energia (Eecsp). Dal *report* emerge che, nella sua strategia per la sicurezza informatica, l'Europa non affronta le problematiche riferite all'energia: manca, infatti, un quadro generale e un sistema coordinato per gestire i rischi di eventuali attacchi da parte di *hackers,* che possono avere effetti dirompenti. Il rapporto UE propone, quindi, un quadro strategico, con l'obiettivo di affrontare le sfide *cyber* nel settore energetico, compreso il nucleare. Il piano è composto da quattro priorità strategiche: identificazione di aree chiave di minaccia e gestione dei rischi, la risposta informatica in caso di un attacco, il continuo miglioramento della *cyber* resilienza e l'accumulo di capacità e competenze richieste per il settore dell'energia. Gli obiettivi generali da raggiungere sono invece: mettere in sicurezza i sistemi energetici che forniscono servizi essenziali per la società europea e per proteggere i dati nei sistemi energetici e la *privacy* dei

cittadini dell'UE. Le criticità rilevate dal *report* sono particolarmente sentite in Italia, dove nel 2016 gli attacchi informatici alle infrastrutture critiche, tra cui quelle dell'energia, sono aumentati del 15% rispetto al 2015. Anche il settore eolico riscontra la necessità di intensificare i sistemi di sicurezza dei dispositivi informatici legati ai sistemi di gestione e manutenzione delle turbine eoliche dei sistemi SCADA, che, nella maggior parte dei casi, non sono stati creati per il *web* e risultano, quindi, obsoleti e più soggetti ad infiltrazioni di *hackers*. In ambito nazionale, sul tema, da ultimo, v. *Documento sulla Strategia Energetica Nazionale (SEN)*, che, con specifici richiami anche alla Direttiva NIS, affronta il tema del rischio *cyber* nelle infrastrutture critiche del settore energetico. Sempre in tema di attacchi *cyber* nel settore energetico, con particolare riferimento agli Stati Uniti, è stato evidenziato che *«Oil and gas companies, including some of the most celebrated industry names in the Houston area, are facing increasingly sophisticated hackers seeking to steal trade secrets and disrupt operations* […]. *A stretch of the Gulf Coast near Houston features one of the largest concentrations of refineries, pipelines and chemical plants in the country, and cybersecurity experts say it's an alluring target for espionage and other cyberattacks. There are actors that are scanning for these vulnerable systems and taking advantage of those weaknesses when they find them* […]. *Homeland Security, which is responsible for protecting the nation from cybercrime, received reports of some 350 incidents at energy companies from 2011 to 2015, an investigation by the Houston Chronicle has found. Over that period, the agency found nearly 900 security flaws within U.S. energy companies, more than any other industry»,* in *http://fifthdomain.com,* 6 marzo 2017. Per le potenziali conseguenze catastrofiche di un attacco cibernetico nel settore energetico, J. KALLBERG, *Surprise: Cyber presents serious environmental consequences* in *http://fifthdomain.com,* 24 marzo 2017. Il tema è così sentito in USA che il Dipartimento dell'Energia (DoE) americano è in procinto di assegnare fino a 50 milioni di dollari ai Laboratori Nazionali del dipartimento da destinare alla ricerca per la sicurezza delle infrastrutture critiche energetiche. I fondi sosterranno la fase iniziale di ricerca e sviluppo di strumenti e tecnologie di nuova generazione per migliorare ulteriormente la resilienza delle infrastrutture critiche energetiche della nazione, tra cui la rete elettrica e l'infrastruttura del gas e del petrolio. Il DoE ha inoltre assegnato finanziamenti di ricerca per sette progetti di *Resilient Distribution Systems*, che stanno sviluppando una tecnologia di distribuzione dell'energia più durevole. Da ultimo, giova evidenziare che la delicatezza di tale problematica risulta comprovata dal recente attacco tramite il *virus "Petya"*, che il 27 giugno 2017, ha colpito, tra l'altro, alcune importanti infrastrutture critiche energetiche in Ucraina (la più importante compagnia nazionale e la centrale di Chernobyl) e sul quale v. *Ukraine: Russian security services were behind global cyberattack,* in *http://fifthdomain.com,* 6 luglio 2017.

([19]) V. *supra* nota 10 e *infra* nota 21.

([20]) In tal senso, «Gli attacchi informatici stanno diventando più frequenti, più organizzati e più costosi nei danni che causano alle amministrazioni governative, alle imprese, alle economie e potenzialmente ai trasporti e alle reti energetiche, nonché alle infrastrutture critiche; questi attacchi possono raggiungere una soglia tale da minacciare la prosperità, la sicurezza e la stabilità nazionale e quella Euro Atlantica. Forze Armate straniere e agenzie di *intelligence,* la criminalità organizzata e/o i gruppi estremisti possono essere ciascuno una fonte di questo tipo di attacchi», *NATO, Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*, 2010, in *http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.*

([21]) Al riguardo, per aumentare le capacità complessive di *cyber-defence*, rivestono un ruolo fondamentale anche la collaborazione e la fiducia reciproca tra Stati dell'UE e alleati della NATO, per approfondimenti v., tra gli altri, L.K. ILVES, T.J. EVANS, F.J. CILLUFFO, and A.A. NADEAU, *European Union and NATO Global Cybersecurity Challenges - A Way Forward,* in *Features, Prism* 6, no. 2, *July* 2016 (127). Detta presa di coscienza ha, quindi, portato anche una maggiore sinergia tra l'UE e la NATO, per tale ragione *«Following up on their Joint Declaration signed last July, the EU and NATO adopted on 6 December 2016 a common set of proposals that aim to broaden and deepen their cooperation substantially. The implementation plan includes concrete 42 proposals in 7 areas of cooperation:* […] *cybersecurity and defence* […]», per maggiori dettagli su questa proposta si rinvia a *http://data.consilium.europa.eu/ doc/document/ST-15283-2016-INIT/en/pdf.* Da ultimo, v. anche la comunicazione congiunta *«Resilience, Deterrence and Defence: Building strong cybersecurity for the EU» JOIN*(2017) 450 *final* del 13 settembre 2017 (par. 4.3 concernente la cooperazione UE-NATO, sulla quale v. F. RUGGE, *Nato o UE: l'importante è fare squadra*, in *Osservatorio Cybersecurity dell'ISPI* dell'ottobre 2017). Al riguardo, la NATO ha deciso di aumentare il livello di partecipazione dell'UE alle esercitazioni per la difesa dai *cyber*-attacchi dell'alleanza anche mediante apposite esercitazioni che si chiameranno «*Cyber Coalition*» e saranno tra le più grandi di questo tipo mai organizzate al mondo. Più in generale, sulle politiche europee di difesa del *cyberspace,* v. E. PLATTEAU e A. GAŁYGA, *European cyberspace in focus,* secondo il quale *«Acknowledged as the fifth dimension of a conflict – along with land, sea, air and space – cyber defence is gradually moving beyond the scope of the purely national domain establishing itself as an issue to be tackled at the EU level»* e ancora W. RÖHRIG, *The European Defence Agency contributes to strengthening EU cyber defence,* secondo il quale *«The EU strives for increased cyber defence capabilities and a trained cyber workforce.* […] *how*

research, technology advancement and collaborative training lead to capability development and an increased awareness of cyber threats», entrambi in *Magazine of European Defence Agency - European defence matters, Issue* 9, 2015 e v. J.P. DARNIS, *Difesa europea: nel futuro, verso agenzia spaziale, di dati e cyber*, in *www.affarinternazionli.it* del 30 ottobre 2017.
A ben vedere, la NATO aveva previsto già da tempo che la minaccia cibernetica era destinata ad aumentare: *«Cyber-attacks are becoming more frequent, more organized and more costly* […]; *they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability»,* in *North Atlantic Treaty Organization,* in *«Active Engagement, Modern Defence: Strategic Concept for the Members of the North Atlantic Treaty Organisation»,* November 19, 2010. Sul tema, v. anche *The History of Cyber-attacks - a Timeline,* in *NATO Review Magazine,* in *http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm;* S. RANGER, *NATO updates cyber defense policy as digital attacks become a standard part of conflict,* ZDNet, June 30, 2014, in *http://www.zdnet. com/nato-updates-cyber-defence-policy-as-digitalattack; Cyber Defence - North Atlantic Treaty Organization,* February 16, 2016, in
http://www.nato.int/cps/en/natohq/topics_78170.htm; R. TEHAN, *Cybersecurity Legislation, Hearings, and Executive Branch Documents, (Washington, DC: The Congressional Research Service, March 30,* 2016), in
https://www.fas.org/sgp/crs/misc/R43317.pdf. Anche per dette ragioni, *NATO working out how to conduct operations in cyberspace*, in *http://fifthdomain.com,* 13 giugno 2017, dal quale emerge che *«A fundamental challenge faced by NATO, particularly in the development and deployment of effective defensive and offensive cyber weaponry tools, is how to optimize collaboration with the cyber intelligence infrastructures of member nations in responding to attacks in an ever-changing cyber battle theater».* Giova rilevare che la politica di *cyber defence* è attuata dalle autorità politiche, militari e tecniche della NATO come dai singoli Stati alleati. Dopo il *summit* di Lisbona del 20 novembre 2010 tra i Capi di Stato e di Governo di tutti i paesi membri, è stato promulgato un nuovo "Concetto Strategico", che pone in evidenza la necessità di sviluppare la difesa contro attacchi cibernetici. In seguito, la NATO ha elaborato un Concetto, una *Policy* e il relativo *Action Plan.* Uno dei principali aspetti di questa politica è stata la creazione della *NATO Cyber Defence Management Authority (CDMA),* con l'unica responsabilità di coordinare la difesa informatica in tutti i quartieri generali dell'Alleanza e nei comandi e nelle agenzie associate, spostando le molteplici reti informatiche di oggi verso un sistema amministrato a livello centrale. Il CDMA della NATO è gestito dal *Cyber Defence Management Board,* che comprende i responsabili degli uffici politici, militari, operativi e tecnici della NATO che si occupano di difesa informatica. Il CDMA è il principale organo di consulenza del Consiglio Atlantico in materia di difesa informatica e offre pure consulenza agli stati membri su tutti i principali aspetti della difesa cibernetica. Il CDMA della NATO opera sotto l'egida della divisione *Emerging Security Challenges* (sfide emergenti alla sicurezza) del NATO HQ (comando e *staff*). A seguito della riorganizzazione della NATO, che ha comportato la soppressione dei *Sub-Commitee* (SC) e di molteplici *Ad Hoc Working Group* (AHWG), nell'ambito del NC3B è stato istituito *l'Information Assurance and Cyber Defence* (IACD) *Capability Panel* (CaP/4) e il dipendente *Capability Team* (CaT) per la *Cyber Defence*, con il compito di definire le linee guida, le strategie e gli *standard* da impiegare in materia di *cybersecurity*, nonché di promuovere la cooperazione, lo sviluppo tecnologico e la standardizzazione tra i paesi dell'Alleanza. In linea con il nuovo "concetto strategico" della NATO, approvato con le dichiarazioni finali del Vertice di Lisbona, la NATO ha avviato nel 2011 un'importante iniziativa tesa ad acquisire una prima capacità di difesa e contrasto verso le emergenti minacce *cyber* alle reti TLC ed ai sistemi informatici propri e dei paesi dell'Alleanza. Si tratta del conseguimento della *Full Operational Capability* (FOC) della *NATO Computer Incident Response Capability* (NCIRC), che consiste, essenzialmente, nell'acquisizione di prodotti e servizi *cyber* relativi alle funzioni di *prevent, detect, react, mitigate and report*, a protezione delle strutture di Comando *Joint* di Vertice della NATO e di quelle dei Comandi territoriali e di teatro subordinati. Il progetto, gestito dalla *NATO Communications and Information Agency* (NCIA), è stato finanziato per un importo di circa 32 M€, più l'onere relativo al mantenimento dei primi anni di esercizio, stimato in circa 24 M€. Il relativo contratto, di natura classificata, e concluso allo scopo di condividere informazioni confidenziali per migliorare la conoscenza del contesto di riferimento e aumentare la protezione delle rispettive reti e sistemi, è stato assegnato ad un raggruppamento industriale multinazionale a guida dell'industria italiana Leonardo, sul quale per approfondimenti, v. *Accordo di collaborazione tra Leonardo e NATO nella* cybersecurity, in *www.analisidifesa.it,* 7 giugno 2017; in generale sulla collaborazione dell'azienda italiana con la NATO nel settore *cyber*, v. T. KINGTON, *Leonardo eyes work on NATO cyber command,* in *http://fifthdomain.com,* 27 settembre 2017 e *Leonardo e l'agenzia NCI estendono i servizi di* cyber security *ai nuovi comandi NATO*, in *analisidifesa.it* del 20 ottobre 2017. Da ultimo, in ambito NATO è in corso l'esame di una proposta che prevede una spesa di circa 3 miliardi di euro per aggiornare la propria tecnologia satellitare e informatica nei prossimi tre anni, al fine di tenere il passo con le nuove minacce. Parte di questa spesa, circa 800 milioni, saranno investiti sui sistemi informatici che contribuiscono a controllare le difese aerea e missilistica e altri 71 milioni serviranno per migliorare la protezione rispetto ad attacchi *cyber* delle 32 principali strutture Nato. La NATO dovrebbe fornire i dettagli del piano a breve,

per poi aprire il processo delle offerte, che dovrebbe attrarre i grandi gruppi occidentali della difesa, come Airbus Group, Raytheon e Lockheed Martin. Per approfondimenti, v. *Cyber security,* quale *roadmap* per la NATO? in *www.cyberaffairs.it, 8 luglio 2017*.

(22) In tal senso, lo scandalo *"WikiLeaks"* (dall'inglese *leak* «perdita», «fuga» di notizie) e la diffusione di notizie nel *cyberspace* hanno allarmato non poco i servizi di *intelligence* (nella fattispecie quelli americani), anche in considerazione della fuga di documenti classificati *"confidential"* e *"secret"*. Ma i timori legati alle *cyber*-tecnologie sembrano persistere, considerato che di recente un nuovo rilascio, cd. *"Vault 7"*, di 8.761 documenti da parte di *"WikiLeaks"* sembrerebbe disvelare nuove attività (di controllo e spionaggio remoto) compiute dai servizi di *intelligence* statunitensi. *"WikiLeaks"* ha affermato che la CIA ha «perso il controllo del suo arsenale», che includerebbe *software* capaci di controllare i *computer* in tutto il mondo e di trasformare un televisore o qualsiasi altro dispositivo elettronico, come uno *smartphone,* in un sistema che capta ogni conversazione, in tal senso v. *Thousands of CIA spy files posted on internet,* in *The Time,* 8 marzo 2017; *Documents Said to Reveal Hacking Secrets of C.I.A.* in *The New York Times,* 8 marzo 2017; *La Cia usa le TV per spiare,* in *Corriere della Sera,* 8 marzo 2017 e *Inside Vault 7: Digging into WikiLeaks "Year Zero" trove of CIA hacking docs,* in *http://fifthdomain.com,* 7 marzo 2017, secondo il quale *«The controversial transparency organization WikiLeaks published on Tuesday an archive of 8,761 documents and files the organization claims originate from the "CIA's global covert hacking program." WikiLeaks alleges the documents were stolen by an unidentified threat actor from the network of the CIA's Center for Cyber Intelligence in Langley, Virginia. The Associated Press cited experts who are reviewing the documents and said the leaked material appeared legitimate. A former NSA employee, speaking to FifthDomain on background, was unable to authenticate the documents but agreed they appeared to be legitimate. Past WikiLeaks publications have proven to be authentic»* e ancora *What CIA cyber spies think of 6 top antivirus programs,* in *http://fifthdomain.com,* 8 marzo 2017. A seguito di tali eventi, il Direttore della CIA ha denunciato *"WikiLeaks" «as a hostile intelligence service and a threat to U.S. national security»,* in *http://fifthdomain.com,* 13 aprile 2017. Tuttavia, ciò che deve far riflettere di più, in termini di sicurezza nazionale, è la capacità dei servizi di *intelligence* (in questo caso americani) di spiare dispositivi comuni, grazie a una superiorità tecnologica rispetto agli altri. Invero, la natura invisibile degli attacchi *cyber* solleva particolari questioni relative alla sicurezza e alla riservatezza delle informazioni, dal momento che è più difficile individuare quando e da quanto tempo si è sotto spionaggio *cyber* (anche da parte di agenzie di *intelligence* di governi alleati) e soprattutto da parte di chi e a quale scopo, poiché tali strumenti vengono utilizzati non solo per accedere a informazioni riservate di carattere politico e inerenti alla sicurezza nazionale, ma anche per raggiungere obiettivi di interesse economico da parte di terzi. Per il ruolo dei servizi segreti nello specifico settore della *cyber* in ambito mondiale, v. AA.VV. *A che serve l'*intelligence *italiana,* in *Limes - A che servono i servizi,* n. 7/2014.

(23) Tuttavia, non di poco momento si presenta la soluzione giuridica del problema in questione, involgendo esso diversi aspetti critici (come, ad esempio, quando un *software* malevolo può essere considerato una *cyber*-arma) che parte della dottrina ha provato a mettere in luce, in tal senso v. M. ROSCINI, *Cyber operations and the use of force in International Law, Oxford, Oxford University Press*, 2014; M.N. SCHMITT, *Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press,* 2013; H.H. DINNISS, *Cyber Warfare and the Laws of War,* Cambridge University Press, 2012; E. TIKK, A.M TALIHÄRM, *International Cyber Security Legal&Policy Proceedings,* CCD COE *Publications,* 2010; E. TIKK, K. KASKA, L. VIHUL, *International Cyber Incidents: Legal Considerations,* CCD COE *Publications,* 2010; W.A. OWENS, K.W. DAM, H.S. LIN, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, National Academies Press,* 2009. Da più parti si è altresì richiamata la possibilità di invocare l'art. 5 del Trattato NATO per determinati attacchi informatici; sul punto v. *NATO might trigger Article 5 for certain cyberattacks, www.defencenews.com* del 31 maggio 2017. Un ruolo importante nell'analisi degli aspetti giuridici nel settore *cyber* è giocato dal *«Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations»,* presentato l'8 Febbraio 2017 a Washington. Il nuovo Manuale, che rappresenta la versione aggiornata del *«Tallinn Manual on the International Law Applicable to Cyber Warfare»* del 2013, si propone di essere l'analisi più comprensiva di come il diritto internazionale esistente sia applicabile alle operazioni cibernetiche. La prima edizione del volume, come indicato dal titolo stesso, analizzava esclusivamente situazioni di alto rischio, ma bassa probabilità (cd. *"High risk-low probability"*), ossia considerava le operazioni cibernetiche unicamente in contesti di conflitto internazionale o guerra (in particolare "Stato contro Stato"). Il nuovo Manuale e si propone, invece, di disciplinare anche quelle operazioni (cd. *"Cyber incidents"*) che avvengono in regimi di pace e che cadono al di sotto del livello di uso della forza, i cd. *"day-to-day cyber incidents"* che gli Stati devono fronteggiare oramai quotidianamente. Oltre all'introduzione stessa di questa tipologia di attacchi, finora ricompresi in una *"grey zone"* del diritto internazionale e, pertanto, di non facile classificazione, il Manuale ed. 2017 inserisce una serie di novità importanti: 1) disciplina il ruolo degli attori non statali, assoggettando anch'essi al diritto internazionale in quanto *proxy* degli Stati; 2) determina le conseguenze di un attacco portato avanti contro soggetti privati, i quali, cadendo sotto la responsabilità degli Stati di appartenenza,

sono potenziali destinatari del diritto di protezione statuale; 3) in ultimo, disciplina la questione che lega l'adozione di contromisure al problema dell'attribuzione, disciplinandola secondo il grado di gravità dell'attacco subito. L'introduzione di queste novità da parte del nuovo Manuale sottolinea non soltanto una maggiore attenzione verso quelle che sono le reali necessità degli Stati, i quali si vedono coinvolti più in incidenti ibridi che in guerre cibernetiche vere e proprie, ma anche la voglia di risolvere in senso pratico il nodo gordiano dell'attribuzione nel *cyberspazio*, al fine di fare un ulteriore passo avanti nella gestione di situazioni divenute ormai all'ordine del giorno.

(24) Lo spionaggio è da sempre il metodo migliore per ottenere vantaggi politici, strategici, economici e militari nei confronti dei nemici e, soprattutto, degli alleati, sia in tempo di guerra che di pace. I cibercriminali e le *cyber-spies*, nel contesto della competizione economica tra paesi, si avvalgono di metodi sempre più sofisticati per infiltrarsi nei sistemi informativi, rubare dati critici o ricattare imprese al fine di accrescere la loro capacità conoscitiva nei confronti delle aziende concorrenti. In particolare, si assiste all'esponenziale aumento dello spionaggio economico, solitamente alla ricerca di segreti industriali, con particolare riguardo a quelli ad alta valenza di innovazione tecnologica, in grado di accelerare, ad esempio nel settore della difesa, lo sviluppo tecnologico di armamenti e colmare quel *gap* capacitivo-militare di cui alcuni Stati godono. L'importanza strategica della possibilità di trafugare segreti militari rimane dunque un aspetto primario della minaccia cibernetica in generale e dal quale nessuno dei protagonisti della scena internazionale può ritenersi immune. Molti paesi hanno assistito, infatti, al furto massiccio di *know-how*, ma anche l'aumento di attività di *cyberwarfare* e, più in generale, di attività sponsorizzate dagli Stati a danno di altri Stati nel ciberspazio dà origine ad una nuova categoria di minacce per gli Stati e le imprese dell'UE, questioni, queste, che anche gli organismi di *intelligence* non possono oramai trascurare. Sull'importanza del tema in questione, *Acting Assistant Attorney General's agenda on foreign cyber espionage*, secondo il quale *«Perhaps the most salient form for this audience is theft by cyber intrusion. In May 2014, in a first-of-its kind case, DOJ indicted five Chinese military hackers for stealing trade secrets and sensitive business information from U.S. companies for the benefit of Chinese competitors. The indictment alleged numerous and specific instances in which uniformed officers of the Third Department of the Chinese People's Liberation Army (PLA) hacked into the computer systems of American nuclear power, metals and solar-products companies to steal trade secrets and sensitive internal communications, such as pricing information and trade litigation strategy, that could be used by Chinese companies for commercial advantage. This was the military officers' full-time day job: our indictment alleged that their activity peaked between 9 a.m. and 12 p.m., their time, stopped for an hour — a healthy lunch break — and then picked up again from 1 p.m. to 6 p.m. No company can expect to always successfully defend against these kinds of organized campaigns»,* in *www.insidecybersecurity.com*, 29 marzo 2017. Per un elenco dei gruppi di spionaggio, v. *Chi sono i 10 gruppi di* cyber *spionaggio più pericolosi,* in *www.difesaesicurezza.com* del 27 aprile 2017 e sull'impatto della minaccia *cyber* nel settore commerciale americano v. T. MCCOY, *Cyberwar's battlefield: The commercial sector,* in *http://fifthdomain.com,* 13 novembre 2017.

(25) Nel 2016, nel mondo sono stati 1.050 gli attacchi con conseguenze considerabili "gravi" (mai così tanti). In particolare, gli attacchi gravi compiuti per finalità di *cybercrime* sono in aumento del 9,8%, mentre crescono a tre cifre quelli riferibili ad attività di *cyber warfare*. In termini assoluti, *cybercrime* e *cyber warfare* fanno registrare il numero di attacchi più elevato degli ultimi sei anni. Il 32% degli attacchi viene sferrato con tecniche sconosciute, in aumento del 45% rispetto al 2015, principalmente a causa della scarsità di informazioni precise in merito tra le fonti di pubblico dominio. A preoccupare maggiormente gli esperti del *Clusit,* tuttavia, è la crescita (1.166%) degli attacchi compiuti con tecniche di *phishing* e *social engineering* ovvero mirati a "colpire la mente" delle vittime, inducendole a fare passi falsi che poi rendono possibile l'attacco informatico vero e proprio. A livello globale la somma delle tecniche di attacco più banali (SQLi, DDoS, Vulnerabilità note, *phishing, malware* "semplice") rappresenta il 56% del totale: questo dato è uno dei più allarmanti, poiché rende evidente la facilità di azione dei cybercriminali e la possibilità di compiere attacchi con mezzi esigui a basso costo. Gli esperti segnalano anche il tema dei "captatori informatici". Si tratta dei "*trojan* di Stato" per le intercettazioni, come quelli realizzati da *"Hacking Team"*. Questi *trojan* sono captatori informatici (conosciuto anche come *software* spia) e sono come armi di distruzione di massa per la *privacy,* perché consentono – con relativa facilità – di intercettare conversazioni, *chat,* spiare utenti attraverso i microfoni e le *webcam* dei *computer* e cellulari. Essi comunicano sfruttando la rete *Internet*, in modalità nascosta e protetta ed inviano quanto appreso ad un centro remoto di comando e controllo che li gestisce; possono cercare tra i file presenti sul dispositivo "ospite" o su altri connessi in rete locale; inoltre dispongono di contromisure che li rendono in grado di nascondersi agli antivirus; sfruttano le vulnerabilità, spesso non ancora note, dei sistemi operativi o degli applicativi per aggirare controlli o contromisure che potrebbero ostacolarli o inibirli. In assenza di regole, i captatori informatici sono un pericolo costante per gli equilibri democratici. Tutti questi elementi indicano l'urgenza di un piano nazionale per la *cybersecurity,* che affronti in modo sistematico il tema, con le giuste risorse, cfr. *Rapporto Clusit 2017,* la nota associazione per la sicurezza informatica italiana (per l'Italia i dati sono elaborati in collaborazione con il *security center* di *Fastweb*).

([26]) Con il termine di *cybersecurity* si intende quell'insieme di tecnologie, programmi, processi e tecniche concepiti e messi in atto per proteggere *computer* e reti informatiche. È una protezione che si sviluppa su due livelli, dunque: uno contenutistico, riguardante i dati, l'altro riguardante l'*hardware*, cioè le macchine. Cercando di essere concisi, si potrebbe definire la *cybersecurity* come l'insieme di precauzioni e interventi «che si possono prendere per proteggere il ciberdominio, in campo sia civile che militare, nei confronti delle minacce associate o che possono nuocere alle loro reti e infrastrutture di informazione interdipendenti», v. in tal senso Commissione europea, «*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace», (JOIN(2013)1),* 7 *February* 2013, p. 3, nota 4. La *cybersecurity* si propone, quindi, di salvaguardare la disponibilità e l'integrità delle reti e dell'infrastruttura (*hardware*), la riservatezza delle informazioni che esse contengono, la protezione *software* degli archivi, dei dati degli utenti, di elaborare progetti di *disaster recovery* e, ma non per questo meno importante, di intervenire sulla formazione (un ente o un'azienda può attrezzarsi con i migliori sistemi di *cyber-defence*, ma il comportamento disattento e superficiale di un dipendente può rivelarsi decisivo). Clamoroso fu il caso del 2008, che permise a degli *hacker* russi di entrare in un *network* chiuso del Pentagono; per riuscirvi piazzarono delle chiavette infette da *virus* nel negozio più vicino alla base NATO di Kabul, immaginando che qualche dipendente statunitense ne avrebbe comprata una per usarla in ufficio, come poi effettivamente accadde). In tal senso, anche diverse aziende del settore tecnologico della difesa hanno mostrato sempre maggiore interesse alla possibilità di offrire prodotti di *cybersecurity* per salvaguardare la disponibilità e l'integrità delle reti e dell'infrastruttura degli apparati militari. L'industria delle armi, infatti, non può trascurare le possibilità offerte dall'alta tecnologia in questo settore: pochi paesi possono disporre della bomba atomica ma tutti possono sviluppare "armi cibernetiche". In questo settore operano, tra l'altro, anche aziende specializzate nel commerciare *software* spia in tutto il mondo, oppure nello svolgere indagini sul *web,* infiltrazione di gruppi digitali e *social media* o analisi dei *big data*. Tra le più note ve ne è, ad esempio, una che conta circa 350 persone sparse in tutto il mondo, di cui un centinaio tra linguisti e psicologi, oltre che uno zoccolo duro di ricercatori di sicurezza informatica e analisi forense, la cui missione è quella di esaminare gli attacchi informatici, ma anche di monitorare e, dove possibile, infiltrare gruppi di cybercriminali, mercenari al soldo di Stati e terroristi.

([27]) Di recente (14 settembre 2017), ad esempio, in Germania è stata istituita una nuova Agenzia ZITiS per la *cybersecurity* come parte di un tentativo centralizzato per affrontare la criminalità informatica e lo spionaggio digitale attraverso la sorveglianza delle telecomunicazioni di massa, la crittografia dei dati e la raccolta informazioni di massa. La ZITiS è un investimento importante, destinato a divenire una risorsa tecnologica a servizio di tutte le agenzie di sicurezza della Germania. Ma anche il governo finlandese ha presentato un disegno di legge per aumentare i poteri di sorveglianza antiterrorismo dell'*intelligence*: la legislazione attuale, infatti, non consente di monitorare le attività su *Internet* di potenziali criminali o terroristi prima che questi abbiano commesso un reato. Il nuovo provvedimento – che sarà discusso in Parlamento a breve – riguarderebbe i servizi di *intelligence* sia militari che civili e permetterebbe di condurre operazioni in patria e all'estero. La questione del monitoraggio delle attività su *Internet* è, tra l'altro, tornata di drammatica attualità proprio in queste ore a seguito degli attacchi terroristici di Barcellona del 17 agosto 2017 in merito al proselitismo, all'arruolamento e all'addestramenti di *kamikaze* sul *web.* Sul reclutamento terroristico tramite *web*, v. G. GIACOMELLO, *Rischi e minacce nel cyberspazio,* in P. FORADORI, G. GIACOMELLO (a cura di), *Sicurezza globale: le nuove minacce,* Bologna 2015, pp. 237-251. Sul tema in generale v. S. MELE, *Terrorism and the Internet: Finding a Profile of the Islamic Cyber Terrorist,* in studi ufficiali della *NATO Science for Peace and Security Series,* 2017.

([28]) È evidente, tuttavia, che l'esigenza di sicurezza in detto settore è globale; in tal senso, di particolare interesse, è la lettura del *«Global Cybersecurity Index»,* realizzato dall'*International Telecommunication Union,* ed. 2017, nel quale, tra le nazioni all'avanguardia, spiccano *Singapore* (che ha un approccio quasi perfetto alla sicurezza cibernetica, al contrario di molti altri paesi avanzati, che evidenziano diverse falle nei loro sistemi di difesa) e *Stati Uniti.* Nei restanti primi dieci posti si ritrovano Malesia, Oman, Estonia, Mauritius, Australia, Georgia, Francia e Canada. La Russia è all'11° posto. L'India è in 25^ posizione, un gradino sopra la Germania. L'I*talia* al 31° posto nel mondo e al 15° in Europa. La Cina, invece, staziona al 34° posto. Per approfondimenti, v. T. BRANT, *Singapore tops US for best cybersecurity,* in *http://fifthdomain.com,* 6 luglio 2017. Sul tema, tra l'altro, giova evidenziare come Singapore avrebbe superato nazioni come gli Stati Uniti, la Russia e la Cina diventando il Paese che lancia più attacchi informatici a livello mondiale. La valutazione proviene dalla società di sicurezza israeliana *«Check Point Software Technologies»* ed è stata ottenuta in base ai risultati di un proprio programma che segue mediamente da otto a dieci milioni di attacchi informatici in tempo reale. Tra l'altro, Singapore, che vuole diventare un centro tecnologico globale, ha recentemente intensificato anche gli sforzi per migliorare la sicurezza informatica dopo aver subito diversi attacchi di alto profilo ai danni delle sue agenzie governative e aziende.

(29) Xavier Bettel, Primo Ministro del Lussemburgo, Ministro delle comunicazioni e dei mezzi di comunicazione e Presidente del Consiglio, ha affermato: «Si tratta di un importante passo verso un approccio più coordinato alla cibersicurezza in Europa. Tutti gli attori, pubblici e privati, dovranno intensificare i loro sforzi, in particolare mediante una maggiore cooperazione tra gli Stati membri e obblighi di sicurezza più rigorosi per gli operatori di infrastrutture e i servizi digitali».

(30) In G.U. UE L 194/1 del 19.7.2016.

(31) In via di principio, con il concetto di "servizio pubblico", si fa riferimento ad attività di attribuzione di beni della vita suscettibili di valutazione patrimoniale, che, sebbene dirette a soddisfare esigenze essenziali per la collettività, si estrinsecano secondo modalità non autoritative. Tali sono, per esempio, la distribuzione del gas e dell'energia elettrica, il servizio elettrico, il servizio sanitario, il servizio idrico, i trasporti pubblici, la gestione dei rifiuti, i servizi telefonici, l'informazione radiotelevisiva, ecc. Nell'ambito di essi, rientra nella nozione di "servizi essenziali" quel complesso di attività prestate nei riguardi degli utenti per il soddisfacimento di bisogni collettivi. Nel campo del diritto pubblico italiano, la Costituzione disciplina i servizi pubblici denominati "essenziali" (art. 43 Cost.), prevedendo la possibilità di una riserva delle relative attività economiche in capo ai pubblici poteri. Vi sono, poi, i «servizi pubblici» definiti «essenziali» dalla l. n. 146/1990 per disciplinare le modalità di esercizio del diritto di sciopero (che annovera, tra gli altri, non solo i trasporti di linea, le poste, le telecomunicazioni e l'informazione radiotelevisiva pubblica, l'istruzione pubblica, la sanità, la raccolta e lo smaltimento dei rifiuti, l'approvvigionamento di energie, ma anche la protezione civile, l'amministrazione della giustizia, i servizi di protezione ambientale e di vigilanza sui beni culturali).
Il diritto europeo, invece, non reca le definizioni di "servizio pubblico" e di "servizi essenziali" ma prevede, nel Protocollo aggiuntivo al Trattato di Lisbona («Protocollo sull'esercizio della Competenza concorrente»), i «servizi d'interesse generale» (accanto ai «servizi di interesse economico generale» e «servizi non economici») assoggettati ad obblighi di servizio pubblico. I servizi di interesse generale designano attività soggette ad obblighi specifici di servizio pubblico proprio perché considerate di interesse generale dalla autorità pubbliche. Sotto questa voce si ritrovano sia attività di servizio non economico (sistemi scolastici obbligatori, protezione sociale, ma anche le funzioni inerenti alla potestà pubblica come la sicurezza, giustizia, la sanità, la difesa militare ed altro) ma si ritrovano anche attività di servizio cd. di interesse economico generale. I servizi di interesse economico generale, quindi, sono una specie del *genus servizi* di interesse generale; si tratta di servizi resi nell'ambito di un mercato concorrenziale, dove, quindi, si trovano ad operare soggetti privati, ma anche soggetti pubblici (tra cui le poste, le comunicazioni, i trasporti di linea, l'energia elettrica e il gas). In altri termini, l'UE non nega il concetto di pubblico servizio negli Stati membri, ma, come ha riconosciuto la Commissione, lo sviluppo dei servizi di interesse generale e il mantenimento di aree di attività economica in forma di pubblici servizi «sono essenziali al progresso della competitività europea, della solidarietà sociale e della qualità della vita dei cittadini» (Comunicazione della Commissione dell'11 settembre 1996, in G.U.C.E., n. C. 281 del 26 settembre 1996, 3. Per un'illustrazione dei contenuti v. il commento di N. RANGONE, in *Giornale di dir. amm.,* 1997, 4, 386).

(32) Per approfondimenti, v. L. FRANCHINA e A. LUCARIELLO, *Cybersecurity, Critical Infrastructures and States Behaviour,* in *www.ispionline.it* del 19 luglio 2017 e v. L. FRANCHINA, L. COLETTA, *La minaccia terroristica alla sicurezza e alle infrastrutture critiche nazionali. Un modello di analisi dei rischi,* in Rivista italiana di *intelligence*, n. 3/2016, p. 27 e ss.

(33) La direttiva è uno degli strumenti giuridici che le istituzioni europee possono utilizzare per attuare le politiche dell'UE. La direttiva viene adottata seguendo una procedura legislativa. Si tratta di un atto giuridico adottato dal Consiglio e dal Parlamento secondo procedure legislative ordinarie o speciali e costituisce uno strumento flessibile usato principalmente per armonizzare le leggi nazionali. Essa richiede ai paesi dell'UE di raggiungere determinati risultati, ma li lascia liberi di scegliere le modalità. La direttiva rientra nel diritto secondario dell'UE. Viene, pertanto, adottata dalle istituzioni dell'UE in conformità con i trattati costitutivi. Una volta adottata, viene recepita nel diritto nazionale dei paesi UE per poter essere applicata. Le direttive sono diverse dai regolamenti e dalle decisioni. A differenza del regolamento, applicabile nella legislazione nazionale dei paesi UE subito dopo la sua entrata in vigore, la direttiva non è direttamente applicabile nei paesi UE: deve prima essere trasposta nell'ordinamento nazionale affinché governi, aziende e individui possano farvi ricorso. Di contro, a differenza della decisione, la direttiva è un testo di applicazione generale per tutti i paesi dell'UE.

(34) Antecedentemente all'adozione delle direttiva in esame, gli operatori che gestivano infrastrutture critiche o fornivano servizi essenziali per il funzionamento della nostra società non erano soggetti ad obblighi appropriati quanto all'adozione di misure di gestione del rischio e allo scambio di informazioni con le autorità competenti. Pertanto, se da un lato le imprese non godevano di incentivi efficaci alla conduzione di una gestione seria del rischio che implicasse la sua valutazione e l'adozione di misure adeguate per garantire la sicurezza delle reti e

dell'informazione, dall'altro una larga parte di incidenti non era segnalata alle autorità competenti e passava inosservata (le informazioni sugli incidenti sono, invece, essenziali per permettere alle autorità pubbliche di reagire, adottare provvedimenti di mitigazione adeguati e fissare le opportune priorità strategiche per la sicurezza delle reti informatiche). A tal riguardo, si pensi che il quadro regolamentare previgente faceva obbligo soltanto alle compagnie di telecomunicazione di adottare misure di gestione del rischio di incidenti di sicurezza delle reti e dell'informazione e di segnalare questo tipo di anomalie. Era però evidente che esistevano anche molti altri settori dipendenti dal supporto delle reti informatiche, che avrebbero dovuto, quindi, essere coinvolti in materia di *cybersecurity*; settori in cui una serie di specifiche infrastrutture e fornitori di servizi erano particolarmente vulnerabili perché dipendenti fortemente dal corretto funzionamento delle reti e dei sistemi informativi. Questi settori, tuttavia, svolgevano e svolgono un ruolo essenziale nel fornire servizi fondamentali di supporto per la nostra economia e la nostra società. La sicurezza dei loro sistemi riveste un'importanza particolare per il funzionamento del mercato interno: si pensi, in particolare, alle banche, alle borse, alla generazione, trasmissione e distribuzione di energia, ai trasporti (aerei, ferroviari e marittimi), alla sanità, ai servizi *internet* e alle amministrazioni pubbliche.

([35]) La strategia per la cibersicurezza e la proposta di direttiva contribuiscono all'agenda digitale europea, intesa ad aiutare i cittadini e le imprese d'Europa ad ottenere il massimo dalle tecnologie digitali. Nel febbraio del 2013, l'Unione Europea si è dotata della sua prima *cyber-strategy*, al riguardo v. O. DE FRANCE, *A cyberstrategy for Europe. Now what about a strategy?,* in *ECFR's Blog,* 15 *February* 2013. L'obiettivo della strategia è dare vita a un ambiente cibernetico sicuro e affidabile, promuovendo e proteggendo i diritti fondamentali e altri valori costitutivi dell'UE. Lo scopo dichiarato della strategia è quello di contribuire a garantire – in collaborazione con gli altri attori nazionali e sovranazionali – un *cyber-spazio «open, safe and secure»*, nella certezza che le infrastrutture informative costituiscono oggigiorno la spina dorsale della crescita economica europea ed un importantissimo strumento per il benessere dei suoi cittadini. La strategia del 2013 mette in lapidaria evidenza come «Perché il ciberspazio rimanga aperto e libero è necessario che nell'ambiente *online* si applichino le stesse norme, gli stessi principi e gli stessi valori che l'Unione europea difende *offline*. Occorre tutelare nel ciberspazio i diritti fondamentali, la democrazia e lo Stato di diritto. La nostra libertà e la nostra prosperità dipendono sempre più dalla solidità e dall'innovazione di *Internet,* che continuerà a fiorire a patto che l'innovazione del settore privato e la società civile ne guidino la crescita. Ma la libertà *online* presuppone la sicurezza. È necessario che il ciberspazio sia protetto da incidenti, attività dolose e abusi: gli Stati hanno un ruolo decisivo nella garanzia della libertà e della sicurezza del ciberspazio. I loro compiti sono numerosi: salvaguardare l'apertura e l'accessibilità, rispettare e proteggere i diritti fondamentali *online* e preservare l'affidabilità e l'interoperabilità di *Internet*. D'altro canto, il settore privato è proprietario e fa funzionare quote notevoli di ciberspazio, per cui la riuscita di qualsiasi iniziativa in questo settore presuppone il riconoscimento del suo ruolo motore. La tecnologia dell'informazione e delle comunicazioni è diventata la spina dorsale della crescita economica e una risorsa critica da cui dipendono tutti i settori dell'economia: oggi queste tecnologie sono alla base dei sistemi complessi che fanno funzionare le nostre economie in settori essenziali come la finanza, la sanità, l'energia e i trasporti, mentre molti modelli di impresa si fondano sulla disponibilità ininterrotta di *Internet* e sul corretto funzionamento dei sistemi informativi. […]». La visione dell'UE delineata in detta strategia si articola intorno a cinque priorità strategiche per affrontare le sfide sopra descritte: raggiungere la ciberresilienza, ridurre drasticamente il cibercrimine, sviluppare una politica e capacità di ciberdifesa connesse alla Politica di Sicurezza e di Difesa Comune (PSDC), sviluppare le risorse industriali e tecnologiche per la cibersicurezza, creare una politica internazionale coerente dell'Unione europea sul ciberspazio e promuovere i valori costitutivi dell'UE. Essa prevede altresì la necessità di rafforzare gli investimenti in ricerca e sviluppo (R&S) e innovazione. In particolare, la R&S può essere il supporto di una politica industriale forte, utile a promuovere un settore europeo delle tecnologie dell'informazione e della comunicazione (TIC) affidabile, a dare impulso al mercato interno e ridurre la dipendenza europea dalle tecnologie straniere: in tal senso, le università e i centri di ricerca svolgono un ruolo determinante nell'incentivare la ricerca, lo sviluppo e l'innovazione in tali settori. La R&S dovrebbe ovviare alle lacune tecnologiche della sicurezza delle TIC, prepararci ad affrontare le sfide di sicurezza di nuova generazione, tenendo conto della costante evoluzione delle esigenze degli utenti, e sfruttare i vantaggi delle tecnologie a doppio uso. Essa dovrebbe anche continuare a supportare lo sviluppo della crittografia; a ciò devono aggiungersi iniziative per tradurre i risultati della R&S in soluzioni commerciali, grazie ai necessari incentivi e alla creazione delle condizioni politiche favorevoli. Ulteriore obiettivo della strategia in questione è quello di promuovere il dialogo e il coordinamento tra gli attori civili e militari nell'UE, con particolare riferimento allo scambio di buone pratiche e di informazioni, ai preallarmi, alla risposta agli incidenti, all'analisi del rischio, alla sensibilizzazione e alla prioritarizzazione della cibersicurezza nonché di curare il dialogo con i *partner* internazionali, in particolare la NATO, con altre organizzazioni internazionali e centri di eccellenza multinazionali, per garantire capacità efficaci

di difesa, individuare settori di cooperazione ed evitare duplicazioni degli sforzi. A ben vedere, quello del 2013 non è né il primo né l'ultimo atto con cui l'Unione europea si è interessata alle problematiche inerenti alla sicurezza informatica e delle informazioni. Da ultimo, ad esempio, durante il recente discorso sullo Stato dell'Unione tenuto il 13 settembre 2017, il presidente della Commissione europea Jean-Claude Juncker ha annunciato una serie di importanti misure (l'iniziativa consiste in una raccomandazione, due comunicazioni, una proposta di regolamento e una proposta di direttiva) in materia di sicurezza cibernetica contenute nella comunicazione congiunta «*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*» JOIN(2017) 450 *final* del 13 settembre 2017 (ma v. anche, *Commission staff working document assessment of the EU 2013 cybersecurity strategy,* SWD(2017) 295 *final* del 13 settembre 2017), la quale si pone tre obiettivi principali per far fronte a un numero crescente di attacchi malevoli verso i sistemi informatici europei (per approfondimenti, v. T. DE ZAN, *I piani della commissione UE per la* cyber-security, in *Airpres,* ottobre 2017, p. 30, T. DE ZAN, *Deterring "bad hombres": the EU cyber diplomatic toolbox,* C. GIUSTOZZI, *Una nuova Agenzia* Cyber *per l'Europa*, L. MARTINO, *Ue e* cybersecurity*: un nuovo approccio strategico,* M. MENSI, *Cybersecurity and the European digital market,* F. RUGGE, Cybersecurity: *l'ora dell'Europa*, F. RUGGE, *Nato o UE: l'importante è fare squadra*, A. SOI, Information Warfare*: la risposta europea,* tutti in *Osservatorio Cybersecurity dell'ISPI* dell'ottobre 2017). Come primo obiettivo l'UE propone una serie di misure per rafforzare la resilienza dell'Unione dagli attacchi cibernetici, quali la proposta legislativa per far dell'ENISA la nuova Agenzia di sicurezza cibernetica europea, la creazione di un *framework* europeo di certificazione per la sicurezza cibernetica di prodotti e servizi e la creazione di un Centro europeo di ricerca in materia di *cybersecurity* e competenze sulla sicurezza cibernetica, che l'UE vorrebbe rendere operativo a partire dal 2018 a fronte di un investimento iniziale immediato di 50 milioni di euro. Il secondo obiettivo dell'UE è la creazione di una deterrenza efficace verso attori statali e non. In questo ambito, viene incoraggiata la diffusione del nuovo protocollo "IPv6", che assegna un singolo indirizzo IP all'utente, che darebbe dei benefici immediati agli organi di polizia impegnati in investigazioni *online* e contestualmente viene portato avanti il lavoro di implementazione relativo al *"cyber diplomacy toolbox"*, attraverso il quale l'UE prevede di poter prendere delle decisioni, come ad esempio le sanzioni, nel contesto della Politica di sicurezza e difesa comune (PSDC) in caso di attacchi informatici provenienti da attori statali stranieri. Infine, il terzo obiettivo dell'UE è il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica. L'Unione si prefigge di fare ciò attraverso nuove e vecchie alleanze, dando priorità agli aspetti di sicurezza in fora dedicati come i cd. "dialoghi cibernetici" e mediante il *"cybersecurity capacity building"* che mira a rafforzare capacità tecnologiche e umane di paesi del vicinato e in via di sviluppo tecnologico. Andando a ritroso deve altresì evidenziarsi come l'UE ha deciso di dare una risposta diplomatica comune ai *cyber* attacchi e lo farà con un "pacchetto di strumenti di diplomazia informatica" come si legge nelle «Conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose» del 19 giugno 2017, in *http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/it/pdf,* dal quale emerge come l'UE ha riconosciuto che il *cyber* spazio è sì una fonte di grandi opportunità, ma contemporaneamente pone anche una serie di grandi sfide. C'è infatti il pericolo crescente di azioni informatiche dolose da parte di attori statali e non statali che possono costituire atti illeciti ai sensi del diritto internazionale. L'UE è però pronta a reagire e ribadisce che gli Stati non dovrebbero consentire consapevolmente l'utilizzo dei rispettivi territori per atti illeciti a livello internazionale, compiuti mediante l'uso delle tecnologie dell'informazione e della comunicazione. Ma, andando a ritroso, la sicurezza del *cyberspace* ha altresì trovato riconoscimento nella comunicazione 5.7.2016 COM(2016) 410 *final* della Commissione UE, recante «*Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*» e ancor prima nella classificazione delle minacce ibride di cui alla Comunicazione congiunta al Parlamento europeo e al Consiglio 6.4.2016 *JOIN*(2016) 18 *final,* relativa al «*Joint Framework on countering hybrid threats a European Union response*» (par. 4.4). Nel novembre 2014 la Commissione europea ha rilasciato un *«Cyber Defense Policy Framework»* con l'intento di chiarire agli Stati Membri quale dovrebbe essere la strada per arrivare ad avere una *«Common Security and Defense Policy»* (CSDP), sulla quale v. anche, *Cybersecurity in the EU Common Security and Defence Policy - Challenges and risks for the EU,* dell'*European Parliamentary Research Service,* maggio 2017. In altre parole, si tratta un insieme di pratiche e *policy* condivise che possano, a livello sistemico e non di singoli attori, fornire un contributo reale in termini di difesa cibernetica nazionale. Il documento ha ribadito diversi concetti importanti che sono anche alla base della direttiva NIS in rassegna. Antecedentemente a questi atti, inoltre, si rinvengono altri documenti ufficiali, quali, in ordine cronologico, la COM(2001)298, ossia il *«Communication Network and Information Security: proposal for a European Policy Approach»* del 2001, documento con il quale la Commissione aveva sottolineato la necessità di innalzare il livello comune di consapevolezza nel campo della *network and information security*. I predetti atti a loro volta furono seguiti dalla COM(2006) 251, recante *«Strategy for a Secure Information Society»* del 2006, i cui elementi principali sono stati approvati dalla risoluzione del Consiglio 2007/068/01 e dalla COM(2009)149, recante *«Protecting Europe from*

large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience», del 2009, che rappresenta un primo modello di *action plan* per la protezione delle infrastrutture critiche dalle minacce provenienti dal *cyber-spazio,* incentrata sulla protezione dell'Europa contro le ciberperturbazioni attraverso il rafforzamento della sicurezza. La comunicazione ha avviato un piano di azione destinato a rafforzare i provvedimenti degli Stati membri in materia di prevenzione e risposta. Detto piano di azione è stato approvato dalle conclusioni della Presidenza della conferenza ministeriale sulla protezione delle infrastrutture critiche informatizzate svoltasi a Tallinn nel 2009. Il 18 dicembre 2009, il Consiglio ha adottato la risoluzione 2009/C 321/01 su «Un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione». Ad esse ha fatto seguito la COM(2010) 245, relativa all'Agenda digitale europea. Di particolare rilievo è altresì la COM(2011)163 relativa alla protezione delle infrastrutture critiche informatizzate, recante *«Achievements and next steps: towards global cyber-security»*, nella quale la Commissione, dopo aver analizzato i risultati conseguiti in seguito all'adozione del piano di azione sulla protezione delle infrastrutture critiche informatizzate del 2009, ha concluso che l'attuazione del piano ha dimostrato l'insufficienza di un approccio esclusivamente nazionale per far fronte alle sfide della sicurezza e della resilienza e ha sottolineato l'opportunità di portare avanti, in Europa, gli sforzi destinati a costruire un approccio coerente e cooperativo nell'UE. Nelle conclusioni del 27 maggio 2011 sulla protezione delle infrastrutture critiche informatizzate, il Consiglio dell'Unione europea ha poi sottolineato l'urgente necessità di rendere i sistemi TIC e le reti resilienti e sicuri nei confronti di qualsiasi turbativa possibile, accidentale o intenzionale, per elevare il livello di preparazione, sicurezza e capacità di resilienza nell'UE, rafforzare le competenze tecniche per permettere all'Europa di raccogliere la sfida della protezione delle reti e delle infrastrutture informatiche e intensificare la cooperazione tra Stati membri, sviluppando meccanismi di cooperazione reciproca in caso di incidenti. Sul piano della creazione di apposite strutture preposte all'attività in questione è altresì da segnalare il Regolamento (CE) n. 460/2004 con il quale l'allora Comunità europea ha istituito, nel 2004, l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), allo scopo di contribuire a garantire un elevato livello di protezione e allo sviluppo di una cultura della sicurezza delle reti e dell'informazione nell'UE. E, ancora, il 28 marzo 2012 la Commissione ha adottato la COM(2012)140, relativa all'istituzione di un Centro europeo per la lotta alla criminalità informatica (EC3). Il centro, istituito l'11 gennaio 2013, fa parte dell'Ufficio europeo di polizia (*Europol*) ed è il punto focale della lotta contro la cibercriminalità nell'UE. EC3 è destinato a raggruppare le competenze europee in materia di cibercriminalità per aiutare gli Stati membri a rafforzare le loro capacità, per fornire loro assistenza nelle indagini contro il cibercrimine, in stretta collaborazione con *Eurojust,* diventando il portavoce degli investigatori europei sulla criminalità informatica a livello di autorità di contrasto e giudiziarie.

([36]) V. Commissione europea, «*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace», (JOIN(2013)1),* 7 *February* 2013, v. anche Doc. 6225/13.

([37]) V. Doc. 11357/13.

([38]) A mente del quale: «1. La delimitazione delle competenze dell'Unione si fonda sul principio di attribuzione. L'esercizio delle competenze dell'Unione si fonda sui principi di sussidiarietà e proporzionalità. 2. In virtù del principio di attribuzione, l'Unione agisce esclusivamente nei limiti delle competenze che le sono attribuite dagli Stati membri nei trattati per realizzare gli obiettivi da questi stabiliti. Qualsiasi competenza non attribuita all'Unione nei trattati appartiene agli Stati membri. 3. In virtù del principio di sussidiarietà, nei settori che non sono di sua competenza esclusiva l'Unione interviene soltanto se e in quanto gli obiettivi dell'azione prevista non possono essere conseguiti in misura sufficiente dagli Stati membri, né a livello centrale né a livello regionale e locale, ma possono, a motivo della portata o degli effetti dell'azione in questione, essere conseguiti meglio a livello di Unione. Le istituzioni dell'Unione applicano il principio di sussidiarietà conformemente al protocollo sull'applicazione dei principi di sussidiarietà e di proporzionalità. I parlamenti nazionali vigilano sul rispetto del principio di sussidiarietà secondo la procedura prevista in detto protocollo. 4. In virtù del principio di proporzionalità, il contenuto e la forma dell'azione dell'Unione si limitano a quanto necessario per il conseguimento degli obiettivi dei trattati. Le istituzioni dell'Unione applicano il principio di proporzionalità conformemente al protocollo sull'applicazione dei principi di sussidiarietà e di proporzionalità».

([39]) La direttiva, infatti, impone agli Stati membri condizioni che corrispondono a quanto è strettamente necessario per raggiungere un livello adeguato di preparazione e permettere una collaborazione basata sulla fiducia. Questo consente agli Stati membri di tenere nella debita considerazione le peculiarità nazionali e garantisce che i principi comuni dell'UE siano applicati in maniera proporzionata. Il vasto campo di applicazione consentirà agli Stati membri di attuare la direttiva tenendo conto dei reali rischi che affrontano a livello nazionale, come individuati nella strategia nazionale in materia di sicurezza delle reti informatiche. Gli obblighi di attuazione della gestione del rischio riguardano solo entità critiche e impongono misure proporzionate ai rischi. Gli obblighi di segnalazione, ad

esempio, riguarderebbero solo incidenti aventi un impatto significativo. Inoltre, le misure non imporrebbero costi sproporzionati perché la normativa vigente in materia di protezione dei dati già impone a molte delle suddette entità, in veste di responsabili del trattamento dei dati, l'obbligo di garantire la tutela dei dati personali. A tal fine, per evitare di imporre oneri sproporzionati ai piccoli operatori, gli obblighi sono proporzionati al rischio corso dalla rete o dal sistema informativo di cui si tratta e non si applicano alle microimprese. I rischi dovranno essere individuati in primo luogo dalle entità assoggettate a tali obblighi, le quali dovranno decidere le misure di mitigazione del rischio da adottare.

(40) Questi soggetti dovranno essere identificati direttamente da ogni Stato membro, all'interno dei seguenti ambiti: energia, trasporti, banche e società finanziarie, salute, acqua e infrastrutture digitali. I criteri che determineranno quali enti saranno inclusi in questa lista sono: l'essenzialità del servizio offerto per il mantenimento di attività critiche in ambito economico e sociale; la dipendenza del servizio da sistemi informatici; il rischio di effetti gravi e significativi che l'incidente di sicurezza può avere sulla fornitura di un servizio essenziale.

(41) Quali: prevenzione dei rischi, garanzia della sicurezza dei sistemi, delle reti e delle informazioni, e capacità di gestione degli incidenti.

(42) Definita dall'art. 4 come «la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi».

(43) La presente direttiva lascia impregiudicata la possibilità per ciascuno Stato membro di adottare le misure necessarie per assicurare la tutela degli interessi essenziali della sua sicurezza, salvaguardare l'ordine pubblico e la pubblica sicurezza e consentire la ricerca, l'individuazione e il perseguimento dei reati. Conformemente all'articolo 346 del Trattato sul funzionamento dell'Unione europea (TFUE), nessuno Stato membro è comunque tenuto a fornire informazioni la cui divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza nazionale.

(44) La direttiva in esame si applica soltanto a quei soggetti pubblici (cfr. art. 4, punto 4), che sono identificati come operatori di servizi essenziali (cfr. art 5, par. 2). Spetta, pertanto, agli Stati membri garantire la sicurezza delle reti e dei sistemi informativi dei soggetti pubblici che non rientrano nel campo di applicazione della direttiva NIS (cfr. anche *infra* nota 47).

(45) Al riguardo, giova rilevare che è possibile che soggetti che operano nei settori e sotto-settori di cui alla direttiva forniscano sia servizi essenziali che non essenziali. Nel settore del trasporto aereo, ad esempio, gli aeroporti forniscono servizi che potrebbero essere considerati essenziali da uno Stato membro, come la gestione delle piste, ma anche una serie di servizi che potrebbero essere considerati non essenziali, come l'allestimento di aree commerciali. Gli operatori di servizi essenziali dovrebbero essere soggetti a specifici obblighi di sicurezza solo in relazione ai servizi considerati essenziali. Ai fini dell'identificazione degli operatori, gli Stati membri dovrebbero, pertanto, definire un elenco di servizi considerati essenziali. Inoltre, ai fini del processo di identificazione, è opportuno che, nel caso in cui un soggetto fornisca un servizio essenziale in due o più Stati membri, tali Stati membri intraprendano discussioni bilaterali o multilaterali tra di loro. Questo processo di consultazione è inteso ad aiutarli a valutare la natura critica dell'operatore in termini di impatto transfrontaliero, consentendo in tal modo a ciascuno degli Stati membri interessati di presentare la propria posizione in merito ai rischi connessi ai servizi forniti. Gli Stati membri interessati dovrebbero, quindi, tener conto delle rispettive posizioni in tale processo e dovrebbero poter chiedere l'assistenza del gruppo di cooperazione preposto.

(46) Giova rilevare che gli attacchi informatici possono interessare anche il settore marittimo. A tal proposito, per rispondere a questa minaccia, una *joint venture* industriale composta da alcune realtà di settore – Bimco, Ocimf, Iumi, Clia, Ics, Intercargo e Intertanko – ha elaborato *«The Guidelines on cyber security board ship», Version 1.1, February* 2016, concernenti la *cybersecurity* a bordo delle navi. Il documento, giunto alla sua seconda edizione, fornisce suggerimenti su come proteggersi dagli *hackers* incrementando le difese di reti e sistemi o stipulando polizze assicurative dedicate. I consigli si concentrano anche sulla gestione della sicurezza informatica durante le comunicazioni con le autorità costiere e i porti. Di recente anche il Comando generale del Corpo delle Capitanerie di porto ha adottato la circolare n. 35 del 7 aprile 2017, al fine di avviare il censimento del livello di *security* della flotta e delle compagnie, riferita al *"Cyber risk management"*. Sui crescenti rischi in tale settore, v. F. CHIAPPETTA, *La gestione dei rischi marittimi informatici alla luce delle linee guida pubblicate dall'IMO,* in *Rivista Marittima Ottobre 2016,* 53 e ss., con ampia casistica, tra la quale emerge quella concernente il famoso caso del porto di Anversa del 2013, in cui *hackers* vicini a organizzazioni criminali dedite al traffico di droga hanno ripetutamente violato i sistemi di tracciamento digitali di *containers,* inserendosi nei sistemi informatici del porto belga e consentendo lo sbarco di droga (cocaina e eroina) come se fosse stata merce qualsiasi, indirizzando poi il trasporto terrestre verso

autotrasportatori complici. Di recente anche paesi emergenti come l'India stanno puntando ad incrementare la *cybersecurity* dell'industria navale. Il Registro nazionale dello *Shipping (IRClass)* ha ad esempio introdotto una serie di regole per prevenire i rischi di *cyber* attacchi verso l'intero settore dei trasporti navali. Le nuove norme si basano su quelle della «*International Maritime Organization (IMO)*» e sugli *standard* interni e internazionali, come quello del «*National Institute of Standards and Technology – US Department of Commerce (NIST)*». Per quanto concerne l'IMO in particolare, essa, con la pubblicazione di linee guida sulla gestione dei *cyber* rischi in ambito marittimo, ha ribadito che la *cybersecurity* sulle navi è fondamentale per garantire la tutela e sicurezza dello *shipping* a livello globale. Il documento dell'IMO è conseguente a un'altra pubblicazione di questo tipo: il «*Maritime Cyber Risk Management in Safety Management Systems*», adottato a giugno del 2017. Quest'ultimo era stato compilato dopo che le due campagne *malware*, *"WannaCry"* e *"PetYa"*, avevano prodotto danni molto ingenti a tutto il comparto che, per la prima volta, è stato attaccato dal *cybercrime* in modo massiccio e violento. Di conseguenza, si è reso necessario aggiornare tutti i meccanismi di difesa cibernetica dai pericoli provenienti dal *cyberspace* e rivolti verso i sistemi critici sia delle navi sia a terra.

([47]) A ben vedere, in questo caso la direttiva in esame parla di «organismi pubblici» in un contesto nel quale la locuzione sembrerebbe fare riferimento a soggetti perlopiù istituzionali pubblici e, comunque, ad entità diverse dal «soggetto pubblico» di cui, invece, parla l'articolo 4, punto 4, che, se letto in combinato disposto con i soggetti elencati nell'allegato II della direttiva, sembrerebbe invece riferibile più ad un operatore (es. impresa pubblica) di servizi. Al riguardo, mi sembra di poter affermare che detta locuzione possa ritenersi non corrispondente a quella di «organismo di diritto pubblico» (che, semmai, potrebbe invece ricomprendere le due categorie anzidette: «organismi pubblici» e «soggetto pubblico»), la cui definizione è ad oggi contenuta nell'art. 3, co. 1, lett. d) del d.lgs. n. 50 del 18 aprile 2016 (cd. "Nuovo codice degli appalti"), il quale riproduce fedelmente il contenuto delle direttive 2014/23/UE, 2014/24/UE e2014/25/UE del 26 febbraio 2014, a loro volta confermative del precedente assetto normativo di cui alle direttive n. 17 e 18/2004. Ai sensi della su citata normativa, rientrano nella nozione di organismo di diritto pubblico gli enti dotati di personalità giuridica che siano stati istituiti per soddisfare specificatamente esigenze di interesse generale, aventi carattere non industriale o commerciale, e che risultano altresì sottoposti ad un'influenza pubblica, in quanto finanziati per la maggior parte dallo Stato, dalle autorità regionali o da altri organismi di diritto pubblico; ovvero, la loro gestione è posta sotto la vigilanza di tali autorità o organismi; ovvero, ancora, il loro organo di amministrazione, di direzione o di vigilanza è costituito da membri, più della metà dei quali è designata da autorità regionali o locali o da altri organismi di diritto pubblico. Trattasi di requisiti non alternativi da loro, ma cumulativi, in quanto, per potersi definire un soggetto come un organismo di diritto pubblico, occorre la loro necessaria compresenza. In particolare, in relazione al requisito del possesso di personalità giuridica (nel corso degli anni infatti la definizione originaria è contenuta nell'art. 3, n. 26 del d.lgs. 12 aprile 2006), ci si è chiesti se nella nozione di «organismo di diritto pubblico» possano farsi rientrare, oltre le persone giuridiche di diritto pubblico, anche quelle di diritto privato. La Corte di giustizia si è da sempre espressa nel senso dell'indifferenza della forma giuridica di diritto interno. Parimenti, sul versante domestico, risulta ormai prevalente la tesi cd. "funzionale", in forza della quale devono considerarsi organismo di diritto pubblico tutti gli enti, compresi anche quelli aventi forma societaria privata, che posseggono i requisiti previsti dalla norma.

([48]) Per approfondimenti, con particolare riferimento al collegamento tra la direttiva NIS e il «Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica» (PN), v. F. LAZZINI, *Come evolverà il ruolo dei CERT con la Direttiva Nis, in www.cyberaffairs.it, 29 luglio 2017*.

([49]) In tal senso, ENISA, *National Cyber Security Strategies. Practical Guide on Development and Execution,* December 2012, in *http://europa.eu/!gC63Tk*.

([50]) Per approfondimenti sugli accordi internazionali in generale, v. *funditus,* B. CONFORTI, *Diritto internazionale,* VII, Napoli, Editoriale scientifica, 2006, pp. 71, 379 e 404.

([51]) Un lungimirante esempio, sebbene tra Stati non appartenenti all'UE, è da rinvenirsi nel recente accordo tra Turchia e Qatar per lo sviluppo di soluzioni *cyber*. In particolare, il Consiglio per la ricerca scientifica e tecnologica della Turchia (Tubitak) e il *Qatar National Research Fund* implementeranno un capitolo dedicato alla sicurezza informatica nell'accordo di cooperazione già siglato dalle due parti a dicembre del 2015. I primi progetti, sembra, si concentreranno sulla difesa di infrastrutture critiche nei settori bancario, delle comunicazioni ed energetico, cfr. *www.cyberaffairs.it, 12 agosto 2017. Con particolare riferimento al Qatar, g*iova segnalare un altro esempio che in linea di principio potrebbe essere seguito, ossia la recente ed interessante iniziativa di costituzione del cd. "Alto comitato *cyber*" che sarà formato da tutti i settori del Paese (dal governo alle industrie, passando per militari, universitari,

mondo finanziario e società civile. Al suo interno ci saranno sotto-comitati per ogni tematica e avrà una serie di sotto commissioni: una per ogni tematica della *information security*) con il compito di definire politiche e programmi nell'ambito della strategia per la *information security*. Inoltre, lavorerà per rafforzare i *firewall* contro le minacce informatiche.

([52]) Ai sensi dell'art. 4, punto 4, si definisce «operatore di servizi essenziali» un soggetto pubblico o privato che soddisfa i seguenti criteri: un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

([53]) Ai sensi dell'art. 4, punti 5 e 6, si definisce «fornitore di servizio digitale» qualsiasi persona giuridica che fornisce un servizio digitale, ossia un servizio ai sensi dell'articolo 1, par. 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio di un tipo elencato nell'allegato III della direttiva in esame (mercato *online,* motore di ricerca *online* e servizi di *cloud computing*). I fornitori di servizi digitali operano solitamente in più Stati membri. Per garantire che siano trattati in modo analogo in tutta l'UE, le norme si applicheranno a tutti gli operatori che offrono tali servizi, con l'esclusione delle piccole imprese.

([54]) Sul delicato argomento della possibilità di applicare sanzioni per chi non attua misure di *cybersecurity*, v. *UK, proposte sanzioni per chi non attua misure di cyber security,* in *www.cyberaffairs.it, 12 agosto 2017, al riguardo, osserva S. MELE, «*l'idea del governo britannico, infatti, è quella di allineare la risposta sanzionatoria per mancata applicazione delle previsioni della Direttiva a quella prevista nel Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea. Fino a 10 milioni di euro o il 2% del fatturato globale per le violazioni minori della Direttiva, come, ad esempio, la mancata cooperazione con l'autorità competente o la mancata denuncia di un incidente di sicurezza. Fino a 20 milioni di euro o il 4% del fatturato per le violazioni considerate più rilevanti, come, ad esempio, la mancata applicazione delle misure di sicurezza considerate adeguate e proporzionali. Misure di sicurezza che, peraltro, sono ben delineate nei loro principi guida di alto livello all'interno dell'allegato 3 al testo proposto in consultazione […]. Occorre evidenziare come questo potenziale allineamento sanzionatorio con la normativa europea in materia di protezione dei dati personali proposto dal governo britannico non può che essere considerato positivamente per numerose ragioni. La prima è senz'altro legata ai destinatari della Direttiva NIS ovvero principalmente agli operatori dei servizi essenziali. Si tratta, quindi, delle principali realtà economiche del Paese, la cui protezione delle informazioni – anche attraverso l'imposizione di sanzioni elevate – risulta fondamentale soprattutto in considerazione delle possibili ricadute negative di eventuali incidenti informatici, finanche sui cittadini. La seconda è legata alla sempre più evidente congiunzione tra dati personali e informazioni pregiate sottratte alle aziende strategiche nazionali. La terza, infine, è legata ad una semplificazione e coerenza globale della normativa in materia di protezione delle informazioni – siano esse dati personali o meno – che passa ovviamente anche attraverso una armonizzazione delle sanzioni comminabili».

([55]) Al riguardo, e con particolare riferimento a norme incriminatrici, è da notare come si debba escludere che le fonti normative dell'ordinamento europeo – per tale intendendosi il complesso di norme giuridiche elaborate dalla istituzioni dell'Unione europea (*i.e.* regolamenti, direttive e decisioni), dei principi di diritto elaborati dalla Corte di Giustizia delle Comunità europee e delle fonti europee convenzionali – possano autonomamente introdurre nuove disposizioni incriminatrici valevoli in ambito interno. La preclusione dell'emanazione di norme che introducono nuovi reati poggia essenzialmente su un *deficit* di democraticità che caratterizza la struttura europea, la quale, in un settore particolarmente delicato in cui vengono operate scelte politiche destinate ad incidere sulla libertà personale, impone un preciso limite all'ambito di produzione normativa che non può che riguardare soprattutto la previsione di nuove incriminazioni. Invero, in ambito europeo, la potestà di emanare atti normativi, dal carattere *lato sensu* legislativo, spetta prevalentemente al Consiglio UE, organo composto da soggetti rappresentanti dei Governi degli Stati membri, mentre al Parlamento, unico e vero organo di legittimazione democratica, i cui membri vengono eletti da cittadini dell'Unione, spetta una ridotta potestà normativa. In tal senso, si ricordi che il fondamento del monopolio penale in capo al Parlamento risiede nel dogma, di stampo illuministico, e che ha pervaso pressoché tutte le legislazioni occidentali, che solo il popolo può legiferare contro se stesso. Inoltre, in tutta la normativa dell'UE non è dato rinvenire alcuna disposizione che faccia riferimento al potere di uno degli organi istituzionali di emanare norme incriminatrici con efficacia diretta negli ordinamenti interni degli Stati membri; quindi, vista la particolare delicatezza della materia, il Trattato istitutivo della Comunità europea, nella sua formulazione originaria, ovvero successiva, avrebbe dovuto prevedere, in ossequio ad un principio di garanzia e cautela, una norma generale di tale tenore; norma che oggi non si rinviene neanche nel «Trattato sul funzionamento dell'Unione europea». In tal senso, non sembra nemmeno possa farsi ricorso all'art. 261 TFUE nella parte in cui fa riferimento alla possibilità per i Regolamenti di prevedere «sanzioni»: tale norma, infatti, si ritiene comunemente (e in mancanza di un'espressa

previsione ed alla luce dei principi appena esposti) faccia riferimento alla possibilità di introdurre sanzioni che non possano avere carattere penale, ma solo amministrativo.

(56) L. RAMPONI, *Minaccia cyber è vero pericolo per Italia ed Europa, in www.cyberaffairs.it, 25 marzo 2017. Lo stesso autore mette in rilievo come «*Tale minaccia esiste già da parecchi anni e viene sviluppata dalla criminalità, dallo spionaggio economico, industriale, diplomatico, politico o bellico, dal terrorismo, sino a delineare la possibilità di una autentica *cyberwar.* Essa investe tutto il sistema Italia ed Europa e può colpire capillarmente tutti i livelli della società, sino al singolo individuo […] è facilmente intuibile come, la messa a punto di una tale organizzazione difensiva unitaria da parte Europea, costituisca un fatto di grande rilevanza politica, dal momento che, per la prima volta, l'Unione metterebbe a punto una organizzazione difensiva completamente integrata sotto la sua egida».

(57) V. *supra* paragrafo 3.

(58) Sul punto, giova evidenziare che, con riguardo alle norme delle direttive, a partire dalla sentenza 6 ottobre 1970, *causa 9/70, Franz Grad c. Finanzamt Traunsteins,* la Corte di Giustizia ha individuato, quali condizioni indefettibili per il prodursi di effetti diretti: la chiarezza, precisione e completezza delle norme; l'assenza di qualsiasi condizione alla loro efficacia; l'inutile decorso del termine per la recezione a livello nazionale, purché invocati in rapporti verticali, cioè per l'attribuzione ai singoli di diritti nei confronti dello Stato o nei confronti di organismi o enti soggetti all'autorità o al controllo dello Stato, ma non anche in rapporti orizzontali, vale a dire tra soggetti privati. Sugli effetti diretti delle norme contenute nei diversi atti europei, v. G. PISTORIO, *Interpretazione e giudici. Il caso dell'interpretazione conforme al diritto dell'Unione europea,* Napoli, 2012, 136 ss. Sugli effetti diretti sul piano amministrativo, v. M. CLAES, *The National Courts' Mandate in the European Constitution,* Oxford, 2005, *passim.* Sul punto, v. CGCE, 28 giugno 2001, C-118/00, *Larsy; Id.,* Sent. 9 settembre 2003, C-198/01, *Consorzio Industrie Fiammiferi; Id.,* CGCE, 29 aprile 1999, C-224/97, *Ciola; Id.,* 4 dicembre 1997, Cause riunite C-258/96 e C-253/96, *Kampelmann, Id.,* 3 ottobre 2002, causa C 347/00, *Barreira Pérez; Id.,* 13 gennaio 2004, causa C-453/00, *Kühne & Heitz; Id.,* 17 febbraio 2005, cause riunite C 453/02 e C 462/02, *Linneweber e Akritidis, Id.,* 12 giugno 2005, Cause riunite C-453/03, C-11/04, C-12/04 e C-194/04, *Fratelli Martini e Cargill, Id.,* 6 marzo 2007, causa C 292/04, *Meilicke e a.; Id.,* 12 febbraio 2008, C-2/06, *Kempter.*

(59) Di recente, il Ministro della difesa, Sen. Roberta Pinotti, intervenendo al Convegno organizzato a Roma il 15 giugno 2017 dalla delegazione italiana presso l'Assemblea parlamentare della NATO in collaborazione con il Centro studi americani, ha evidenziato che «non dobbiamo restare indietro e accontentarci di raggiungere la semplice capacità di sopravvivenza a un'aggressione cibernetica. Per prevenire, servono investimenti e attenzione politica. […]. Nell'ambito dei poteri dello Stato, la difesa ha la specifica responsabilità di operare nel particolare "dominio" dei conflitti armati che hanno una loro dimensione cibernetica. Nella dimensione internazionale, dobbiamo contribuire a una sicurezza condivisa, che non potrà prescindere dalla sicurezza degli spazi cibernetici. La decisione presa in ambito NATO di elevare lo spazio cibernetico a "dominio delle operazioni" vuol dire che questa sfera della sicurezza è già ora una responsabilità condivisa a livello multinazionale». Il Ministro ha altresì rilevato che «serve il lavoro di ciascuno di noi in ogni settore, proprio per la complessità della minaccia, e serve che l'attenzione complessiva dell'opinione pubblica faciliti quelle scelte di investimenti che la politica sente necessarie e che in questo campo sicuramente devono andare avanti. […]. Il cosiddetto "virtuale" diventato paradossalmente più reale del reale, sempre più centrale per la nostra quotidianità, per la nostra sicurezza, per la qualità della nostra vita sia come singoli individui che come comunità nazionale e internazionale». Ciò comporta, ha aggiunto il Ministro, tutta una serie di rischi, da quelli «più direttamente percepiti dagli individui, come la tutela della *privacy,* alla minaccia di eventi persino catastrofici, come il sabotaggio informatico delle infrastrutture critiche, passando per la dimensione immateriale della conoscenza e della percezione degli eventi come i pericoli di interferenza nei processi elettorali […]. Nel cyberspazio, tra monete non tracciabili, mercati di ogni colore, armi informatiche, manipolazione dell'informazione e distorsione delle notizie sembra esserci sempre meno spazio di manovra per i tradizionali Stati nazionali, bypassati da altri organismi molto più adattabili ed evolutivi, più capaci di seguire dinamicamente, se non di dettare, regole di funzionamento e di "vita" della rete globale, regole sempre più pericolosamente slegate da considerazioni di natura etica e solidale. Non ci sorprende più, ormai, che molti colossi del *web* siano in grado di andare allo scontro economico e legale, con sempre maggiore successo, con le istituzioni di molti paesi del mondo per questioni economiche e di libertà d'azione […]. Tutto deve farci riflettere: il mondo del *cyber* sarà sempre di più il nostro mondo, e in questo mondo sarà sempre più cruciale la definizione dei rapporti tra Stati (quali rappresentanti dei diritti e degli interessi delle comunità nazionali) e una pluralità di soggetti non statuali, ma comunque presenti nel cyberspazio con realtà e modalità sempre più complesse. Ciò in tutto il mondo e anche ovviamente nel nostro Paese», in *Atti Convegno «Il pericolo corre in rete. La nuova frontiera della minaccia cibernetica»,* Roma, 15 giugno 2017.

(60) Anche il Capo di Stato Maggiore della difesa, Gen. Claudio Graziano, è intervenuto sull'argomento, evidenziando che «Lo spazio cibernetico rappresenta un vero e proprio nuovo teatro di operazioni non esclusivamente ad appannaggio delle componenti militari, ma in cui trovano spazio anche organizzazioni e individui non necessariamente riconducibili ad entità statuali […]. La minaccia cibernetica sta assumendo un crescente rilievo in forma direttamente proporzionale alla "dipendenza informatica" da parte dei paesi tecnologicamente più avanzati e costituisce oggi uno dei più efficaci metodi di lotta asimmetrica». Entrando, poi, nello specifico delle implicazioni della minaccia *cyber* in ambito militare, il Capo di Stato Maggiore della difesa ha evidenziato che «l'elevato livello tecnologico che caratterizza anche gli assetti delle nostre Forze Armate ci espone ad attacchi *cyber* che possono avere una diretta incidenza in molteplici aspetti delle attività militari, come la gestione dei sistemi d'arma e le comunicazioni tattiche ed operative durante operazioni militari. Ormai il 60% della nostra attività è *cyber*. Il Comando interforze per le operazioni cibernetiche (CIOC) sta già operando e raggiungerà la piena capacità nel 2019», in *Atti Convegno «Il pericolo corre in rete. La nuova frontiera della minaccia cibernetica»,* Roma, 15 giugno 2017.

(61) In ambito nazionale la tematica è da tempo sotto i riflettori. Il Comitato Parlamentare per la Sicurezza della Repubblica (Co.Pa.Si.R.), nel luglio 2010, ha pubblicato una relazione sulle «possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico», formulando delle precise raccomandazioni al Governo (al riguardo, si rinvia a COPASIR, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, 7 luglio 2010, p. 17, *http://www.senato.it/leg/16/BGT/Schede/docnonleg/19825.htm*). La relazione sottolinea altresì come un attore fondamentale per la *cybersecurity* in Italia sia il comparto *intelligence* e, quindi, il Sistema di informazione per la sicurezza della Repubblica, che svolge un ruolo decisivo per quanto riguarda l'attività di monitoraggio e controllo delle minacce informatiche che attentano alla sicurezza del "Sistema-Paese". In seguito, la Presidenza del Consiglio dei Ministri, con decreto del 12 ottobre 2011, ha istituito il «Gruppo di studio per la sicurezza dell'utilizzo dello spazio cibernetico», allo scopo di formulare una proposta organizzativa per mettere a sistema le strutture esistenti ed eventualmente proporre eventuali interventi normativi al fine di realizzare uno strumento operativo nazionale per la *cybersecurity*. Successivamente, il legislatore italiano ha puntato fin da subito sull'elemento della cooperazione, esplicitando in maniera chiara quest'esigenza dapprima nel decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013 e, più di recente, nel nuovo decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, recante gli «Indirizzi per la protezione cibernetica e la sicurezza informatica nazionale» (sul quale v. *infra* paragrafo 4.1).

(62) Pubblicato nella G.U. del 27 luglio 2005, n. 173.

(63) Pubblicata nella G.U. del 13 agosto 2007, n. 187.

(64) La legge n. 133 del 7 agosto 2012, recante «Modifiche alla legge 3 agosto 2007, n. 124, concernente il «Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto», ha attribuito al Dipartimento informazioni per la sicurezza (DIS) il ruolo di coordinamento delle attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali (articolo 3, co. 1). La legge del 2007, come novellata, attribuisce dunque al DIS un ruolo fondamentale in ambito *cybersecurity*. L'elenco delle relazioni trasmesse al parlamento ai sensi della richiamata legge è consultabile al sito *https://www.sicurezzanazionale.gov.it/sisr.nsf/.../relazione-annuale.html.* Per un primo esame sulla normativa nel settore *cyber* in rapporto alla sicurezza nazionale, v. S. FINI, *L'identità nel* cyber *spazio e la normativa nazionale*, in *Informazioni della difesa,* supplemento al n. 6/2014, *Lo spazio cibernetico tra esigenze di sicurezza nazionale e tutela delle libertà individuali,* 199.

(65) Pubblicato nella G.U. del 30 aprile 2008, n. 101. Detto decreto dispone che sono da considerare infrastrutture critiche informatizzate di interesse nazionale i sistemi e i servizi informatici di supporto alle funzioni istituzionali di: a) ministeri, agenzie ed enti da essi vigilati, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute; b) Banca d'Italia ed autorità indipendenti; c) società partecipate dallo Stato, dalle regioni e dai comuni interessanti aree metropolitane non inferiori a 500.000 abitanti, operanti nei settori delle comunicazioni, dei trasporti, dell'energia, della salute e delle acque; d) ogni altra istituzione, amministrazione, ente, persona giuridica pubblica o privata la cui attività, per ragioni di tutela dell'ordine e della sicurezza pubblica, sia riconosciuta di interesse nazionale dal Ministro dell'interno, anche su proposta dei prefetti - autorità provinciali di pubblica sicurezza. Per un commento, v. R. SETOLA, *Pubblicato il decreto del Ministero dell'interno che individua le infrastrutture critiche informatizzate,* in *Safety&Security,* giugno 2008, 15 e ss.

(66) Pubblicato nella G.U. del 30 ottobre 2015, *n.* 253.

(67) Pubblicata nella G.U. n. 302 del 30 dicembre 2015, S.O. n. 70/L.

([68]) Di cui, a seguito del d.P.C.M. 6 settembre 2016, 135 milioni sono destinati al Comparto *intelligence,* i restanti 15 (pari ad un decimo come previsto dalla norma) al Servizio di Polizia Postale e delle Comunicazioni, che gestisce il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic), cfr. testo *Risposta ad interrogazione innanzi alla I Commissione permanente (Affari costituzionali, della Presidenza del Consiglio e interni), Atto Camera dei deputati del 26 ottobre 2016*. Nel testo della risposta si legge altresì che il Dipartimento informazioni per la sicurezza (DIS) «ha tenuto a precisare che le informazioni relative ad entrambi i tipi di interventi sono coperte da riservatezza».
([69]) Pubblicato nella G.U. del 13 aprile 2017, n. 87.
([70]) Pubblicato nella G.U. del 19 marzo 2013, n. 66. Detto d.P.C.M. 24 gennaio 2013 ha definito l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicando a tal fine i compiti affidati a ciascuna componente. Il modello organizzativo-funzionale persegue la piena integrazione anche con le attività espletate dalle strutture del Ministero della difesa dedicate alla protezioni delle proprie reti e sistemi, nonché alla condotta di operazioni militari nello spazio cibernetico.
([71]) Si veda il comunicato della Presidenza del Consiglio dei ministri, Dipartimento informazioni per la sicurezza (in G.U. n. 41 del 19 febbraio 2014, documento poi reso pubblico circa un mese dopo, il 20 febbraio 2014).
([72]) Anche in questo caso si veda il comunicato della Presidenza del Consiglio dei ministri, Dipartimento informazioni per la sicurezza (in G.U. del 19 febbraio 2014, n. 41, documento poi reso pubblico circa un mese dopo, il 20 febbraio 2014).
([73]) Adozione comunicata sulla G.U. del 31 maggio 2017, n. 125.
([74]) Per la realizzazione dei quali, in ambito difesa, lo Stato Maggiore della Difesa, ciascuna Forza Armata e il Segretariato Generale della Difesa e Direzione Nazionale degli Armamenti stanno fornendo il proprio contributo (v. *supra*, nota 60 e *infra,* nota 89 e 101).
([75]) Di detto atto particolare rilevo è il richiamo al ruolo della ricerca nazionale, nella parte in cui prevede «Nel percorso di accrescimento delle capacità e potenzialità del Paese, inoltre, deve essere riconosciuto un fondamentale rilievo, attese le repentine evoluzioni tecnologiche cui è soggetta la materia, al settore della ricerca e sviluppo delle attività di sicurezza informatica e alla cooperazione, per queste finalità, con università e centri di ricerca anche privati».
([76]) Approvato il 21 aprile 2015 dal Consiglio supremo di difesa e presentato al Parlamento 14 maggio 2015.
([77]) Per quanto concerne il cd. "Libro bianco", v. paragrafi 32, 68, 93, 94, 103, 173 e 195. Il CIOC è ampiamente descritto nell'audizione parlamentare presso la IV Commissione della Camera dei Deputati, seduta n. 9 dello scorso 25 gennaio 2017, nella quale il Generale Claudio Graziano, Capo di Stato Maggiore della difesa, ha evidenziato «[…] entro il 2017 sarà possibile realizzare il Nucleo iniziale del Comando interforze per le operazioni cibernetiche che – di fatto – ha già preso forma, per poi raggiungere, intorno alla fine del 2018, la capacità di condurre operazioni cibernetiche. In tale arco temporale, 2017-2019, occorrerà quindi completare soprattutto la protezione dell'info dominio della Difesa e acquisire i principali elementi capacitivi ovvero infrastruttura del comando, potenziamento della protezione del dominio, assetti»). Sulla recente istituzione del CIOC, v. anche, *Nasce il Comando Interforze per le Operazioni Cibernetiche. Intervista al Capo di Stato Maggiore della Difesa, Generale Claudio Graziano,* in *Informazioni della difesa,* n. 3/2017, 6 e *ivi*, p. 11, per i compiti del neocostituito Comando, v. F. VESTITO e COL. F. MUNNO, *Il Comando interforze per le operazioni cibernetiche – CIOC* (v. anche *supra* nota 60 e *infra* nota 89).
([78]) Pubblicata nella G.U. del 4 aprile 2017, n. 79. Il testo richiama la Direttiva del Presidente del Consiglio dei ministri 1 agosto 2015, evidenziando «l'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di eventi, quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi, visto anche l'inasprirsi del quadro generale con un preoccupante aumento degli eventi cibernetici a carico della pubblica amministrazione; sollecita, quindi, tutte le Amministrazioni e gli Organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici a dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di *standard* minimi di prevenzione e reazione ad eventi cibernetici. Al fine di agevolare tale processo, l'Agenzia per l'Italia Digitale si è impegnata a rendere prontamente disponibili indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori *partner* del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte».
([79]) Realizzato dal CIS-Sapienza e dal Laboratorio Nazionale di *cybersecurity* e pubblicato nel febbraio 2016, rappresenta un linguaggio comune in grado di agevolare, se non di permettere, il dialogo tra attori diametralmente

opposti, siano questi all'interno dell'organigramma delle imprese o delle pubbliche amministrazioni (ad esempio tecnici e dirigenti), siano organizzazioni vere e proprie in corso di collaborazione o di appalti di fornitura.

([80]) Realizzato dal CIS-Sapienza e dal Laboratorio Nazionale di *Cybersecurity,* pubblicato nel marzo 2017 e giunto alla sua quarta edizione, presenta 15 controlli essenziali di *Cybersecurity,* destinati principalmente a piccole e micro imprese italiane e corredati da un guida all'implementazione degli stessi. I controlli sono derivati dal *«Framework nazionale per la cyber security 2015»,* presentato nel 2016, ma sono rivolti alle organizzazioni, in particolare piccole-medie-micro imprese, che non hanno capacità tecniche sufficienti per adottare il *Framework* (nello specifico, come imprese *target* sono definite quelle che non hanno struttura interna che si occupa di *cybersecurity* e per le quali valga almeno una delle caratteristiche specificate dal *report,* tra le quali il possesso di proprietà intellettuale/*know how,* l'offerta di servizi via *web* e l'esistenza di accordi di riservatezza con i propri fornitori). Da ultimo, a cura dello stesso CINI, si segnala l'approntamento del cd. "Libro Bianco 2.0", alla redazione del quale stanno lavorando oltre quaranta università e i maggiori centri di ricerca del Paese, finalizzato ad individuare una serie di progetti destinati a decisori politici e settore industriale per contribuire a mettere in *cyber* sicurezza il Paese.

([81]) Il Comitato è aperto a tutte le organizzazioni di ricerca nazionali. In fase iniziale, è costituito dal Consiglio nazionale delle ricerche (CNR) e dal Consorzio interuniversitario nazionale per l'informatica (CINI). Il CINI consorzia 44 università pubbliche, riunendo, attraverso il Laboratorio nazionale di *cybersecurity*, più di 300 ricercatori nell'area della *cybersecurity*. Il CNR, attraverso il Dipartimento di ingegneria, ICT e tecnologie per energia e trasporti (Diitet), ha promosso un'area progettuale sulla *cybersecurity* che coinvolge più di 100 ricercatori che operano negli istituti dell'ente presenti su tutto il territorio nazionale. Il coordinamento del Comitato è stato affidato al direttore del Laboratorio nazionale di *cybersecurity*. Esso si propone di coordinare l'eccellenza nazionale della ricerca nel settore *cyber* e di realizzare azioni a livello nazionale e internazionale per il "Sistema-Paese", tra le quali: progettare un ecosistema nazionale più resiliente agli attacchi *cyber*; migliorare la continuità di servizio delle infrastrutture critiche, della pubblica amministrazione e delle filiere produttive strategiche; sviluppare piani di formazione per aumentare la *"workforce* nazionale" in *cybersecurity*; migliorare la consapevolezza di imprese e cittadini rispetto alle minacce *cyber*; infittire la collaborazione con organizzazioni omologhe europee e internazionali. Il lavoro di coordinamento svolto dal Comitato dovrebbe permettere, inoltre, di rafforzare l'eccellenza scientifica italiana in questo settore grazie alla promozione di attività nazionali e internazionali e al continuo flusso informativo che sarà realizzato tra le università, istituti di ricerca e la società nelle sue varie articolazioni.

([82]) All'inizio del 2017 è balzato agli onori della cronaca il cd. "Caso Occhionero", concernente i due fratelli arrestati il 9 gennaio con l'accusa di aver avviato un'attività di *cyber*-spionaggio. Le indagini condotte dalla Polizia postale e coordinate dalla Procura della Repubblica di Roma, con la collaborazione del *Federal Bureau of Investigation* (FBI), hanno portato alla luce una vera e propria centrale di *cyber*-spionaggio che attraverso intercettazioni informatiche ha raccolto per anni dati sensibili e notizie riservate su più di 1.700 *computer*. In particolare, è emerso che sarebbero stati 18.327 gli intercettati tramite il *malware "Eye Pyramid"* in un arco di almeno 5 anni (ma probabilmente anche di più) e per un traffico presumibilmente di centinaia di migliaia di comunicazioni. Diversi analisti hanno rilevato che in molti casi i sistemi informatici aggrediti sono certamente di interesse militare o relativi all'ordine e sicurezza pubblica o, comunque, di interesse pubblico. L'elenco del personale intercettato riguarderebbe ministri, segretari di partito e personalità politiche varie, ma anche autorità religiose, monetarie, mondo degli affari e alti vertici militari, ecc.: si parla di 18 categorie di intercettati. Il che, unito al numero inusuale di oltre 18.000 sorvegliati, significa una raccolta informativa sistematica e di ampio raggio. Nel caso in esame, che viene comunemente fatto rientrare in un caso di spionaggio, la stampa ha sostenuto che la tecnologia usata faccia pensare agli americani, ma anche a russi e cinesi.

Di recente, nel marzo 2017, i giudici del tribunale del riesame di Roma nella motivazione della mancata scarcerazione hanno evidenziato che «La tipologia dei sistemi infettati induce a ritenere significativo il pericolo per la sicurezza dello Stato e colora la condotta delittuosa in maniera particolarmente grave aprendo anche a scenari inquietanti». Ma questo, seppur eclatante, non è certo l'unico episodio noto. Infatti, un altro episodio che ha messo a dura prova la resilienza delle strutture cibernetiche è quello accaduto nel corso del 2016 e rivelato nel febbraio 2017, che ha visto parte della rete informatica del *Ministero* degli affari *esteri e* della *cooperazione* internazionale controllata da un'entità esterna. Una pesante offensiva che ha dato accesso a numerose informazioni sul personale diplomatico, militare e probabilmente dei servizi *intelligence* operanti in Italia e all'estero, a numerose *mail*, nonché a parte della documentazione informatizzata proveniente e indirizzata verso le sedi diplomatiche italiane. Gli analisti ritengono gli attacchi verosimilmente riconducibili a *"Uroburos"*, un *malware* diffuso dal gruppo "Apt28", per molti

legato al "Gru", l'agenzia di *intelligence* militare russa; secondo una ricerca di Eset, società di sicurezza informatica, dietro questi atti ci sarebbe invece il gruppo di *cyber* spionaggio russo *"Turla"*.
Lo strumento usato per violare i sistemi di sicurezza sarebbe la *backdoor "Gazer"* (secondo Eset, «Il successo di *"Gazer"* può essere spiegato dai metodi avanzati che utilizza per spiare i propri obiettivi e dalla sua capacità di rimanere attivo sui dispositivi infetti, lavorando nell'ombra per spiare il più a lungo possibile un computer. Gli attacchi alle ambasciate e ai ministeri effettuati finora tramite *"Gazer"* mostrano tutte le caratteristiche principali delle campagne di *cyber* spionaggio attribuite a *"Turla"*, che utilizzano tecniche di *spear-phishing* per distribuire una *backdoor* di primo stadio, cui si affianca una *backdoor* di secondo stadio che cattura le informazioni dal computer infetto e le invia al gruppo di *cyber* criminali tramite connessione ai server C&C»). Tuttavia, non si esclude che ad agire siano stati anche i cinesi della *"K3Chang"* e *"Zegost"*, con l'obiettivo di reperire informazioni sulla tutela degli interessi finanziari europei, cfr., seppur con il beneficio del dubbio, considerato che non è dato sapere a quali analisti faccia riferimento l'autrice dell'inchiesta, tra l'altro relativa a fatti passati e già balzati agli onori della cronaca, F. BULFON, *L'inchiesta. Dalle carte della NATO ai report su Siria e Libia i segreti della Farnesina rubati da Russi e cinesi, Repubblica* 14 agosto 2017.
([83]) I servizi di *intelligence* nazionali sono ben consapevoli dell'importanza e soprattutto della crescita esponenziale della minaccia cibernetica, prova ne è che mentre le Relazioni dei servizi di *intelligence* nazionali sulla politica dell'informazione per la sicurezza del 2007 e del 2008 inserivano brevemente le minacce cibernetiche in un'ottica di minacce alla sicurezza economica nazionale, di converso, a partire dalla Relazione del 2009 (p. 93), veniva posto in luce come «con riferimento agli scenari di potenziale incidenza sulla sicurezza economica e sulla più generale architettura di sistema che sorregge il concreto funzionamento, le attività quotidiane e i programmi di sviluppo della Nazione, un fondamentale campo di sfida per l'*intelligence* sarà quello della *cybersecurity*. Ciò a cospetto di una minaccia che ha ormai assunto caratura strategica, tanto da essere considerata dai principali attori internazionali un fattore di rischio di prima grandezza, direttamente proporzionale al grado di sviluppo raggiunto dalle tecnologie dell'informazione». A questa prima analisi hanno fatto seguito la Relazione del 2010 (pag. 30 e ss.), che ha valutato la minaccia come «di potenziale impatto sul Sistema-Paese e sulla stessa sicurezza nazionale», la Relazione del 2011 (p. 65 e ss.), la quale ha avvertito che la minaccia deve essere considerata «con prioritaria attenzione», fino a darne la qualificazione, nella Relazione 2012 (p. 37 e ss.), di «sfida più impegnativa per il Sistema-Paese» e la Relazione del 2013, che si apre addirittura con una disamina fenomenica del fenomeno *cyber* (ma vedi anche p. 21 e ss.). La Relazione del 2014 (p. 81) evidenzia, invece, che per il comparto *intelligence* la «minaccia *cyber* ha continuato a rivestire elevata priorità informativa. Sono state crescenti e più mirate le attività di contrasto poste in essere dall'*intelligence* al fine di garantire allo spazio cibernetico – ove si sviluppa una parte significativa della crescita economica e sociale del Paese – adeguati livelli di sicurezza». Mentre la Relazione del 2015 (p. 11) rileva che «a delineare il complessivo profilo strategico dell'*intelligence* nazionale è, altresì, intervenuta la particolare cogenza e impellenza con cui le evoluzioni di contesto hanno connotato tre dei macro-obiettivi della pianificazione informativa: il terrorismo internazionale, la *cybersecurity,* la sicurezza economico-commerciale e finanziaria». Ed ancora, particolare rilievo alla tematica è dato dalla Relazione del 2016, la quale specifica che la «minaccia cibernetica» costituisce, in prospettiva, la vera e propria «nuova frontiera» per l'*intelligence* e per le amministrazioni italiane che concorrono alla sicurezza nazionale, al punto da qualificarla come una delle tre principali sfide per il "Sistema-Paese" italiano assieme al terrorismo jihadista e alla minaccia economico-finanziaria. Più di recente l'ultima Relazione dei servizi di *intelligence* (2017) evidenzia che «il monitoraggio dei fenomeni di minaccia collegati con il *cyberspace* ha evidenziato un costante *trend* di crescita in termini di sofisticazione, pervasività e persistenza a fronte di un livello non sempre adeguato di consapevolezza in merito ai rischi e di potenziamento dei presidi di sicurezza», la stessa lamenta altresì «la persistente vulnerabilità di piattaforme *web* istituzionali e private, erogatrici in qualche caso di servizi essenziali o strategici, che incidono sulla sicurezza nazionale, e la presenza di un sostanziale sbilanciamento del rischio, generalmente contenuto, in capo agli attori della minaccia rispetto a quello dei *target*». In detta ultima relazione, si è altresì continuato «a rilevare una diversificazione dei *target,* delle modalità attuative e delle finalità degli attacchi in base alla matrice della minaccia: da quelle più rilevanti per gli *asset* critici e strategici connesse al *cybercrime,* al *cyber-espionage* ed alla *cyberwarfare,* a quella terroristica ed *hacktivista,* più stabili nella condotta e negli obiettivi». In particolare, «sono emersi elementi di novità in relazione ai *target* privati. Se nel 2015 *target* principali degli attacchi *cyber* risultavano quelli operanti nei settori della difesa, delle telecomunicazioni, dell'aerospazio e dell'energia, nel 2016 figurano ai primi posti il settore bancario con il 17% delle minacce a soggetti privati (+14% rispetto al 2015), le agenzie di stampa e le testate giornalistiche che, assieme alle associazioni industriali, si attestano sull'11%». Queste ultime, prosegue il *report,* «costituiscono una *"new entry",* insieme al settore farmaceutico che, con il suo 5% degli attacchi verso *target* privati, si posiziona al fianco di settori "tradizionali" come quelli della difesa, dell'aerospazio e

dell'energia. Tra questi ultimi, solo quello energetico ha fatto registrare un aumento, pari al 2%, rispetto all'anno precedente, mentre quelli di difesa e dell'aerospazio hanno fatto segnare un decremento, rispettivamente, del 13% e del 7%». Con specifico riferimento all'aerospazio, giova rilevare che l'industria italiana Leonardo sta lavorando con l'Agenzia Spaziale Europea (ESA) per uno studio per la gestione della sicurezza dei dati del programma europeo di navigazione satellitare "Galileo". In particolare Leonardo sta sviluppando un'architettura di riferimento e definendo requisiti e processi per la gestione della sicurezza informatica del programma, in accordo con le recenti normative europee in materia di *cybersecurity*. L'obiettivo di Leonardo, da quanto emerso in occasione della conferenza *Cybertech Europe* 2017, è supportare l'ESA nella definizione di un sistema allo stato dell'arte per il monitoraggio della sicurezza di "Galileo", anche alla luce dell'introduzione di nuovi requisiti di missione del sistema e di nuovi *standard* e procedure di sicurezza relativi alla rete satellitare europea. «La *cybersecurity* delle infrastrutture spaziali è sempre più strategica. È necessario sviluppare nuove tecnologie, anche in una logica di collaborazioni internazionali, capaci di proteggere gli *asset* satellitari, che hanno un ruolo essenziale nella vita quotidiana dei cittadini e nel funzionamento delle infrastrutture critiche delle nazioni, dalle comunicazioni ai trasporti alla difesa. Difenderli dalle minacce *cyber* è diventato imprescindibile», così, Alessandro Profumo, Amministratore Delegato di Leonardo, in occasione della conferenza *Cybertech Europe* 2017, ma per approfondimenti sul tema v. M. SPAGNULO, Internet *su satelliti a prova di* hacker, in *Airpres,* ottobre 2017, p. 40, nel quale l'autore mette in evidenza che nell'era informatica dei rischi globali, ogni nazione studia come rendere più sicure le proprie comunicazioni, comprese quelle satellitari, non immuni da pericoli, rilevando come il programma cinese "*Quess*" stia consolidando le basi tecnologiche per le comunicazioni quantistiche, le cui chiavi crittografiche potrebbero rappresentare una frontiera inespugnabile per gli *hackers*.

([84]) Sulle distinte funzioni dello Stato in materia di difesa e sicurezza (esercitate dal Ministero della difesa), da un lato, e in materia di ordine e sicurezza pubblica (esercitate dal Ministero dell'interno), dall'altro, si è soffermato anche Cons. St., sez. per gli atti normativi, parere n. 7762/2012, adunanza dell'11 ottobre 2012. Le attività della difesa e della sicurezza nazionale sono regolamentate nel «Codice dell'ordinamento militare» di cui al d.lgs. n. 66/2010, mentre quelle concernenti il Ministero dell'interno sono enucleate nel d.lgs. 30 luglio 1999, n. 300, per quanto riguarda le funzioni dell'ordine e della sicurezza pubblica (art. 14) e nella legge 1 aprile 1981, n. 121, recante «Nuovo ordinamento dell'amministrazione della pubblica sicurezza». Per approfondimenti sul tema del ruolo (e dei limiti) dei servizi di *intelligence* nei vari Stati dell'Unione europea, v. il *Report Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, del 2015.

([85]) Nel settore della sicurezza della Repubblica, sotto il coordinamento del Dipartimento delle informazioni per la sicurezza (DIS), operano, altresì, due Agenzie di informazioni («Agenzia informazioni e sicurezza esterna» - AISE e «Agenzia informazioni e sicurezza interna» - AISI), i cui compiti sono ripartiti dalla legge 3 agosto 2007, n. 124 (recante «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto»), la quale richiede a entrambe le agenzie *de quibus* di informare con continuità e tempestività, tra gli altri, il Ministero della difesa (con riferimento all'attività dell'AISE) e il Ministero dell'interno (con riguardo all'attività dell'AISI). Tale legge ha riformato il sistema di informazione per la sicurezza della Repubblica; su tale riforma, v. AA.VV. *I servizi di informazione e il segreto di Stato (legge 3 agosto 2007, n. 124)*, Milano, 2008. Sulla sicurezza dello Stato in generale v. A. MASSERA, C. MOSCA, *I servizi di informazione*, in AA.VV. *Trattato di diritto amministrativo. Diritto amministrativo speciale* (a cura di S. Cassese), I, Milano, Giuffrè, 2000, 370 ss.

([86]) Per il ruolo dei servizi segreti italiani nello specifico settore della *cyber*, v. G.P. SCOTTO DI CALTABIANO, *A che serve l'*intelligence *italiana,* in *Limes - A che servono i servizi,* n. 7/2014, pp. 189 e ss., nel quale l'autore rileva come i continui progressi tecnologici della comunicazione e dell'informazione hanno reso il ciberspazio un elemento indispensabile per le società e le economie nazionali e come pertanto i servizi segreti italiani stiano focalizzando la loro attenzione su nuove sfide, a cominciare dalle partite geopolitiche e/o inerenti l'uso strategico delle reti informatiche, con l'obiettivo di impedire il cd. *"downgrading"* strutturale dell'economia italiana nell'epoca della globalizzazione economica.

([87]) Il Dipartimento delle informazioni per la sicurezza (DIS) è l'organo di cui si avvalgono il Presidente del Consiglio dei ministri e l'Autorità delegata per l'esercizio delle loro funzioni e per assicurare unitarietà nella programmazione della ricerca informativa, nell'analisi e nelle attività operative di AISE e AISI. Al DIS spetta, inoltre, il coordinamento delle attività informative indirizzate alla protezione delle infrastrutture critiche e dello spazio cibernetico del Paese, In sintesi, il DIS: coordina l'intera attività di informazione per la sicurezza, compresa quella relativa alla sicurezza cibernetica e ne verifica i risultati; è informato costantemente delle operazioni di AISE e AISI e trasmette al Presidente del Consiglio dei ministri le informative e le analisi prodotte dal Sistema; raccoglie informazioni, analisi e rapporti prodotti da AISE e AISI, da altre amministrazioni dello Stato e da enti di ricerca;

elabora analisi strategiche o relative a particolari situazioni da sottoporre al CISR o ai singoli Ministri che lo compongono; promuove e garantisce lo scambio informativo tra i servizi di informazione e le Forze di polizia; esercita il controllo sulle attività di AISE e AISI attraverso l'Ufficio centrale ispettivo; vigila sulla corretta applicazione delle disposizioni emanate dal Presidente del Consiglio dei ministri in materia di tutela amministrativa del segreto di Stato e della documentazione classificata; impartisce gli indirizzi per la gestione unitaria del personale di DIS, AISE e AISI; gestisce unitariamente gli approvvigionamenti e i servizi logistici comuni a DIS, AISE e AISI; elabora con AISE e AISI il piano di acquisizione delle risorse umane, materiali e strumentali; cura le attività di promozione della cultura della sicurezza e la comunicazione istituzionale. Per approfondimenti, v. M. CALIGIURI, *Cyber intelligence. Tra libertà e sicurezza,* Donzelli Editore, 2016, XII 98 e ss.; v. anche *http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/cyber-intelligence-la-sfida-dei-data-scientist.html.*

([88]) Con la sentenza F.lli Costanzo, la Corte precisa che «tutti gli organi dell'amministrazione, compresi quelli degli enti territoriali, come i comuni» sono tenuti ad applicare le disposizioni direttamente efficaci e in mancanza i singoli potranno avvalersene in giudizio di fronte ai giudici nazionali, *CGCE, F.lli Costanzo, C-103/88,* in *Racc.,* p. 1839, p.to 31.

([89]) V. *supra* nota 73 e 74. Il nuovo "Piano" – rivisitato congiuntamente dalle amministrazioni che compongono l'architettura nazionale *cyber* (Comparto *intelligence,* Ministero degli affari esteri e della cooperazione internazionale, Ministero dell'interno, Ministero della difesa, Ministero della giustizia, Ministero dell'economia e delle finanze, Ministero dello sviluppo economico, Agenzia per l'Italia digitale, Ufficio del Consigliere militare del Presidente del Consiglio) – mantiene, invero, un impianto sostanzialmente invariato rispetto alla sua precedente versione, mirando a sviluppare alcuni indirizzi strategici, quali: il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il "Sistema-Paese"; il miglioramento delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati; l'incentivazione della cooperazione tra istituzioni e imprese nazionali; la promozione e diffusione della cultura della sicurezza cibernetica; il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica; e, infine, il rafforzamento delle capacità di contrasto alle attività e contenuti illegali *online.* Il "Piano", in linea di continuità con quello relativo al biennio 2014-2015 e alla luce dell'esperienza maturata nel corso dello stesso, individua gli indirizzi operativi, gli obiettivi da conseguire e le linee d'azione da porre in essere per dare concreta attuazione al «Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico» (QSN), alla luce degli indirizzi per la protezione cibernetica e la sicurezza informatica indicati dal Presidente del Consiglio dei ministri nella sua qualità di organo di vertice dell'architettura nazionale *cyber.* In particolare, rispetto al precedente "Piano", le principali direttrici dell'intervento di revisione degli undici indirizzi operativi del PN hanno riguardato in particolar modo l'indirizzo operativo n. 5 «Operatività delle strutture nazionali di *incident prevention, response e remediation*», riconsiderando il sistema dei CERT pubblici sulla base della progressiva unificazione di CERT Nazionale e CERT PA in un'unica struttura ovvero sulla creazione di una rete nazionale di CERT che risponda ad un soggetto con specifici poteri di coordinamento e il potenziamento delle capacità di *intelligence,* di polizia e di difesa civile e militare. Il "Piano" prevede anche un supporto alle iniziative del Ministero della difesa volte a istituire un Comando interforze operazioni cibernetiche (CIOC), deputato alla protezione dei sistemi e delle reti del Dicastero della difesa, nonché all'effettuazione delle operazioni in campo cibernetico (per approfondimenti, v. *supra*, nota 60), e alla realizzazione, presso la Scuola Telecomunicazioni delle Forze Armate di Chiavari (STELMILIT), di un poligono *cyber* virtuale nazionale (cd. *Cyber range*), per la realizzazione del quale il Ministero della difesa, anche nell'ambito delle attività del «Piano di ricerca militare» (PNRM) – facenti capo al Segretariato Generale della Difesa e Direzione Nazionale degli Armamenti e in particolare al Reparto "Innovazione Tecnologica" – sta fornendo il proprio rilevante contributo (v. *supra,* nota 74 e *infra* nota 101).

Infine, nel "Piano" nazionale è previsto uno specifico piano d'azione dedicato ad un nucleo essenziale di iniziative, cui attribuire carattere di priorità ed urgenza, per approfondimenti v. *www.cyberaffairs.it,* del 3 giugno 2017 (con commenti di C. GIUSTOZZI e S. MELE) e ancora v. S. MELE, in *www.cyberaffairs.it,* del 17 giugno 2017 che rileva come «[…] nel nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica l'elemento di più evidente e rilevante novità risiede proprio nella volontà del governo italiano di dare avvio alla creazione di una fondazione o di un fondo *di venture capital* per il finanziamento di *startup* e/o per la partecipazione al capitale societario di realtà imprenditoriali d'interesse. Novità che, peraltro, deve essere letta soprattutto in raccordo con l'ulteriore e lungimirante obiettivo di istituire un Centro nazionale di Ricerca e Sviluppo in *cybersecurity* e un Centro nazionale di crittografia. La sensazione, allora, è che anche il governo italiano sia intenzionato a muoversi nella medesima direzione di quanto fatto tempo fa dagli Stati Uniti o di quanto Israele oggi sembra accingersi a realizzare. E di questo non si può che fare un plauso al governo Gentiloni». Per un commento sul PN, v. altresì M. IASELLI, *Cyber security: pubblicato il Piano Nazionale,* in *www.altalex.it* del 14 giugno 2017.

(90) V. *supra* nota 71.
(91) Al CISR viene assegnata la facoltà di emanare direttive al fine di innalzare il livello della sicurezza informatica del Paese, avvalendosi a tal fine del supporto del cosiddetto CISR Tecnico e del Dipartimento per le informazioni e la sicurezza (DIS). Il CISR, in caso di crisi cibernetica, partecipa alle determinazioni del Presidente del Consiglio dei ministri, con funzioni di consulenza e di proposta, nonché di deliberazione in alcuni casi specifici; propone al Presidente del Consiglio dei ministri l'adozione del quadro strategico nazionale; delibera il piano nazionale per la sicurezza dello spazio cibernetico, sulla cui attuazione esercita anche funzioni di sorveglianza.
(92) Per approfondimenti v. anche A. PANSA, *Audizione davanti alle Commissioni riunite Affari costituzionali e Difesa del Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS),* sulle problematiche legate alla difesa e alla sicurezza nello spazio cibernetico.
(93) A ben vedere, già la relazione del Co.Pa.Si.R. del 2010 chiudeva con una raccomandazione importante per il Governo, affinché questo adottasse «un impianto strategico-organizzativo che assicuri una *leadership* adeguata e predisponga chiare linee politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati». Già allora, infatti, veniva suggerita l'individuazione di una struttura di coordinamento, da istituire presso la Presidenza del Consiglio dei ministri o l'autorità delegata, che si occupasse di tutte le maggiori questioni di *cybersecurity,* Co.Pa.Si.R., *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale, cit.,* p. 49.
(94) L. TRICARICO, *Dal Dpcm cyber al Consiglio per la sicurezza nazionale,* in *www.cyberaffairs.it,* del 6 maggio 2017.
(95) S. MELE, *Le tre novità che cambieranno la* cyber security *nazionale, con il nuovo decreto,* in *www.agendadigitale.eu,* del 14 aprile 2017.
(96) Composto da rappresentanti dei ministeri principali, delle agenzie di *intelligence*, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale.
(97) Invero, per incrementare il livello di resilienza cibernetica, è essenziale investire sul fattore tecnologico, solo così si può garantire lo sviluppo e l'evoluzione di competenze *cyber* di alto livello, sia in ambito scientifico sia industriale.
(98) Al riguardo, solo per citare un esempio, per le attività ed i relativi progetti del «Piano di ricerca militare» (PNRM) – facenti capo al Segretariato Generale della Difesa e Direzione Nazionale degli Armamenti e in particolare al Reparto "Innovazione Tecnologica" – nell'ambito della valutazione dei progetti relativi al PNRM 2017 è stato inserito, di concerto con lo Stato Maggiore della difesa, un apposito *cluster* capacitivo/tecnologico relativo alla *cybersecurity*.
(99) La *cybersecurity* «rappresenta infatti non solo uno dei più promettenti settori dal punto di vista della crescita del mercato, ma anche un ambito strategico di grande interesse per governi e aziende. Si stima che in tale settore il mercato globale possa superare nel 2020 i 155 miliardi di dollari. A riprova di ciò, gli investimenti da parte dei fondi di *venture capital* nel settore della sicurezza cibernetica sono passati dai 340 milioni di dollari nel 2009 ai 3 miliardi di dollari nel 2016, con oltre 300 operazioni commerciali andate a buon fine, in tal senso cfr. S. MELE, in *www.cyberaffairs.it,* del 3 giugno 2017. Un primo tangibile segnale che sembrerebbe confermare detto approccio si rinviene nella proposta di legge n. 4660 (Camera dei deputati), presentata il 25 settembre 2017 che mira alla costituzione e allo sviluppo di *start-up* innovative nel settore della *cybersecurity* e a rafforzare la competitività tecnologica nel settore della sicurezza cibernetica. In detta direzione si sta muovendo anche il Regno Unito dove le aziende che si occupano di *cybersecurity* si sono unite per proteggere il Paese dalle minacce informatiche. L'acceleratore di *startup «Level39»* ha recentemente lanciato il programma *«Cyber39»*, il cui obiettivo è far lavorare insieme le imprese del settore per difendere la nazione dai pericoli del *cyberspace*. Detta iniziativa non servirà solo per contrastare le minacce cibernetiche, ma anche per trovare e sviluppare nuove tecnologie. A questo proposito, *«Level39»* ha presentato il *Cyber Demonstration Centre (CDC)*; detta struttura ospiterà le *start-up*, che potranno esibire e illustrare i loro prodotti e le loro innovazioni tecnologiche. Questo sembra essere l'orientamento anche del Ministro della difesa, Sen. Roberta Pinotti, che in occasione del *Cybertech Europe* 2017, ha messo in luce proprio l'aspetto della «condivisione» di responsabilità pubblico-privato degli aspetti legati alla sicurezza informatica, attraverso il rispetto delle regole, la lotta alla *cyber* criminalità e la produzione di contenuti positivi. Ad avviso del Ministro, infatti, «Non può essere solo lo Stato, nelle sue varie articolazioni, a tutelare la sicurezza del sistema e il rispetto delle regole». Nella medesima occasione anche Alessandro Profumo, Amministratore Delegato di Leonardo, ha evidenziato che la *cyber* sicurezza «è una priorità assoluta» sia per un'azienda industriale sia per una nazione, «perché da essa dipendono crescita economica, sviluppo della conoscenza, capacità di attrarre investimenti […]. Ed è anche una questione globale che impone lo sforzo congiunto di istituzioni, mondo accademico e della ricerca, industria, cittadini».

(100) In tal senso, un esempio virtuoso da prendere a riferimento potrebbe essere quello israeliano, dove una delle agenzie d'*intelligence* israeliana (il *"Mossad"*) ha lanciato il cd. *"Libertad"*, un fondo di investimento per *start-up* che sviluppano tecnologie innovative che potrebbero essere utilizzate dalla medesima agenzia d'*intelligence* israeliana. «L'idea, nonostante i pochissimi dettagli disponibili, sembra ricalcare quella messa in atto dalla Cia – ormai 18 anni fa – con il fondo *In-Q-Tel*, ha come naturale obiettivo quello di dare accesso diretto ed esclusivo a questa agenzia di *intelligence* alle più avanzate e utili innovazioni nel campo delle nuove tecnologie, garantendole la possibilità di scegliere di finanziare le idee più interessanti rispetto alle finalità da raggiungere», in tal senso S. MELE, *Un* cyberspark *da bissare,* in *Airpres,* settembre 2017, p. 57. Il fondo – che offrirà, per ogni progetto, fino a 568mila dollari di capitale *"equity-free"* per scopi di ricerca e sviluppo in cambio dell'utilizzo non esclusivo della tecnologia sviluppata, senza imporre alle imprese finanziate restrizioni o pagamento di *royalties* – investirà in aziende che svilupperanno "tecnologia all'avanguardia" in campi di innovazione tecnologica come la robotica, la produzione energetica, la crittografia, la miniaturizzazione, il cd. *profiling* e l'analisi testuale. Per il ruolo dei servizi segreti israeliani, e del *"Mossad"* in particolare, nello specifico settore della *cyber*: v. A. RAPAPORT, *La metemorfosi dell'*inteligence *israeliana,* in *Limes - A che servono i servizi,* n. 7/2014, p. 119 e ss. A ben vedere, detta attività governativa di impulso allo sviluppo di nuove tecnologie nel campo sia civile che militare non è nuova per Israele. Da diversi anni, ormai, il Paese è infatti diventato un punto di riferimento internazionale; il governo israeliano ha da tempo puntato gran parte della sua attenzione istituzionale sulle questioni relative alla sicurezza cibernetica, sia sotto il profilo militare e di *intelligence*, per la salvaguardia dei propri interessi strategici, sia come veicolo e volano dello sviluppo economico del Paese. L'impegno di Israele in questo settore nasce dalla «consapevolezza che la sicurezza cibernetica non è una moda, ma un qualcosa che è determinante ora, e che lo sarà per almeno i prossimi dieci anni […]. Le aziende israeliane – ha aggiunto – sono le più attaccate al mondo. Oltre il 99% degli attacchi sono molto semplici, eppure ci concentriamo proprio su quella piccola percentuale che resta […]. I governi sanno come difendersi, è il lato delle imprese a rappresentare il problema principale, Israele è totalmente favorevole alla cooperazione e a un approccio collaborativo, in particolare con gli alleati occidentali. […]. Il mondo sta già cambiando, e dietro l'angolo potrebbe esserci un 11 settembre cibernetico che deve essere considerato come una possibilità reale», in tal senso si è espresso l'ambasciatore di Israele in Italia Ofer Sachs, in *www.cyberaffairs.it, 30 settembre 2017 e v. anche Tutti i progetti di Israele sulla* cyber security, in *www.analisidifesa.it*, 1 ottobre 2017. Già in passato comunque il Paese in questione si è distinto per iniziative che hanno consentito allo stesso di assurgere al ruolo di nazione all'avanguardia nello sviluppo di soluzioni tecnologiche (per ulteriori approfondimenti sul tema, v. *supra* nota 15). Tra di esse può essere ricordata una delle più importanti iniziative che prende il nome di *«Yozma»*, un programma governativo finalizzato ad incrementare gli investimenti da parte dei fondi di *venture capital* in tecnologia israeliana (il programma esordì con un meccanismo basato su un rapporto di uno e mezzo a uno: se i *partner* israeliani riuscivano a raccogliere 12 milioni da investire in tecnologia israeliana, il governo avrebbe erogato fondi per 8 milioni). Ovvero la fondazione *«Binational industrial Research and development» (BIRD)* concepita come strumento per promuovere *joint venture* israelo-americane e sostenerle, per approfondimenti, cfr. D. SENOR e S. SINGER, *Laboratorio Israele. Storia del miracolo economico israeliano,* pp. 164 e ss. Più di recente (2014), Israele ha acquisito in questo ambito una posizione dominante a livello globale grazie al suo *«CyberSpark»* a Be'er Sheva: un parco tematico dove governo, università e aziende private possono concentrare i loro sforzi sullo sviluppo di soluzioni nel settore della *cybersecurity*. Stando alle ultime stime ufficiali, grazie a questa iniziativa Israele ha fatto nascere nel suo *«Cyber-Spark»* circa 350 aziende nazionali aventi come *core business* proprio la sicurezza cibernetica, le quali esportano annualmente e in tutto il mondo servizi e tecnologie per circa 6 miliardi di dollari. Al riguardo, giova evidenziare che l'architettura nazionale della sicurezza isrealiana, che coinvolge sia l'industria della difesa sia l'esercito, ha guadagnato una reputazione eccellente a livello internazionale in termini di capacità di innovazione tecnologica. Israele conta, tra l'altro, la seconda più alta concentrazione di aziende di *cyber* difesa al mondo dopo gli Stati Uniti, con i quali ha, tra l'altro, recentemente siglato un accordo mediante il quale verrà avviato un progetto che porterà alla creazione di un gruppo di lavoro focalizzato sulla *cybersecurity,* come annunciato da Thomas Bossert, assistente del presidente Usa Donald Trump per la Sicurezza nazionale e l'antiterrorismo, il 26 giugno 2017 a Tel Aviv durante l'edizione 2017 della *"Cyber Week"*. L'organismo includerà rappresentanti statunitensi e israeliani di diversi ministeri e organizzazioni di difesa e sicurezza, compresi gli affari esteri, la giustizia e l'*intelligence*. Le rispettive agenzie saranno «focalizzate sulla ricerca e l'arresto degli avversari cibernetici prima che questi possano infiltrarsi nelle reti e raggiungere le infrastrutture critiche, individuando anche modi precisi per rendere responsabili di fronte alla legge gli aggressori»; ha dichiarato ancora Bossert, «Crediamo che l'agilità che Israele ha nello sviluppare soluzioni porterà alla creazione di difese informatiche innovative che possiamo testare ed adottare in America» (per l'innovazione istituzionale in atto nella sicurezza informatica in Israele, v. *«National Cyber Security Organization: Israel», Report* del

NATO Cooperative Cyber Defence Centre of Excellence). Per quanto concerne invece i rischi delle infrastrutture critiche americane si veda il *«Report: Critical infrastructure under risk of '9/11-level cyber attack»* dell'agosto 2017, nel quale si legge che *«The time to act is now. As a Nation, we need to move past simply studying our cybersecurity challenges and begin taking meaningful steps to improve our cybersecurity to prevent a major debilitating cyber-attack»*. Nell'agosto 2017, anche uno s*tudio del «National Infrastructure Advisory Council»* (*NIAC*), *corredato di raccomandazioni per il governo americano, ha messo in evidenza come u*n *cyber* attacco generalizzato all'infrastruttura critica nazionale americana è da tempo considerato una minaccia incombente e catastrofica (in *https://www.hsdl.org/?abstract&did=803545*). Il documento offre diverse raccomandazioni per i principali *stakeholder* del governo USA per prevenire un attacco informatico che secondo lo studio potrebbe avere effetti simili a quello dell'11 settembre 2001. L'elenco di suggerimenti include la creazione di una rete di comunicazione separata e sicura per le reti più critiche; un sistema gestito dal settore privato che alimenti la condivisione di informazioni da macchina a macchina; il rafforzamento delle capacità della forza lavoro informatica; e la creazione di protocolli per la declassificazione delle informazioni sulle *cyber* minacce, da condividere con i proprietari e gli operatori delle infrastrutture. «Il dominio *cyber*», evidenzia ancora lo studio, «è l'unica arena dove le aziende private sono la prima linea di difesa in un attacco a livello nazionale sulle infrastrutture statunitensi. Quando un attacco informatico può causare gli stessi danni o le conseguenze di un attacco cinetico, richiede una *leadership* nazionale e un coordinamento stretto delle risorse, delle capacità e delle autorità collettive». In generale, sul piano delle iniziative per l'innovazione tecnologica degli Usa nel settore della *cyber*, v. la *Cyber S&T COI Needs Statement Response* dell'8 agosto 2017, ossia una nota con la quale il Dipartimento della difesa americano ha inviato all'industria di settore un avviso nel quale elenca una serie di esigenze tecnologiche innovative del Pentagono in campo *cyber* che abbracciano diverse tematiche, tra le quali la difesa informatica autonoma (e sottocategorie); la consapevolezza situazionale informatica, pianificazione e supporto decisionale (e sottocategorie); la *cybersecurity* per infrastrutture, *endpoint* ed *edge device* (e sottocategorie); i sistemi di controllo, sicurezza dell'IoT (e sottocategorie); la sicurezza *hardware* e *software* (e sottocategorie). Di recente anche la *«Defense Advanced Research Projects Agency» (DARPA)* ha elaborato una lista aggiornata di aziende in grado di partecipare a progetti di ricerca in operazioni di cyberspazio (CSO), sul tema v. *DARPA wants who's who of cyberspace,* in *http://fifthdomain.com,* 29 agosto 2017. In generale, su detto ultimo aspetto relativo al ruolo dell'innovazione tecnologica nel settore della *cybersecurity* degli Stati Uniti e sulla necessità di politiche di settore centralizzate, v. anche *De-complicating cybersecurity at the federal level,* in *http://fifthdomain.com,* 8 marzo 2017 e ancora, con particolare riferimento all'*intelligence* geospaziale, *NGA's Digital Attack Team looks to tackle technology's biggest ideas,* in *www.c4isrnet.com,* 1 agosto 2017. Di recente, sulla necessità di una revisione normativa e della costituzione di un'agenzia che curi le attività di *cybersecurity* nell'ambito del *Department of Homeland Security,* v. M. MCCAUL, «[…] *expects in the next few weeks to introduce legislation to reorganize and elevate the Department of Homeland Security's cybersecurity functions, a bill he says the committee should mark up by the end of the spring. The introduction of the much-anticipated bill would mark the beginning of a renewed legislative push to establish a cybersecurity agency within DHS, which was a top priority for the Obama administration and McCaul in the last Congress*», in *www.insideCybersecurity.com*, 28 marzo 2017. Da ultimo sulla sinergia tra il settore governativo americano e quello privato nel campo della *cybersecurity,* v. C. CUMMISKEY, *DHS office leading the way on federal cyber innovation,* secondo il quale *«One office in the federal government is having an outsized, positive impact on bringing private sector innovation to government cybersecurity problem solving. The Cybersecurity Division (CSD) of the Science & Technology Directorate at the Department of Homeland Security has figured out how to crack the code in swiftly delivering cutting edge cyber technologies to the operators in the field. Some of these programs include: cybersecurity for law enforcement, identity management, mobile security and network system security»,* in *http://fifthdomain.com,* 26 settembre 2017.

([101]) In tal senso, un precedente virtuoso tuttora in via di implementazione può rinvenirsi (v. *supra* note 74 e 89), ad esempio, nella realizzazione, presso la Scuola Telecomunicazioni delle Forze Armate di Chiavari (STELMILIT), di un poligono *cyber* virtuale nazionale (cd. *Cyber range*), per la realizzazione del quale il Ministero della difesa, anche nell'ambito delle attività del «Piano di ricerca militare» (PNRM) – facenti capo al Segretariato Generale della Difesa e Direzione Nazionale degli Armamenti e in particolare al Reparto "Innovazione Tecnologica" – sta fornendo il proprio rilevante contributo.

([102]) In generale, sull'approccio strategico nazionale al tema della *cyber,* v. S. MELE, *I principi strategici delle politiche di cybersecurity,* in *Approfondimenti del Sistema di informazione per la sicurezza della Repubblica*, 5 dicembre 2013 e ancora A. RIGONI, *Cyber-security: serve una strategia nazionale,* in *Corriere delle Comunicazioni*, 6 aprile 2013, *http://www.corrierecomunicazioni. it/it-world/20603_cybersercurity-rigoni-serve-una-strategia-nazionale.htm.*

([103]) Il *Computer Emergency Response Team* (CERT) nazionale è una struttura individuata, a norma dell'articolo 16 *bis* del d.lgs. n. 259 del 2003, recante il «Codice delle Comunicazioni elettroniche», presso il Ministero dello sviluppo economico. Si tratta di una struttura destinata a potenziare i meccanismi di risposta agli incidenti informatici e gli

strumenti di rilevazione e contrasto alle minacce. Il CERT nazionale ha avviato le sue attività a partire dal 5 giugno 2014. Esso opera a supporto di cittadini e imprese con l'obiettivo di incrementare la consapevolezza e la cultura della sicurezza nell'utilizzo di servizi *online*, fornendo informazioni tempestive su potenziali minacce informatiche, raccomandazioni e consigli utili per la prevenzione, contromisure per la risoluzione di incidenti informatici con impatto significativo. Per assicurare un'azione efficace, il CERT opera sulla base di un modello cooperativo pubblico-privato: ha avviato, infatti, la collaborazione con importanti imprese che gestiscono infrastrutture informatizzate. Sulla base di tale collaborazione è stato istituito un Tavolo tecnico permanente per garantire un confronto costante tra i principali attori coinvolti e quindi migliorare e velocizzare le azioni di risposta ad eventuali incidenti informatici. Il CERT ha avviato anche una stretta collaborazione con il CERT-PA (CERT delle Pubbliche Amministrazioni che opera all'interno dell'Agenzia per l'Italia Digitale), CERT Difesa e CNAIPIC (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche che opera nell'ambito del Servizio di polizia postale e delle comunicazioni). In ambito internazionale, il CERT nazionale ha già avviato forme di dialogo con CERT europei, extra-europei e con il CERT-EU (CERT dell'Unione Europea sostenuto dall'Agenzia europea per la sicurezza ENISA). Il CERT è, sia nel mondo pubblico sia in quello privato, il punto di contatto principale per la gestione degli incidenti critici e in generale per la prevenzione della minaccia *cyber*, è però un dato inconfutabile che buona parte delle amministrazioni pubbliche ovvero delle infrastrutture critiche nazionali non abbiano ancora formalmente costituito un CERT o stiano cominciando ora il percorso per la sua realizzazione; i pochi CERT attualmente operativi sono, inoltre, ancora troppo focalizzati sulla protezione interna dell'organizzazione e non nascono con un vero e proprio spirito di cooperazione nell'ottica di garantire un'univoca capacità di *cybersecurity* nazionale.

([104]) In tal senso, v. S. MELE, *Cyber Strategy & Policy Brief,* Volume 02 - Febbraio 2016.

([105]) In tal senso, v. S. MELE, *ibidem,* p. 8.

([106]) Il Consiglio dei ministri del 3 marzo 2017 ha approvato un disegno di legge che delega il Governo al recepimento delle direttive europee in cui è inserita, tra le altre, anche la direttiva in rassegna («Legge di delegazione europea 2016»). Come è noto, l'idea della legge comunitaria nacque con la cd. "legge La pergola" nel 1989 e poi venne rivista nel 2005, per un quadro su tale sistema, cfr. A. CELOTTO, *Legge comunitaria*, in *Enc giur.*, XVIII, Roma, 1995. Il sistema è stato di recente modificato con la legge n. 234 del 2012, che ha provveduto a sdoppiare le leggi, istituendo la "legge di delegazione" e la "legge europea" (su tale riforma, v. P. CARETTI, *La legge n. 234/2012 che disciplina la partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea: un traguardo o ancora una tappa intermedia?* in *Le regioni,* n. 5-6, 2012, p. 839 ss.).

([107]) Il 2016 è stato l'anno peggiore per la sicurezza informatica e tra i più colpiti c'è l'Italia. Per la prima volta, il nostro Paese è nella *top ten (*precisamente al quarto posto) degli attacchi più gravi registrati e per numero di "vittime". Sono le evidenze presentate nel rapporto *Clusit* 2017. Una particolarità italiana sono gli attacchi cc.dd. *ransomware,* quei *malware* che criptano tutti i file dell'*hard disk* chiedendo un riscatto all'utente per sbloccarli. In particolare, il principale *malware* rilevato in Italia è *"ZeroAccess",* seguito da *"Nivdort"*. Nella lista dei primi dieci *malware* riscontrati, le diverse versioni di *"GameOver Zeus"* hanno lasciato spazio anche a *"Conficker"* (frutto probabilmente dell'elevata diffusione delle varie versioni dell'omonimo *malware* già rilevata anche nel 2015) e *"Salityv3"* (un'altra novità rispetto al 2015). In particolare, l'elevata diffusione del *trojan "Nivdort"* (conosciuto anche come *"Bayrob"*) può essere ricondotta ad alcune campagne massive di *spam* rilevate soprattutto a inizio 2016. "*Sality*" è invece un *virus* identificato la prima volta nel 2003 e oggi diffuso nelle versioni 3 e 4, varianti particolarmente resistenti ai più diffusi *tool* di protezione/rimozione. Nel rapporto si legge che «Le aziende si trovano in una situazione di costante svantaggio. Purtroppo gli strumenti a loro disposizione (*firewall, antivirus,* etc.) sono sempre più in difficoltà nel fornire risposte immediate e complete. Solo una parte limitata delle aziende ha la possibilità di acquistare soluzioni così avanzate da azzerare in maniera quasi completa il rischio derivante da qualsiasi tipologia di minacce».

([108]) La fondamentale importanza dell'allocazione delle funzioni è nota e risalente nella teoria degli apparati pubblici, al riguardo uno dei principali studiosi del tema, M. S. GIANNINI, riprese e sviluppò l'idea esposta nel 1959 in uno scritto dal titolo *In principio sono le funzioni*, in *Amministrazione civile*, II, 3, pp. 11 ss., evidenziando che i problemi organizzativi, del personale e procedurali sono accessori e conseguenti a quelli sostanziali, relativi alla migliore allocazione delle funzioni amministrative.

([109]) Per approfondimenti si rinvia a C. GIUSTOZZI, Cybersecurity *e Nis: "Ecco i punti che l'Italia deve ancora sistemare",* in *www.agendadigitale.ue* del 27 ottobre 2017.

([110]) Per ciò che concerne il modello proposto per l'autorità nazionale in tema di *cyber* sicurezza, M. MENSI, in *ww.cyberaffairs.it, 7 ottobre 2017, secondo il quale «*per delineare il modello ottimale di *governance* vi sono già *best practice* a

cui far riferimento, che sono quelle in tema di protezione delle infrastrutture critiche (CIIP) a cui è dedicato uno studio dell'ENISA del 2016. Al riguardo le autorità nazionali in tema di *cyber* sicurezza possono essere una o più, già esistenti o da crearsi ad hoc, secondo un modello centralizzato (quello adottato in Francia) oppure decentrato (come in Svezia, Irlanda, Cipro, Austria, Finlandia). In tale secondo caso, perché il sistema funzioni correttamente è essenziale che sia predisposto un accurato insieme di regole per il coordinamento dei vari soggetti e che vi sia comunque un unico punto di contatto a livello nazionale. Importante altresì rafforzare la capacità operativa dei CSIRT, i gruppi di intervento in caso di incidenti, che debbono essere dotati di adeguate risorse, con la possibilità di attingere a quelle del programma DSI – *Cybersecurity Digital Service Infrastructures di Connecting Europe* (CEF)».

([111]) Per approfondimenti v. *supra* par. 1 e nota 21.