


Verso l'Agencia per la Cibersicurezza Nazionale. Una proposta concreta

Di Stefano Mele

**GIANNI &
ORIGONI**



Da tempo emerge con forza l'esigenza per il Governo italiano di ripensare – in un'ottica evolutiva – all'architettura nazionale in materia di sicurezza cibernetica, al fine di far fronte alle sempre più pressanti esigenze del settore, che richiedono ormai una più concreta focalizzazione sulle sfide da fronteggiare, oltre che maggiore coordinamento e sinergia tra tutti gli attori coinvolti.

In tal senso, le recenti parole del **Sottosegretario Franco Gabrielli** – dal 1º marzo 2021, **Autorità delegata per la Sicurezza della Repubblica** – tese a stimolare un dibattito sull'esigenza di creare una specifica agenzia che sia focalizzata sul tema della *cybersecurity* non possono che essere accolte con estremo favore.

Pertanto, senza alcuna pretesa di completezza e di profondità di analisi, ma con il solo scopo di offrire un supporto iniziale per la riflessione pubblica e per il decisore politico, di seguito si proveranno ad individuare sinteticamente le principali competenze che potrebbero rappresentare il nucleo fondativo della – quantomai auspicabile – **Agenzia per la Cibersicurezza Nazionale (ACN)**.

“L'esigenza di creare una specifica agenzia che sia focalizzata sul tema della *cybersecurity* non può che essere accolta con estremo favore.”

Perché un’Agenzia per la Cibersicurezza Nazionale (ACN)?

Il DPCM del 17 febbraio 2017, definisce, in un contesto unitario e integrato, l’attuale 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 nazionale.

Il vero elemento di novità introdotto – ormai oltre quattro anni fa – da questo DPCM è stato senz’altro il ruolo sempre più centrale e preponderante che il Dipartimento delle Informazioni per la Sicurezza (DIS) ha acquisito nel settore della sicurezza cibernetica, diventando il vero e proprio “braccio operativo” sul piano strategico del Presidente del Consiglio dei ministri, nonché il collante tra il Comitato Interministeriale per la Sicurezza della Repubblica (CISR), la pubblica amministrazione e il settore privato. Dal giorno di questa riforma, infatti, spetta al Direttore Generale del DIS il compito di adottare tutte le iniziative ritenute più idonee per definire le linee di azione utili ad innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti deputati alla prevenzione, al contrasto e alla risposta in caso di crisi cibernetica.

Questa riforma, inoltre, ha posto il Nucleo Sicurezza Cibernetica (NSC) al centro dell’azione del governo italiano, facendolo transitare dall’Ufficio del Consigliere Militare alla struttura del Dipartimento delle Informazioni per la Sicurezza (DIS) e affidandogli compiti assolutamente rilevanti sia in materia

di raccordo con tutti gli attori che intervengono a vario titolo nella materia della sicurezza cibernetica, che di prevenzione e preparazione ad eventuali situazioni di crisi cibernetica.

Una strutturazione, questa, figlia in realtà dell’urgenza con cui, nel 2013, il governo Monti dovette reagire alle pressioni dell’Unione Europea e della NATO per l’evidente ritardo nel settore della *cybersecurity* che il nostro Paese accusava nei confronti degli alleati. L’allora Presidente del Consiglio dei ministri vide proprio nel Dipartimento delle Informazioni per la Sicurezza (DIS) l’unica “ancora di salvezza” capace di potersi prendere carico del gravosissimo compito di strutturare la governance nazionale in questo settore. Ciò, malgrado questo ruolo stridesse in maniera evidente con il compito istituzionale affidato dalla Legge 124/2007 al Dipartimento delle Informazioni per la Sicurezza (DIS), ovvero quello di supportare il Presidente del Consiglio dei ministri e l’Autorità Delegata, ove istituita, nell’esercizio delle loro funzioni e assicurare unitarietà nella programmazione della ricerca informativa, nell’analisi e nelle attività operative di AISE e AISI.

È questo lo scenario – qualcuno direbbe, l’antefatto – da cui occorre partire oggi per delineare in maniera quanto più puntuale possibile l’ambizioso progetto della creazione dell’Agenzia per la Cibersicurezza Nazionale (ACN).

L'assorbimento delle competenze del Dipartimento delle Informazioni per la Sicurezza.

Il primo obiettivo di questa nuova struttura dovrebbe essere quello di riallineare i compiti del Dipartimento delle Informazioni per la Sicurezza (DIS)

Considerato il contesto, quindi, appare evidente come il primo obiettivo di questa nuova struttura dovrebbe essere quello di riallineare i compiti del Dipartimento delle Informazioni per la Sicurezza (DIS) a ciò che ci si attende da una struttura deputata alle attività di intelligence.

La norma costitutiva dell'Agenzia per la Cibersicurezza Nazionale (ACN) dovrebbe preoccuparsi, quindi, di riordinare quegli interventi normativi europei e nazionali nel settore della sicurezza cibernetica che nel tempo si sono susseguiti e che hanno posto in evidenza i limiti della nostra attuale architettura. Ciò dovrebbe avvenire partendo essenzialmente dall'assegnare all'Agenzia per la Cibersicurezza Nazionale (ACN) tutti quei compiti finora sotto la responsabilità del Dipartimento delle Informazioni per la Sicurezza (DIS) che non siano ascrivibili alle attività puramente di intelligence (anche *cyber*).

In tale ottica, quindi, dovrebbero essere ricondotte sotto la competenza dell'Agenzia per la Cibersicurezza Nazionale (ACN) tutte le iniziative identificate nell'art. 6, comma 1, del DPCM del 17 febbraio 2017, ovvero quelle idonee a definire le necessarie linee di azione di interesse generale aventi come obiettivo quello di innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti, perseguendo, in particolare, l'individuazione e la disponibilità dei più adeguati ed avanzati supporti tecnologici

in funzione della preparazione alle azioni di prevenzione, contrasto e risposta in caso di crisi cibernetica da parte delle amministrazioni ed enti pubblici e degli operatori privati.

Inoltre, considerato il ruolo di organo deputato alla gestione di eventuali crisi di natura cibernetica, si dovrebbe procedere nell'assegnare all'Agenzia per la Cibersicurezza Nazionale (ACN) anche la supervisione del **Nucleo per la Sicurezza Cibernetica (NSC)**, che, per l'effetto, dovrebbe essere trasportato funzionalmente sotto le sue competenze. Guardando, infine, al contenuto della Direttiva NIS e alle numerose previsioni in materia di sicurezza cibernetica presenti al suo interno, oltre a quanto si dirà successivamente nell'apposito paragrafo, fin da ora appare opportuno anticipare che l'Agenzia per la Cibersicurezza Nazionale (ACN) dovrebbe svolgere non solo il ruolo di **Punto di Contatto Unico** nazionale su questo tema, finora in capo al Dipartimento delle Informazioni per la Sicurezza (DIS), ma anche sovrintendere le attività del **CSIRT Italia**, che quindi andrebbe collocato al suo interno.

L'assorbimento delle competenze del Ministero dello sviluppo economico.

Il Ministro dello Sviluppo Economico, attraverso l'azione dell'odierna Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica – Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione (DGTCI-ISCTI), ha finora svolto, con un unanime e riconosciuto apprezzamento, il ruolo di area tecnica nell'ambito delle comunicazioni del Ministero. Ad essa, inoltre, nel corso degli anni, sono stati demandati anche alcuni importantissimi ruoli nel settore della sicurezza informatica, che oggi si potrebbe immaginare di traslare verso la costituenda Agenzia per la Cibersicurezza Nazionale, ovvero quello di:

Organismo di Certificazione della Sicurezza Informatica (OCSI),

che gestisce lo schema nazionale per la valutazione e certificazione della sicurezza della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione;

Centro di Valutazione (Ce.Va.),

della sicurezza informatica di prodotti e sistemi destinati a gestire i dati coperti da Segreto di Stato o di cui è vietata la divulgazione;

Centro di Valutazione e Certificazione Nazionale (CVCN),

diventato operativo di recente grazie alla normativa sul Perimetro di Sicurezza Nazionale Cibernetica, il quale prevede alla valutazione dei beni, sistemi e servizi ICT destinati ad essere impegnati all'interno delle infrastrutture tecnologiche per l'esercizio di una funzione essenziale dello Stato o per la prestazione di un servizio essenziale per gli interessi dello Stato;

Autorità competente in materia di sicurezza delle reti e dei sistemi informativi per i settori dell'energia e delle infrastrutture digitali,

compito demandato al Ministero dello sviluppo economico dal D.lgs. 18 maggio 2018, n. 65, di attuazione della Direttiva (UE) 2016/1149, meglio nota come "Direttiva NIS";

Autorità Nazionale di Certificazione della Cibersicurezza,

previsto dall'art. 58 del Regolamento (UE) 2019/881, meglio conosciuto come "Cybersecurity Act".

Infine, per coerenza sul piano della *governance*, si potrebbe valutare anche un ruolo di supporto – quantomeno – da parte dell'Agenzia nell'individuazione delle misure tecniche e organizzative adeguate per la sicurezza e l'integrità delle reti e dei servizi di comunicazione elettronica, che sempre questo Ministero svolge nella sua veste di **Autorità competente per la sicurezza delle reti di comunicazione elettronica.**





Assorbimento delle competenze del DIS e degli altri Ministeri in relazione all'attuazione della Direttiva NIS.

Il D.lgs. 18 maggio 2018, n. 65, ha dato attuazione in Italia alla Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione Europea, meglio nota come "Direttiva NIS".

Coerentemente con quanto previsto dal dettato europeo, il legislatore italiano ha previsto che l'attuazione di questa normativa fosse demandata all'**Autorità competente NIS**, prevedendo, però, che questo ruolo fosse spalmato tra tutti i Ministeri che, *ratione materiae*, potessero avere un diretto riferimento con i servizi essenziali da proteggere, ovvero:

Il Ministero dello sviluppo economico per il settore energia e per il settore infrastrutture digitali;

Il Ministero delle infrastrutture e dei trasporti per il settore trasporti;

Il Ministero dell'economia e delle finanze per il settore bancario e per il settore infrastrutture dei mercati

Il Ministero della salute per l'attività di assistenza sanitaria;

Il Ministero dell'ambiente e della tutela del territorio e del mare per il settore fornitura e distribuzione di acqua potabile.

In linea con quanto anticipato per il Ministero dello sviluppo economico all'interno dello specifico paragrafo, anche per tutti gli altri Ministeri dovrebbe trovare applicazione la traslazione di tutte le competenze derivanti dalla Direttiva NIS all'interno della nuova Agenzia per la Cibersicurezza Nazionale (ACN), che diventerebbe, quindi, l'**unica Autorità competente NIS** del nostro Paese.

Lo stesso approccio, infine, dovrà tenersi per il ruolo di **Punto di Contatto Unico**, ovvero l'organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione Europea, che, come già detto in precedenza, dovrebbe trasferirsi dal Dipartimento delle Informazioni per la Sicurezza (DIS) all'Agenzia per la Cibersicurezza Nazionale (ACN).

Stessa sorte dovrebbe essere prevista anche per le attività del **CSIRT Italia**.

Assorbimento delle competenze del DIS e del Ministero dello sviluppo economico in relazione al dettato del Perimetro di Sicurezza Nazionale Cibernetica.

L'obiettivo della normativa sul Perimetro di sicurezza nazionale cibernetica è quello di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipenda l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

Questa normativa assegna sia al Dipartimento delle Informazioni per la Sicurezza (DIS) che al Ministero dello sviluppo economico (MiSE) compiti di assoluta rilevanza per il funzionamento e la coerenza del cosiddetto "Perimetro Cyber".

In particolar modo, al Dipartimento delle Informazioni per la Sicurezza (DIS) sono demandati tutti i compiti "gestionali" degli adempimenti richiesti da questa normativa e dai suoi decreti attuativi, oltre che l'attività di verifica della *compliance* dei soggetti pubblici. Contestualmente, al Ministero dello sviluppo economico (MiSE) spettano la responsabilità delle attività del Centro di Valutazione e Certificazione Nazionale (CVCN) e quelle di verifica della compliance dei soggetti privati.

Oltre a quanto già descritto nei paragrafi relativi al trasferimento delle competenze del Dipartimento delle Informazioni per la Sicurezza (DIS) e del Ministero dello sviluppo economico (MiSE), appare indiscutibile come all'Agenzia per la Cibersicurezza Nazionale (ACN) dovrebbero essere affidati anche tutti i compiti "gestionali" affidati a queste due strutture in relazione alle previsioni del Perimetro di sicurezza nazionale cibernetica.

Assorbimento delle competenze dell’Agenzia per l’Italia digitale (AgID).

L’Agenzia per l’Italia Digitale è l’agenzia tecnica della Presidenza del Consiglio dei ministri che ha il compito di garantire la realizzazione degli obiettivi dell’Agenda digitale italiana e contribuire alla diffusione dell’utilizzo delle tecnologie dell’informazione e della comunicazione, favorendo l’innovazione e la crescita economica.

Il D.lgs. n. 82/2005, meglio noto come il Codice dell’Amministrazione Digitale (CAD), assegna all’Agenzia per l’Italia digitale (AgID) alcune funzioni che, nell’ottica di una maggiore coerenza con la riforma in atto, parrebbero fin da ora ascrivibili alle competenze dell’Agenzia per la Cibersicurezza Nazionale (ACN), ovvero senz’altro i ruoli di:

Autorità di vigilanza sui servizi fiduciari

ai sensi dell’articolo 17 del Regolamento UE 910/2014 (Regolamento eIDAS), sui gestori di posta elettronica certificata, sui soggetti accreditati che erogano servizi di conservazione a norma, nonché sui soggetti, pubblici e privati, che partecipano a SPID;

Autorità di vigilanza sull’applicazione delle misure minime di sicurezza ICT per le Pubbliche Amministrazioni

In quest’ultimo caso, inoltre, potrebbe risultare in linea con gli obiettivi della riforma prevedere anche che l’Agenzia per la Cibersicurezza Nazionale (ACN) svolga – quantomeno – un ruolo di supporto nei confronti dell’Agenzia per l’Italia digitale (AgID) nella fase di redazione e aggiornamento delle suddette misure minime di sicurezza o di altri simili interventi di settore.

Assorbimento delle competenze di tutti gli altri attori istituzionali in relazione alle attività di vigilanza sulle normative di settore.



Lo stratificarsi delle norme europee e nazionali nel settore della sicurezza cibernetica su un'architettura istituzionale "frammentata" ha fatto sì che siano attualmente numerosi gli attori istituzionali a cui è demandata la responsabilità di vigilare all'interno di quest'ambito.

Coerentemente con quanto finora affermato, l'Agenzia per la Cibersicurezza Nazionale (ACN) dovrebbe assumere, quindi, anche il compito di organismo unico per tutte le attività di vigilanza sulla corretta applicazione delle suddette norme (es., Direttiva NIS, Perimetro di Sicurezza Nazionale Cibernetica, ecc.).

L' Agenzia per la Cibersicurezza Nazionale (ACN) sarebbe il luogo più adatto per ottemperare all'obbligo europeo di costituzione del *Centro Nazionale di Competenza per lo Sviluppo Industriale, Tecnologico e della Ricerca in Materia di Cybersecurity*

Il delicato equilibrio di incardinamento e di relazioni.

Per quanto finora brevemente analizzato, appare evidente come la miglior collocazione della nascente Agenzia per la Cibersicurezza Nazionale (ACN) sia la **Presidenza del Consiglio dei ministri** (ovviamente al di fuori del Comparto Intelligence) con una diretta dipendenza dal Presidente del Consiglio. Nonostante ciò, appaiono fin da ora chiare le inevitabili – e peraltro opportune – intersezioni tra l'Agenzia e l'intero **Sistema di Informazione per la Sicurezza della Repubblica (SISR)**.

Sul piano delle altre amministrazioni, invece, appare altrettanto rilevante, da un lato, l'esigenza di salvaguardare le specifiche competenze di settore sviluppate dal **Ministero dell'Interno** (Polizia Postale e CNAIPIC), dal **Ministero della Difesa** (Comando per le Operazioni in Rete – COR), dal **Ministero degli Esteri** (mondo *cyber diplomacy*) e dal **Ministero Innovazione Tecnologica e Transizione Digitale** (mondo *e-Gov*), dall'altro, invece, quello di poter immaginare fin da

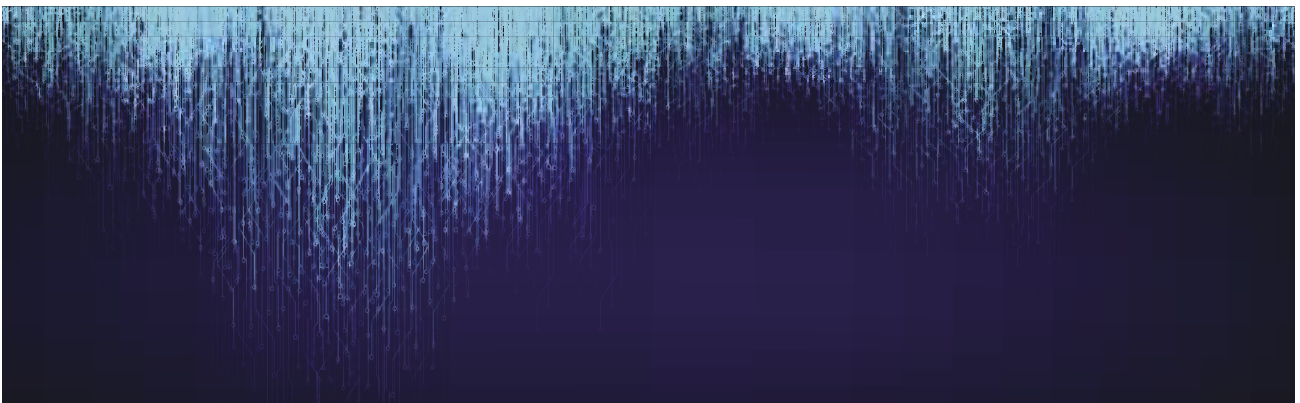
ora che queste amministrazioni possano avere proprio all'interno dell'Agenzia per la Cibersicurezza Nazionale (ACN) un proprio piccolo e agile nucleo che faccia da "congiunzione" tra i due mondi.

Questo approccio, infatti, favorirebbe la nascita e lo sviluppo di azioni, progetti e interventi nel settore della sicurezza cibernetica a più ampio respiro e a maggior impatto operativo.

Se guardiamo, infine, alle interconnessioni con l'Unione Europea, oltre a quanto già detto in materia di Direttiva NIS, appare evidente come l'Agenzia per la Cibersicurezza Nazionale (ACN) sarebbe il luogo più adatto per ottemperare anche all'ormai imminente obbligo europeo di costituzione del **Centro Nazionale di Competenza per lo Sviluppo Industriale, Tecnologico e della Ricerca in Materia di Cybersecurity**, rappresentando così, come richiesto dalla normativa, il nostro centro nazionale di coordinamento.

Un'Agenzia per la Cipersicurezza Nazionale: l'approccio degli altri Paesi.

Per saggiare la bontà del progetto e per verificare se questa traiettoria sia o meno quella predominante, appare opportuno, in chiusura, rivolgere l'attenzione alle esperienze degli altri principali Paesi europei e del Regno Unito, gli unici che possono e devono costituire un benchmark coerente rispetto alle aspirazioni dell'Italia.



La **Francia**, ad esempio, già dal 2009, attraverso la creazione dell'Agence Nationale de la *Sécurité des Systèmes d'Information* (ANSSI), ha operato una riorganizzazione molto simile a quella che oggi si auspica in Italia. Questa importantissima struttura, infatti, ha anzitutto la responsabilità sul piano politico-strategico del tema della sicurezza cibernetica.

Essa svolge il ruolo, appunto, di autorità nazionale per la difesa dei sistemi di informazione e supporta il Primo Ministro francese su questi temi attraverso l'azione del *Secrétaire Général de la Défense et de la Sécurité Nationale* (SGDSN), a cui riporta. Su un piano maggiormente operativo, inoltre, l'ANSSI racchiude al suo interno anche le competenze del *Centre Gouvernemental de Veille, d'Alerte et de Réponse aux Attaques Informatiques*, ovvero il CERT-FR, così come quelle del *Centres d'Évaluation de la Sécurité des Technologies de l'Information* (CESTI), che si occupa della certificazione dei livelli di sicurezza cibernetica dei prodotti.

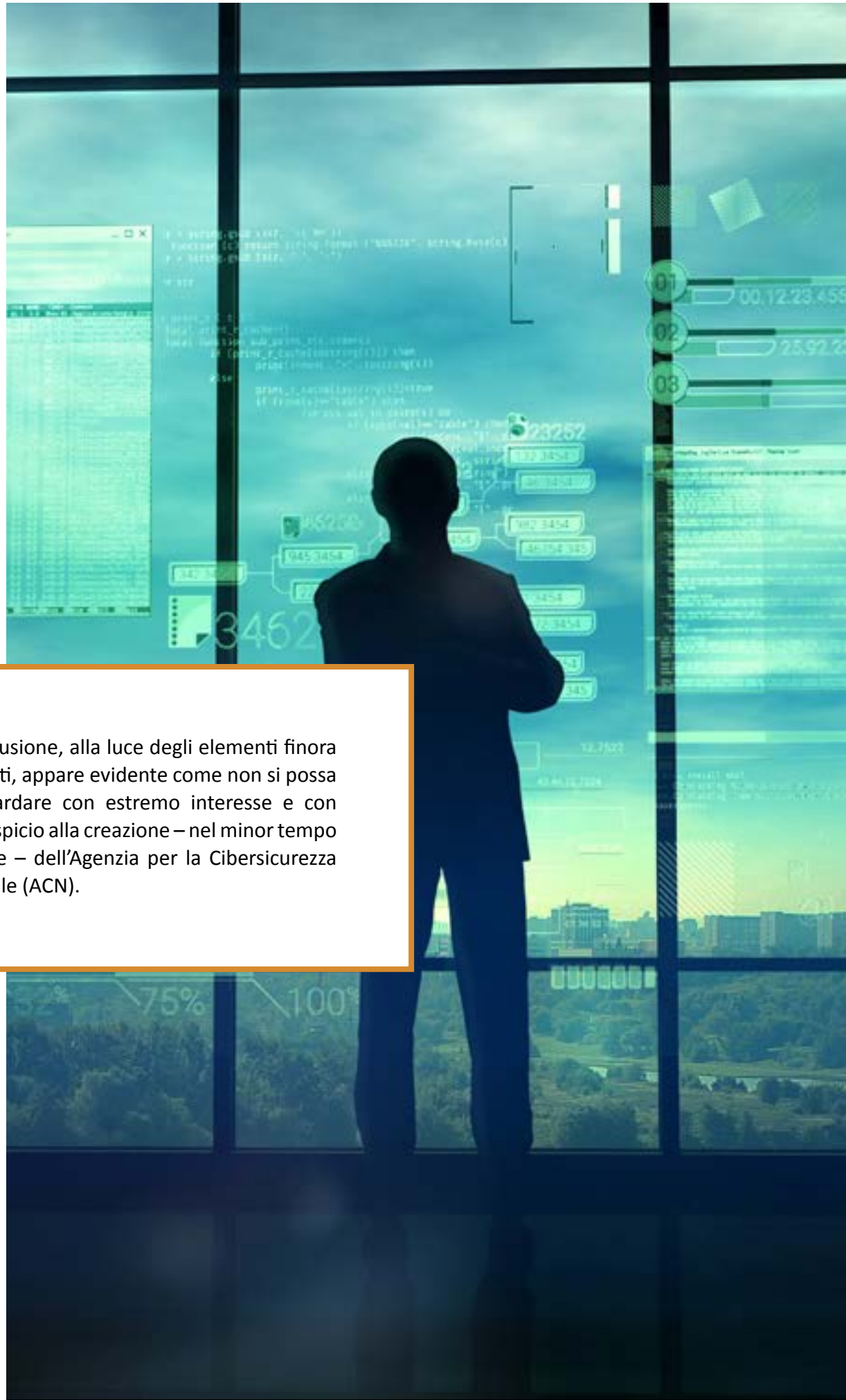
Su una linea molto simile a quella francese si è posto anche il **Regno Unito** con la costituzione, nel 2016, del proprio *National Cyber Security Centre* (NCSC). Questa importantissima struttura, infatti, rappresenta l'autorità indipendente per la sicurezza cibernetica del Regno Unito.

Essa funge da punto di contatto unico su questi temi per tutto il settore industriale e delle PMI, per le agenzie governative e la pubblica amministrazione in generale, fino alle università e ai partner internazionali.

L'NCSC, peraltro, sin dalla sua creazione, ha raccolto l'eredità e le competenze del vecchio CERT-UK e del *Centre for Protection of National Infrastructure* e rappresenta, oggi, anche il fautore dei principali progetti di informazione e formazione sui temi della *cybersecurity*.

La **Germania**, infine, pur discostandosi dagli altri attori qui richiamati in relazione alla strutturazione dell'architettura nazionale in tema di sicurezza cibernetica, assegna al *Bundesamt für Sicherheit in der Informationstechnik* (BSI), ovvero all'Ufficio Federale per la Sicurezza delle Informazioni, il ruolo di propria autorità per la *cybersecurity*. Infatti, benché la *cyber strategy* tedesca del 2011 abbia creato – e il suo aggiornamento del 2016 abbia confermato – il *Cyber-Sicherheitsrat* (Cyber-SR), ovvero il Consiglio per la Sicurezza Cibernetica, affidando ad esso il ruolo permanente di organo federale di consiglio sul piano strategico per i temi della *cybersecurity*, il BSI costituisce il reale esecutore dell'agenda governativa su questi temi e il punto di sintesi tra il piano strategico e quello operativo.

In tale ottica, peraltro, sarà senz'altro molto interessante seguire la sua evoluzione e il suo ampliamento di poteri alla luce dell'ormai imminente riforma della governance in materia *cyber* contenuta nel cosiddetto "IT Security Act 2.0".



In conclusione, alla luce degli elementi finora analizzati, appare evidente come non si possa che guardare con estremo interesse e con ogni auspicio alla creazione – nel minor tempo possibile – dell’Agenzia per la Cibersicurezza Nazionale (ACN).

Verso l'Agencia per la Cibersicurezza Nazionale. Una proposta concreta

Il presente documento viene consegnato esclusivamente per fini divulgativi. Esso non costituisce riferimento alcuno per contratti e/o impegni di qualsiasi natura.

Per ogni ulteriore chiarimento o approfondimento Vi preghiamo di contattare:

Stefano Mele

Partner

Proprietà Intellettuale, TMT e Cybersecurity

Roma/Milano

+39 06 478751/+39 02 763741

smele@gop.it

GIANNI &
ORIGONI