La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*

Simone Poletti

Abstract

L'elaborato si pone l'obiettivo di analizzare l'innovativo settore della *cybersecurity* e nello specifico il contrasto ai più critici incidenti informatici lesivi della sicurezza nazionale. Il saggio muove dall'analisi delle caratteristiche peculiari e delle contingenze che hanno imposto un cambio di prospettiva nella politica criminale di contrasto a tali condotte criminose, e successivamente indaga la normativa unionale e nazionale con uno specifico *focus* sulla struttura e sui contenuti delle norme istitutive del Perimetro di sicurezza nazionale cibernetica (l. 133/2019) e dell'Agenzia per la cybersicurezza nazionale (l. 109/2021).

The current paper aims to analyse the cybersecurity branch, and in particular the opposition against the most critical cyberattacks concerning national security. This paper begins with the analysis of the peculiarities and the contingencies that have changed policymakers strategies against these criminal behaviours. It then studies the European and national laws with a particular focus on the structures and the contents that establish the national cybersecurity perimeter (l. 133/2019), and those that establish the Cybersecurity national agency (l. 109/2021).

Sommario

1. Una prospettiva innovativa: la nascita del Dominio Cibernetico. – 2. La prospettiva sovranazionale. – 3. Le normative nazionali: l'istituzione del Perimetro di Sicurezza Nazionale Cibernetica e dell'Agenzia per la Cybersicurezza Nazionale

Keywords

incidenti informatici – perimetro di sicurezza nazionale cibernetica – resilienza – Direttiva NIS – transnazionalità

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1. Una prospettiva innovativa: la nascita del Dominio Cibernetico

A partire dallo scorso decennio, all'interno delle grandi potenze economiche mondiali, si è sviluppata una sempre più sentita necessità di concepire la "sicurezza" come un elemento non legato esclusivamente alla sua fisicità e ad una sua estrinsecazione nel mondo esteriore, quanto piuttosto ad un elemento multidimensionale da affrontare in maniera olistica per essere in grado di delineare tutte le sfaccettature in cui essa si concettualizza. Questa innovativa lettura della "sicurezza" ha portato grandi attenzioni alla sua concezione dematerializzata e digitale, generando uno sviluppo esponenziale dell'analisi e degli strumenti per la tutela della sicurezza cibernetica. Ad avvalorare questa affermazione, si consideri il recente riconoscimento da parte della NATO della presenza di un quinto dominio da proteggere (in aggiunta ai quattro domini tradizionali: terreste, marittimo, aereo e spaziale): il dominio cibernetico[1].

La nascita del dominio cibernetico e di conseguenza le istanze di difesa dello stesso, sono determinate dall'utilizzo massivo di strumenti informatici al fine di perpetrare crimini; da una lettura dei rapporti più rilevanti in tema di sicurezza informatica (si pensi ad esempio al rapporto Clusit[2]) è manifesto l'incremento esponenziale dell'utilizzo di dispositivi informatici per finalità illecite. Circa le modalità di esecuzione, bisogna sottolineare la varietà di forme che li caratterizzano (*malware,* sfruttamento di vulnerabilità*, advance persistent threat,* attacchi *DDOS*, ecc.) che sfociano in un utilizzo preponderante di *malware* tendenzialmente di tipo *crypto ransomware*[3]. Un aspetto collaterale che tuttavia riveste un primario interesse per il tema, verte sulle modalità che hanno reso massivo ed esponenziale il fenomeno criminoso, nonostante il numero ristretto di soggetti in possesso delle competenze necessarie per provvedere alla realizzazione dei *software* malevoli. La spiegazione di questa situazione peculiare è rintracciabile nel fenomeno del cd. *malware as a service*[4], da intendersi come vero e proprio mercato digitale – di natura illecita – nel quale un limitato numero di soggetti altamente qualificati nel settore informatico sviluppa *malware* al fine di venderli o porli in locazione a terzi, i quali, seppur inetti con riguardo alle competenze informatiche, sono in grado di reperire ed utilizzare facilmente tali *malware* contribuendo di fatto all'esponenziale crescita degli attacchi informatici.

La nuova centralità della tutela del dominio cibernetico ha portato alla realizzazione di una politica criminale appositamente congegnata per aderire alle particolari caratteristiche degli attacchi informatici, quali la dematerializzazione e l'aterritorialità che

---

[1] A. Marziali, *Cybersecurity: come la NATO si adatta alle nuove sfide | ISPI (ispionline.it),* in *ispionline.it*, 23 giugno 2020.

[2] Si veda *Rapporto Clusit 2022 sulla sicurezza ICT in Italia*, disponibile in clusit.it, marzo 2022, 13 ss.

[3] *Rapporto Clusit 2021 sulla sicurezza ICT in Italia*, disponibile in clusit.it, 2021, 28; E. Kalaimannan - S. John K. - T. DuBose - A. Pinto, *Influences on ransomware's evolution and predictions for the future challenges*, in *Journal of Cyber Security Technology*, 1(1), 2017, 27 ss.

[4] M. Macdonald - R. Frank, *The network structure of malware development, deployment and distribution*, in *Global Crime*, 18(1), 2017, 49 ss.; A.S.A. Bander - M.A. Maarof - S.Z.M. Syed, *Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions,* in *Computers & Security*, 74, 2018, 147-148.

comportano la perdita di rilevanza dei confini nazionali e della spazialità, dal momento che la digitalizzazione permette di operare da remoto a partire da ogni angolo di mondo. La linea di demarcazione che ha portato alla creazione di una politica criminale *ad hoc* focalizzata sul contrasto *ex ante* del fenomeno – mediante l'inserimento di obblighi in capo a soggetti privati, di ingenti sanzioni amministrative pecuniarie e, nel caso italiano, di una fattispecie incriminatrice di pericolo astratto – è determinata dalla severità dell'attacco perpetrato (da valutarsi sulla base del numero di soggetti e dell'area geografica coinvolta, nonché della messa in pericolo per la sicurezza nazionale). Questa tipologia di attacchi, lesiva per l'appunto della sicurezza nazionale, risulta di grande rilievo in quanto è in grado di impedire lo svolgimento di funzioni essenziali o l'erogazione di servizi essenziali, cagionando importanti disservizi sul territorio in grado di ledere diritti costituzionalmente riconosciuti ai cittadini (diritto alla salute, diritto all'istruzione, diritto alla sicurezza ecc.). Proprio la gravità di questo frangente ha spinto alla configurazione ed alla implementazione (sia a livello unionale che a livello nazionale) di misure appositamente congegnate, caratterizzate da elementi *sui generis*; in primo luogo esse si distinguono per la loro spiccata natura preventiva basata sull'assunto per cui il respingimento della totalità degli attacchi informatici risulti impossibile – seppure fortemente implementabile mediante misure di elevato tasso tecnico quali lo sviluppo di strumenti di intelligenza artificiale appositamente predisposti per rilevare nuove tipologie di *malware*[5] – e sul dato incontrovertibile che anche un singolo attacco di severità elevata o critica ai danni di infrastrutture o servizi, in grado pertanto di cagionare una lesione alla sicurezza nazionale, avrebbe conseguenze disastrose; questo motivo ha portato alla creazione di infrastrutture ed architetture cibernetiche congegnate nell'ottica di generare un'elevata sicurezza dei sistemi informatici, al contempo riducendo il numero di attacchi in grado di superare le protezioni ed aumentando la resilienza e la resilienza operativa[6] dei sistemi informatici[7].

Urge sottolineare come questa particolare tipologia di attacchi può rientrare tra le condotte idonee alla configurazione di una cd. *Cyber war* [8], dal momento che nei conflitti contemporanei sempre più spesso a fianco alle condotte tradizionali si pongono azioni altamente digitalizzate ed informatizzate per colpire le infrastrutture critiche – militari e civili – come strategia di indebolimento dell'avversario.

In secondo luogo è fondamentale notare come gli strumenti di contrasto al fenomeno

[5] Si vedano gli interventi di R. Forsi - M. Pereira all'interno del *webinar "*Ransomware, l'intelligenza artificiale a supporto della cybersecurity nella PA e nelle imprese*"*, in cybersecitalia.it, 24 settembre 2021.

[6] Da intendersi come la capacità di un sistema informatico di erogare servizi e rimanere parzialmente in funzione nel momento in cui sta subendo un attacco informatico.

[7] Per un approfondimento sull'importanza del tema della resilienza dei sistemi e del frangente preventivo, si veda l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, Comunicazione congiunta al Parlamento europeo e al Consiglio, *Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l'Ue,* in *ec.europa.eu*, 13 settembre 2017.

[8] Per *Cyber War* si intende un conflitto di natura militare perpetrato in un contesto diverso da quello tradizionale, che si svolge all'interno del dominio cibernetico, con il fine di arrecare danni e malfunzionamenti alle infrastrutture critiche di un Paese mediante l'utilizzo di attacchi informatici. Per un approfondimento sul tema si veda A. Giannulli - A. Curioni, *Cyber war. La guerra prossima ventura,* Fano, 2019.

debbano essere calati in un'ottica unionale ancor prima di quella nazionale in quanto, a causa degli elementi peculiari degli attacchi informatici precedentemente richiamati, la dimensione nazionale e i rigidi confini territoriali nulla hanno a che vedere con queste condotte criminali, caratterizzate da un'elevata flessibilità nell'utilizzo di *server, internet service provider* e reti straniere che permettono di eludere gli strumenti di contrasto operanti in maniera rigida all'interno dei soli confini nazionali.

Un terzo ed ultimo elemento distintivo di tali strumenti è caratterizzato dal ruolo fondamentale che si instaura tra i soggetti pubblici e i soggetti privati, rendendo il partenariato tra essi un perno fondamentale per un efficace ed efficiente funzionamento delle architetture cibernetiche sviluppate[9]. Ciò è determinato dalla rapidità con cui la tecnologia evolve e dalla necessità di ingenti investimenti per mantenere sempre aggiornati gli strumenti e le architetture di contrasto, aspetto che è svolto in maniera più efficiente se ai soggetti governativi viene affiancata un'ampia platea di soggetti privati interessati alla massimizzazione del profitto e all'aggiornamento delle proprie tecnologie.

Questo approccio integrato permette peraltro di incrementare notevolmente l'*awareness* e la *cyber hygene*[10] tra i soggetti privati, elemento di primaria importanza per ridurre l'incidenza e il numero di attacchi informatici con esito positivo.

In termini penalistici tale fenomeno normativo risulta particolarmente interessante dal momento che, con tali previsioni, si è configurato un nuovo paradigma penalistico volto all'anticipazione della tutela penale, necessaria per controbilanciare e rendere maggiormente efficace la politica criminale repressiva contenuta all'interno di fattispecie incriminatrici tradizionali che, seppur ben congegnate, risultano inefficaci a causa delle peculiari caratteristiche che contraddistinguono gli attacchi informatici.

2. La prospettiva sovranazionale

Grazie alla consapevolezza che si è raggiunta sul tema, è stata sviluppata, all'interno dell'Unione europea, un'azione di contrasto armonizzata del fenomeno. Da un punto di vista normativo, l'assetto è variegato sia per la presenza di previsioni nazionali ed unionali, sia per la presenza di diverse tipologie di atti – direttive, regolamenti, comunicazioni ecc. – che generano un'elevata disorganicità sul tema. A livello unionale si possono rilevare due principali misure volte al rafforzamento dei sistemi cibernetici europei: la direttiva (UE) 1148/2016 cd. Direttiva NIS (la quale ha subito un recente aggiornamento) [11] – *Network and Internet Security* – e il regolamento (UE) 881/2019, cd.

[9] L'essenzialità del coinvolgimento dei privati e dei loro investimenti nel settore tecnologico è fortemente richiamata anche dall'ex Direttore dell'ACN Roberto Baldoni. Si veda Palazzo Chigi, *Cybersicurezza, Gabrielli e Baldoni presentano la Strategia nazionale,* in ***youtube.com,*** 25 maggio 2022.

[10] Da intendersi come l'insieme delle buone pratiche che l'utente medio deve praticare nell'utilizzo di dispositivi informatici, al fine di ridurre notevolmente la possibilità di subire un attacco informatico. Per un approfondimento sul tema si veda R. Proli - E. Valguarnera, *Il Cybercrime e le strategie dell'Unione Europea. (dirittopenaleglobalizzazione.it),* in ***dirittopenaleglobalizzazione.it***, 28 agosto 2018.

[11] 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, GU 2016 L

Cybersecurity Act [12].

Con la Direttiva NIS si configura, per la prima volta, l'individuazione di alcuni soggetti privati o pubblici – identificati come operatori di servizi essenziali e fornitori di servizi digitali – tenuti a rispettare alcuni obblighi in tema di innalzamento delle misure di sicurezza per i propri sistemi informatici ed in tema di notifica degli incidenti rilevanti subiti. La *ratio* di questa previsione è di garantire una maggior sicurezza dei sistemi e di creare un sistema di comunicazione – strutturato sulla presenza di un punto di contatto unico per ogni Stato membro e sulla presenza di un *cooperation group* a livello unionale per agevolare lo scambio di informazioni – che sia in grado di diffondere le caratteristiche degli incidenti rilevanti subiti al fine di mettere in allerta tutti gli altri operatori rientranti nel perimetro della Direttiva NIS per scongiurare ulteriori attacchi. Seppur il modello e l'ottica di realizzazione sia lodevole, a distanza di più di un lustro è stato possibile notare, oltre a diversi effetti positivi generati, un elenco di difetti che hanno contraddistinto la direttiva; gli aspetti critici sono molteplici, quale l'assenza di un termine specifico entro cui provvedere alla notifica (la quale deve avvenire "senza ritardo"), l'elevata discrezionalità in capo agli Stati membri sia nella individuazione delle autorità competenti sia nella possibilità di comminare sanzioni ai soggetti che non hanno ottemperato alle previsioni della direttiva; tuttavia il difetto più importante riguarda l'eccessiva discrezionalità conferita agli Stati membri nell'identificazione degli operatori di servizi essenziali che ha portato i diversi Stati a procedere "in ordine sparso" utilizzando – a seconda dei casi – un modello granulare o un modello non granulare [13] che ha portato ad una mancata armonizzazione – ravvisata dai *report* del *cooperation group* [14] – aggravata anche dal fatto che le specifiche soglie per l'identificazione degli operatori di servizi essenziali (che riguardano l'impatto dell'incidente, il numero di utenti ed il territorio geografico coinvolti) variano da Stato membro a Stato membro, comportando un inevitabile naufragio della previsione unionale. Queste conclusioni sono possibili grazie alle oculate valutazioni di *assessments* stabilite dalle istituzioni europee, che hanno ottenuto tali riscontri grazie all'apertura di un proficuo dialogo con le società ed i privati europei [15], generando per l'appunto quel partenariato necessa-

194/1*;* direttiva (UE) 2022/2555 del 14 dicembre 2022, del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), GU 2022 L 333/80.

[12] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»), GU 2019 L 171/15.

[13] Per modello granulare bisogna intendere un modello che individua molti differenti sotto-settori all'interno di un macro settore, permettendo una maggior capillarità e specificità nell'individuazione dei soggetti. Il modello non granulare, viceversa, configura l'individuazione di un numero particolarmente ridotto e generico di sotto-settori e in taluni casi si limita all'indicazione di un unico macro settore senza ulteriori specificazioni. Per un'approfondita analisi sul tema si veda *Relazione della Commissione al Parlamento europeo e al Consiglio, di valutazione della coerenza degli approcci adottati dagli stati membri per l'identificazione di servizi conformemente all'articolo 23, paragrafo 1, della direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi*, COM (2019), in ec.europa.eu, 28 novembre 2019.

[14] Cooperation Group, *Annual Report NIS Directive Incidents 2019,* in ec.europa.eu, December 2020.

[15] European Commission, *Revision of the Network and Information Security Directive: Questions and Answers*,

rio per uno sviluppo organico e sostenibile degli strumenti di protezione cibernetica. Ciò ha recentemente portato all'accoglimento della proposta di aggiornamento della Direttiva NIS[16], mediante l'emanazione di un atto volto ad ampliare i settori inseriti all'interno della misura ed alla risoluzione delle problematiche sopra indicate[17].

Per quanto invece concerne il cd. *Cybersecurity Act,* l'obiettivo della normativa è parzialmente difforme in quanto il fine ultimo mira alla creazione di un mercato digitale europeo unico caratterizzato da sicurezza ed efficienza per tutti gli operatori e gli utilizzatori[18]. Per garantire ciò, tuttavia, non individua comuni obblighi di implementazione di misure di sicurezza, bensì prevede la creazione di un quadro di certificazione europea per alcuni prodotti *ICT,* consistente in un processo volto alla verificazione della sussistenza dei requisiti minimi previsti dagli *standard* in materia, in grado di verificare la sicurezza cibernetica e l'adeguatezza informatica del bene, con la finalità di garantire l'autenticità, l'idoneità e la sicurezza informatica dello stesso. In tal modo il regolamento mira ad ottenere la *security by design*, cioè la creazione di *software, hardware* ed applicativi europei che siano sicuri ed affidabili fin dalla loro progettazione e non solo in un secondo momento con l'applicazione di idonee misure di sicurezza[19].

Questa previsione, per quanto ad oggi sia rimessa alla mera volontà degli Stati membri, risulta considerevolmente importante anche per il superamento di uno dei maggiori ostacoli che portano le società a non investire in *cybersecurity*, cioè l'incapacità di vedere l'incremento della sicurezza cibernetica dei propri sistemi come un investimento, ma di considerarlo esclusivamente come una spesa da sostenere. Generando un prodotto certificato, autentico e sicuro, riconosciuto come tale a livello unionale, esso ottiene un maggiore valore intrinseco a seguito delle sue comprovate specificità che pertanto pongono le basi per considerarlo un investimento[20].

Per completare il sistema tracciato dal *Cybersecurity Act* bisogna richiamare la fondazione dell'*European Cybersecurity industrial, technology and research competence centre,* cioè il centro di competenza di Bucarest che avrà il compito di mettere in comunicazione il settore pubblico e privato di tutta l'Unione europea per convogliare fondi ed investimenti destinati allo sviluppo della sicurezza cibernetica all'interno dell'Unione[21].

---

in digital-strategy.ec.europa.eu, 19 October 2021; M. Negreiro, European Parliament Research Service, *Briefing – EU Legislation in Progess: The NIS 2 Directive. A high common level of cybersecurity in the EU,* at europarl.europa.eu, December 2021; European Commission, *Commission Staff working document, executive summary of the impact assessment report*, SWD (2020), in eur-lex.europa.eu, 16 December 2020; M. Giuliana Antonio, *Direttiva NIS, la grande riforma: il processo di revisione e i prossimi passi,* in *agendadigitale.eu*, 5 ottobre 2020.

[16] European Commission Proposal, COM/2020/823 final, *Proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive /EU) 2016/1148*, at eur-lex-europa.eu, 16 December 2020.

[17] Direttiva (UE) 2022/2555, cit.

[18] Per una disamina completa sul tema, si veda F. Campara, *Il cybersecurity act,* in A. Contaldo - D. Mula (a cura di), *Cybersecurity Law: disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa, 2020, 57 ss.

[19] R. Proli - E. Valguarnera, *Il Cybercrime e le strategie dell'Unione Europea,* cit.

[20] F. Campara, *Il cybersecurity act,* cit., 57 ss.

[21] Per una panoramica sullo sviluppo della struttura, le competenze ed il funzionamento si veda *cybersecurity-centre.europa.eu.*

3. Le normative nazionali: l'istituzione del Perimetro di Sicurezza Nazionale Cibernetica e dell'Agenzia per la Cybersicurezza Nazionale

Sul piano nazionale l'assetto normativo è peculiare, in quanto il legislatore non si è limitato alla ratifica della Direttiva NIS, bensì ha provveduto alla creazione di uno strumento maggiormente pregnante, quale il Perimetro di Sicurezza Nazionale Cibernetica, mediante l'emanazione del d.l. 105/2019, convertito in l. 133/2019[22].
L'assetto normativo è variegato in quanto oltre alla previsione del decreto convertito in legge, sono stati emanati quattro differenti decreti del Presidente del Consiglio dei Ministri ed un decreto del Presidente della Repubblica; il rimando all'utilizzo di tali previsioni è indicato all'interno della legge sul "Perimetro" che ha rimesso a norme di rango inferiore, da emanare con una cadenzata scansione temporale, una serie di previsioni particolarmente tecniche che difficilmente sarebbero potute essere stabilite in sede parlamentare, garantendo in questo modo una maggior efficienza e celerità nella creazione dell'architettura prestabilita. Urge notare che, per l'emanazione di tali fonti di rango secondario, il legislatore ha saggiamente affiancato al Presidente del Consiglio dei ministri il Comitato Interministeriale per la Sicurezza della Repubblica (CISR), per garantire una maggiore intersettorialità e trasversalità delle previsioni.
Da un punto di vista contenutistico il primo aspetto da sottolineare è la *ratio* della previsione, espressa dall'art. 1, c. 1, che sancisce la garanzia di un'elevata tutela dei sistemi informatici e delle reti che, se interrotti o danneggiati, sono in grado di cagionare un pregiudizio per la sicurezza nazionale [23]. Da questa lettura si può osservare a chiare lettere come la tutela prevista dal "Perimetro" riguardi esclusivamente gli incidenti di particolare gravità in grado di mettere in pericolo lo Stato e la sua sicurezza, risultando estranei alla previsione gli incidenti minori che riguardano la criminalità comune, non in grado di cagionare un pregiudizio sì gravoso. La necessità di provvedere a questa distinzione è quanto mai sentita, dal momento che l'inserimento di un soggetto all'interno del "Perimetro" è tutt'altro che indifferente per tale soggetto, che risulta onerato da alcuni obblighi e limitazioni particolarmente stringenti ed economicamente rilevanti di cui deve farsi carico; per siffatto motivo è sancita l'esclusione da questa previsione di tutti quei soggetti dai quali non possa scaturire una lesione alla sicurezza nazionale in caso di attacco informatico. D'altro lato un'estensione eccessiva di questa previsione, al di fuori del perimetro di tutela della sicurezza nazionale, genererebbe un'eccessiva anticipazione della tutela penale con conseguente torsione del principio di offensività, ed obblighi eccessivamente ingenti a fronte di un pericolo di insufficiente gravità. A conferma di quanto affermato, i requisiti che permettono alle autorità competenti di individuare i soggetti da inserire all'interno del "Perimetro" sono stringenti e riguar-

[22] L. 133/2019, recante "Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica" (G.U. 272 del 20 novembre 2019).

[23] Art. 1, c. 1, l. 133/2019: «[…] assicurare un livello elevato di sicurezza delle reti, dei servizi informativi e dei sistemi informatici […] da cui dipende l'esercizio di una funzione essenziale dello stato, ovvero la prestazione di un servizio essenziale […] dal cui malfunzionamento, interruzione […] ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale».

dano esclusivamente gli operatori che erogano servizi essenziali o svolgono funzioni essenziali, ma che al contempo devono essere dotati di una rete e di sistemi informatici che se interrotta o distrutta sia idonea a cagionare una lesione alla sicurezza nazionale. Una volta individuati dalle autorità competenti, tali soggetti, notificati del loro inserimento all'interno del "Perimetro", debbono provvedere alla comunicazione – entro sei mesi – dell'elenco della componentistica *ICT* e delle proprie reti e sistemi informatici, elenco che dovrà essere aggiornato in caso di modifiche o di nuove acquisizioni; la finalità è di garantire la conoscenza approfondita di tutti i sistemi informatici e delle componentistiche che sono parte del "Perimetro" al fine di valutarne e monitorarne l'affidabilità, a protezione della sicurezza nazionale. Interessante notare come, al fine di garantire una più elevata protezione dei sistemi e solo a determinate condizioni [24], sia conferito in capo al Presidente del Consiglio dei ministri il potere di interrompere un sistema informatico a seguito di una crisi cibernetica, per moderare gli effetti negativi cagionati dall'attacco.

Oltre all'onere sopracitato, i soggetti parte del "Perimetro" sono sottoposti a tre differenti obblighi, i quali devono essere rispettati a pena di subire le sanzioni pecuniarie disposte dall'art. 1, c. 9, della legge sul "Perimetro"[25]; inoltre, in caso di mancata comunicazione o false informazioni ai fini dell'aggiornamento degli elenchi della componentistica rientrante nel "Perimetro", l'art. 1, c. 11, della medesima norma predispone un reato di pericolo astratto [26] – si tratta dell'unica fattispecie incriminatrice penale inserita dalla previsione normativa – che punisce, mediante la reclusione da uno a cinque anni, il soggetto agente che operi con il fine di ostacolare le procedure di verificazione dei requisiti per l'inserimento all'interno del "Perimetro" [27]. Sulla bontà di tale

[24] Le condizioni sono particolarmente stringenti e sono contenute all'interno dell'art. 5, l. 133/2019. Queste consistono nella presenza di una situazione oggettiva di crisi cibernetica o di imminente e grave rischio per la sicurezza nazionale, nella indispensabilità della disattivazione di un sistema o una rete, nella durata minore possibile di tale assenza di fruibilità della rete ed infine del requisito di proporzionalità.

[25] Art. 1, c. 9, l. 133/2019. Nello specifico le singole sanzioni riguardano: «[...] il mancato adempimento degli obblighi di predisposizione e di aggiornamento dell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera b); il mancato adempimento dell'obbligo di notifica di cui al comma 3, lettera a); l'inosservanza delle misure di sicurezza di cui al comma 3, lettera b); la mancata comunicazione di cui al comma 6, lettera a), nei termini prescritti; l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e l'espletamento dei servizi informatici di cui al comma 2, lettera b), in violazione delle condizioni imposte dal CVCN o in assenza del superamento dei test di cui al comma 6, lettera a); la mancata collaborazione per l'effettuazione delle attività di test di cui al comma 6, lettera a); il mancato adempimento delle prescrizioni indicate dal Ministero dello sviluppo economico o dalla Presidenza del Consiglio dei ministri in esito alle attività di ispezione e verifica; il mancato rispetto delle prescrizioni di cui al comma 7, lettera b)».

[26] Art. 1, c. 11, l. 133/2019: «Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote».

[27] Per una disamina completa sulla fattispecie incriminatrice si rimanda a L. Picotti, M.R. Vadalà, *La nuova legge sulla sicurezza cibernetica (l. 133/19): i profili penalistici | Sistema Penale | SP"*, in *sistemapenale.it,* 5

previsione si pongono alcuni dubbi; se da un lato la struttura della fattispecie come reato di pericolo astratto può essere parzialmente accettata per l'elevata importanza del bene giuridico tutelato, d'altro lato questa decisione presta il fianco alle critiche tradizionali che accompagnano i reati di pericolo astratto circa la torsione del principio di offensività.

Un ulteriore problema, di carattere generale, riguarda il rischio di incrementare una già esasperata proliferazione di fattispecie incriminatrici *extra codicem* generando disorganicità e confusione tra le diverse previsioni. Questo aspetto vale non solamente per la fattispecie incriminatrice bensì anche per le norme settoriali in tema di sicurezza cibernetica che, a seguito della creazione di due previsioni di carattere generale quali le leggi istitutive del "Perimetro" e dell'Agenzia per la Cybersicurezza Nazionale, rischiano di creare sovrapposizioni pericolose di ardua interpretazione. Si auspica un riordino della materia a seguito della definitiva entrata in funzione dell'Agenzia, momento focale per una prima valutazione completa sull'architettura predisposta e sul suo funzionamento.

Conclusa tale parentesi inerente alle sanzioni predisposte, il primo obbligo è previsto dal d.P.C.M. 81/2021[28], in ottemperanza all'art. 1, c. 3, della legge sul "Perimetro", ed impone di apportare ed implementare le idonee misure di sicurezza cibernetica ai propri sistemi; queste misure devono essere predisposte con finalità differenti tra loro in quanto devono essere in grado di aumentare la possibilità di identificazione dei punti deboli della propria architettura cibernetica, incrementare il livello di protezione dei sistemi ed essere in grado di rilevare e rispondere alle eventuali minacce ravvisate, oltre al fatto di garantire un ripristino dei sistemi celere ed adeguato a seguito di un incidente.

Il secondo obbligo – disposto dal medesimo decreto di cui sopra, ai sensi dell'art. 1, c. 2, lett. b) – risulta particolarmente importante ai fini dell'incremento della sicurezza degli operatori, dal momento che prevede la necessità per i soggetti parte del "Perimetro" di notificare celermente allo CSIRT nazionale (*Computer Security Incident Response Team*[29]) l'incidente, allegando le sue caratteristiche; la finalità di questa notifica è duplice: da un lato lo CSIRT nazionale fornisce direttive al soggetto colpito al fine di ripristinare quanto più velocemente possibile e con le modalità idonee i sistemi informatici colpiti, d'altro lato permette allo CSIRT nazionale di comprendere le caratteristiche dell'attacco e le finalità, in modo tale da creare *patch,* aggiornamenti e *best practices* da condividere con tutti gli altri soggetti del "Perimetro" per limitare l'ondata infettiva del *malware* o più in generale dell'attacco perpetrato.

L'aspetto più discusso permane quello legato alle tempistiche, le quali richiedono la notifica entro un'ora nel caso di incidenti gravi (ad esempio *system failure* o danneggiamento di un sistema informatico) e di sei ore per gli incidenti meno gravi (ad esempio

dicembre 2019.

[28] D.P.C.M. 81/2021, recante "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informatici e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n.105, convertito, con modificazioni, dalla legge 18 novembre 2019, n.133, e di misure volte a garantire elevati livelli di sicurezza" (G.U. 138 dell'11 giugno 2021).

[29] Il *Computer Security Incident Response Team* (CSIRT) è l'organismo che si occupa della risposta e del recupero del sistema informatico colpito dall'attacco informatico. Le sue competenze sono di elevata tecnicità ed il suo ruolo risulta centrale nel contrasto agli attacchi cibernetici.

le condotte di infiltrazione e di *lateral movement* all'interno dei sistemi); è stato riscontrato dagli esperti del settore come questo frangente temporale sia eccessivamente limitato per comprendere la tipologia dell'attacco, redigere il rapporto e notificarlo allo CSIRT mentre contestualmente si opera per delimitare e contrastare la minaccia[30]. A render ancor più oneroso l'obbligo, recentemente è stato inserito un ulteriore aggravio alla notifica – per la quale bisogna provvedere entro settantadue ore – per gli incidenti subiti dai soggetti parte del "Perimetro", ai danni di sistemi informatici di loro proprietà ma non facenti parte del "Perimetro"[31]. Questa previsione pare esulare dalla *ratio* di tutela della sicurezza nazionale, seppur finalizzata ad aumentare la sicurezza dei sistemi informatici nazionali. A mero titolo informativo bisogna indicare la presenza della possibilità di provvedere ad una notifica volontaria (di cui all'art. 4 del d.P.C.M. 81/2021), anche per quei casi che non rientrano all'interno del novero di incidenti per i quali la notifica risulta obbligatoria; permangono tuttavia notevoli dubbi circa le modalità, dal momento che la norma risulta silente sul tema.

L'ultimo obbligo – in ottemperanza all'art. 1, c. 6, della legge sul "Perimetro" – è posto in tema di *procurement*, da intendere quale fase di acquisizione di nuova componentistica *hardware* e *software* da parte dei soggetti all'interno del "Perimetro". La finalità è quella garantire una tutela più completa possibile per i sistemi informatici, ponendo dei vincoli di sicurezza ed affidabilità anche ad ogni strumentazione o componente *ICT* che il soggetto abbia intenzione di inserire all'interno dei propri sistemi. Con tale previsione, sancita dal d.P.R. 54/2021[32] e da due ulteriori d.P.C.M.[33], si impone al soggetto parte del "Perimetro" di notificare al Centro di Valutazione e Certificazione Nazionale (CVCN) la volontà dell'acquisizione di nuova componentistica, la quale sarà sottoposta a test specifici sulla sicurezza e sull'affidabilità della stessa, svolti dai Laboratori Applicativi di Prova (LAP) accreditati presso il CVCN. Tale componentistica, pertanto, sarà soggetta alla condizionalità del superamento dei test, senza i quali non potrebbe essere inserita nei sistemi informatici parte del "Perimetro". Se da un lato questa misura è di fondamentale importanza per il mantenimento della sicurezza anche durante gli aggiornamenti delle reti informatiche, dall'altro lato cagiona rallentamenti nella fase acquisitiva – per i test sono previsti infatti quarantacinque giorni di tempo, prorogabili fino a sessanta giorni nei casi eccezionali – e genera ulteriori oneri

[30] S. Mele, *Convegno:* "*Le nuove reti per l'industria italiana e per i consumatori*", 8 aprile 2021, in cybersecitalia.it; M. Santarelli, *Perimetro cibernetico, un'ora per denunciare un incidente: modalità e impatti per le aziende*, in *cybersecurity360.it,* 4 febbraio 2021.

[31] F. Cerciello, *Nuovi obblighi di notifica degli incidenti: quali conseguenze per i soggetti inclusi nel PSNC,* in *cybersecurity360.it*, 29 settembre 2022.

[32] D.P.R. 54/2021, recante "Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133" (G.U. 97 del 23 aprile 2021).

[33] D.P.C.M. 81/2021, recante "Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133" (G.U. 198 del 19 agosto 2021); d.P.C.M. 92/2022, recante "Regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa, ai sensi dell'articolo 1, comma 7, lettera b), del decreto-legge 21 Settembre 2019, n.105, convertito, con modificazioni, dalla legge 18 Novembre 2019, n. 133*"* (G.U. 164 del 15 luglio 2022).

finanziari, incrementando la pressione economica per i soggetti parte del "Perimetro". Sul tema, infatti, la quasi totalità della dottrina si esprime in termini critici circa l'assenza della defiscalizzazione degli investimenti in tema di *cybersecurity*[34] che avrebbe incentivato una crescita tecnologica sostenibile ed ambienti cibernetici maggiormente sicuri.

Risulta interessante notare come ci sia una continuità nelle previsioni nazionali ed unionali, in quanto entrambe perseguono lo stesso obiettivo di un ambiente cibernetico, e quindi di un mercato digitale, che sia sicuro ed efficiente, e ciò viene ricercato mediante la già citata creazione di una *cybersecurity by design*, che permetta un'attenzione alla sicurezza fin dalle fasi progettuali e non esclusivamente come un mero attributo valutato *ex post,* generando maggiore sicurezza e maggior valore intrinseco dei beni in tal modo progettati.

A *latere* di quest'ottica composita e multiforme creata con il "Perimetro", si pone la nascita dell'Agenzia per la Cybersicurezza Nazionale (ACN) con la l. 109/2021. Trattasi di un evento fondamentale per l'incremento della sicurezza cibernetica nazionale; l'Agenzia ha visto la luce a seguito della pressante necessità della creazione di un'*authority* di elevatissima competenza in ambito di sicurezza cibernetica [35]. Precisamente l'Agenzia ha assorbito le competenze che precedentemente erano ripartite tra un elevato numero di soggetti non adeguatamente competenti sul tema, situazione che aveva portato all'inefficacia ed alla disorganicità del sistema; tuttavia sarebbe sbagliato pensare che l'Agenzia racchiuda al suo interno qualsivoglia competenza in ambito di sicurezza cibernetica, in quanto la stessa svolge un ruolo centrale solo per quanto riguarda la sfera dell'incremento e del mantenimento della resilienza dei sistemi informatici nonché il recupero degli stessi in caso di incidente (questo specifico ruolo è svolto dallo CSIRT nazionale in seno all'Agenzia a seguito della trasmigrazione dal DIS)[36].

Tra le competenze che non sono incardinate presso l'Agenzia, per garantire una maggior efficienza del sistema, si annovera l'aspetto repressivo, demandato principalmente alla Polizia di Stato nella sua specialità della Polizia Postale e delle Comunicazione e del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.) soggetto preposto agli interventi nel caso di incidenti rientranti nel "Perimetro", l'attività di *threat intelligence*, demandata alle Agenzie di Intelligence (Agenzia informazioni e sicurezza interna (AISI) ed Agenzia informazioni e sicurezza interna (AISI)) e l'attività di difesa cibernetica militare, demandata al dicastero della

[34] F. Fabbri, *Consiglio Ue su attacchi informatici. Intervista a Stefano Mele*, in *cybersecitalia.it,* 26 febbraio 2021; A. Tofalo, *CyberSec2022. Tofalo (Comm. Difesa): "La sicurezza deve essere un investimento, bisogna defiscalizzare i costi per la cyber"*, ivi, 7 marzo 2022.

[35] Si pensi che si è iniziato a disquisire della necessità di una Agenzia *ad hoc* da diverso tempo; il Comitato parlamentare per la sicurezza della Repubblica (COPASIR), per esempio, ne aveva indicato la necessità nel 2019 e successivamente l'ex sottosegretario di Stato alla Presidenza del Consiglio, autorità delegata per l'informazione e la sicurezza nonché ex capo della Polizia di Stato, Franco Gabrielli, ha espresso la necessità di creare una struttura *ad hoc* per sottrarre al DIS competenze che non gli appartenevano. Si veda, COPASIR, A. Urso, *Relazione sull'attività svolta dal 1° gennaio 2021 al 9 febbraio 2022*, in *parlamento.it;* F. Gabrielli, *Sicurezza. Audizione di Franco Gabrielli alla Camera: creazione di un'Agenzia per la Cybersecurity | Ministero dell'Interno*, in *interno.gov.it*, 30 giugno 2021.

[36] Si veda l'intervento di N. Ciardi presso il Convegno, *Nuove minacce criminali*, Roma, in *cybersecitalia.it,* 3 febbraio 2022.

Difesa e ad un organismo *ad hoc* di recente formazione quale il Comando per le Operazioni in Rete (COR).

Da un punto di vista operativo, l'Agenzia funge da vero e proprio punto di riferimento per i soggetti e le autorità facenti parte ed operanti nel "Perimetro"; grazie alla recente emanazione della strategia di cybersicurezza[37], ha fornito indicazioni sugli obiettivi e sulle modalità di raggiungimento degli stessi in tema di sicurezza e resilienza dei sistemi, e fornisce inoltre – mediante una comunicazione diretta con gli operatori e tramite il suo sito istituzionale e quello dello CSIRT[38] – *best practices*, *alert*, indici di compromissione ed ogni qualsivoglia comunicazione importante per la protezione o per il recupero dei sistemi informatici. In quest'ottica si nota l'importanza dell'obbligo di notifica previsto dalla normativa istitutiva del "Perimetro", in quanto essa garantisce una miglior continuità negli aggiornamenti per affrontare le ultime minacce tecnologiche palesatesi. L'Agenzia risulta fondamentale anche nel ruolo di implementazione del partenariato tra il settore privato ed il settore pubblico, aspetto deducibile dall'osservazione della strategia dalla quale emergono i tre pilastri fondamentali alla base dell'Agenzia: non solo la protezione e la risposta, aspetti precedentemente trattati, ma anche lo sviluppo. Quest'ultimo elemento risulta dirimente, in quanto, in un settore altamente tecnologico come quello della sicurezza cibernetica, sviluppare tecnologie all'avanguardia per rimanere al passo con le minacce risulta essenziale e l'unica modalità per garantire ciò è permettere l'inserimento dell'investimento e delle capacità di ricerca del settore privato[39]. A conferma di ciò, si pensi che l'Agenzia è stata indicata come punto di contatto unico con il Centro per le Competenze Europeo con sede a Bucarest, per garantire uno sviluppo che non sia condizionato dai confini territoriali, per agevolare lo sviluppo europeo di tecnologie avanzate ed implementare il percorso – lungo ed accidentato – che l'Unione europea sta conducendo per il raggiungimento della sovranità tecnologica unionale.

Analizzando la situazione configuratasi, è sempre più evidente la necessaria implementazione di misure e normative che trascendano i confini territoriali nazionali, per procedere – come si stanno adoperando l'Unione europea e i suoi Stati membri – alla creazione di infrastrutture interconnesse tra loro. Ciò è dimostrato anche dalla necessità – sentita fortemente anche dai privati – di aggiornare l'ormai superata Direttiva NIS, con una sua versione che rispecchi effettivamente le necessità degli operatori, cioè di includere un numero più elevato e dettagliato di settori che ad oggi non rientrano in questa *community* di protezione sovranazionale, e di rendere la misura maggiormente armonizzata limitando

[37] Strategia nazionale di cybersicurezza 2022-2026, in acn.gov.it; Palazzo Chigi, *Cybersicurezza, Gabrielli e Baldoni presentano la Strategia nazionale,* cit.

[38] Si vedano acn.gov.it e csirt.gov.it.

[39] L'essenzialità del coinvolgimento dei privati e dei loro investimenti nel settore tecnologico è fortemente richiamata anche dall'ex direttore dell'ACN Roberto Baldoni. Si veda Palazzo Chigi, *Cybersicurezza, Gabrielli e Baldoni presentano la Strategia nazionale,* cit.

Da sottolineare come sia presente uno strumento che mira a favorire questo coinvolgimento tra il settore pubblico e quello privato: in seno all'Agenzia è infatti stato creato uno speciale comitato tecnico scientifico composto da membri della comunità della *cybersecurity* afferenti sia al mondo industriale che al mondo accademico. Per un *focus* sul tema si veda, L. Franchina, *Agenzia cyber, nominato il Comitato tecnico scientifico: quale ruolo nello sviluppo della Strategia cyber nazionale*, in *cybersecurity360.it*, 16 giugno 2022.

la discrezionalità degli Stati membri nella identificazione dei settori e dei soggetti e nella comminazione di sanzioni, onde evitare la creazione di "sacche" di criminalità informatiche che possano approfittare dei disallineamenti all'interno dei differenti Stati membri.
Il percorso intrapreso dalle istituzioni unionali, forte degli *assessments* sul tema della cybersicurezza, sta fortunatamente procedendo spedito; infatti, sul finire dello scorso anno, è stata pubblicata nella Gazzetta Ufficiale dell'Unione europea l'aggiornamento della Direttiva NIS (la cui versione originale è stata contestualmente abrogata)[40] che gli Stati membri sono tenuti a recepire entro un termine di ventuno mesi. Le caratteristiche salienti di questo aggiornamento introducono i correttivi a lungo richiesti dai privati, quali: il considerevole ampliamento dei settori interessati agli obblighi previsti dalla suddetta direttiva, finalizzato a garantir loro un'elevata sicurezza cibernetica (con un'attenzione particolare per la tutela della *supply chain* mediante l'innalzamento delle misure di sicurezza cibernetica anche per le piccole società non facenti parte del "Perimetro"); una minor discrezionalità in capo agli Stati membri per quanto concerne l'identificazione di tali soggetti, grazie all'introduzione di un criterio dimensionale maggiormente organico volto ad armonizzare il novero dei soggetti rientranti nel "Perimetro" e grazie alla rideterminazione dei medesimi attori che vengono ora suddivisi in soggetti essenziali e soggetti importanti; l'introduzione di un termine di ventiquattro ore entro cui provvedere all'inoltro di un preallarme dell'attacco informatico e di un termine di settantadue ore per provvedere alla notifica dettagliata dell'incidente allo CSIRT competente (la direttiva risulta dettagliata sul tema, in quanto enuncia le caratteristiche degli incidenti significativi che sono oggetto dell'obbligo della notifica)[41].
Le novità apportate dall'aggiornamento della direttiva NIS sono puntuali e risultano, al momento, dei correttivi validi, quanto meno sulla carta; bisogna ora attendere gli ulteriori sviluppi osservando il recepimento della direttiva da parte degli Stati membri e i successivi atti unionali volti a fornire maggior dettaglio circa le misure tecnico-operative ed organizzative che saranno imposte ai soggetti parte del "Perimetro" al fine di elevarne la sicurezza cibernetica.
Risulta infine interessante notare come, all'interno delle proposte accolte nell'aggiornamento della Direttiva NIS, si rintraccino molti elementi analoghi o comuni con quelli del Perimetro di Sicurezza Nazionale Cibernetica, ed il fatto che queste proposte siano l'esito di interazioni tra le istituzioni unionali e le società private, dimostra come almeno sulla carta la struttura del "Perimetro" – al netto delle sue criticità che solo con il tempo ed un adeguato rodaggio potranno essere mano a mano depurate – sia una struttura vincente, destinata a portarci verso una maggiore sicurezza cibernetica ed al raggiungimento degli obiettivi rimarcati a più riprese dall'Unione europea: la creazione di un mercato digitale europeo sicuro ed efficiente, ed il raggiungimento della sovranità tecnologica europea.

[40] Direttiva (UE) 2022/2555, cit.

[41] Per una disamina approfondita sulle novità apportate dalla cd. Direttiva NIS 2, si vedano: *Direttiva NIS 2: ecco come prepararsi a recepire i nuovi obiettivi di cyber security*, in *cybersecurity360.it*, 9 gennaio 2023; P. Licata, *Infrastrutture critiche e digitali, in vigore le direttive Nis 2 e Cer (corrierecomunicazioni.it)*, in *corrierecomunicazioni.it,* 16 gennaio 2023; D. Singh Dhoor, *Cibersicurezza, la Direttiva NIS 2 (altalex.com)*, in *altalex.com,* 24 gennaio 2023; G. Zappaterra, *Direttiva NIS2 approvata: i nuovi obblighi di cyber sicurezza per le aziende*, in *agendadigitale.eu,* 15 novembre 2022.