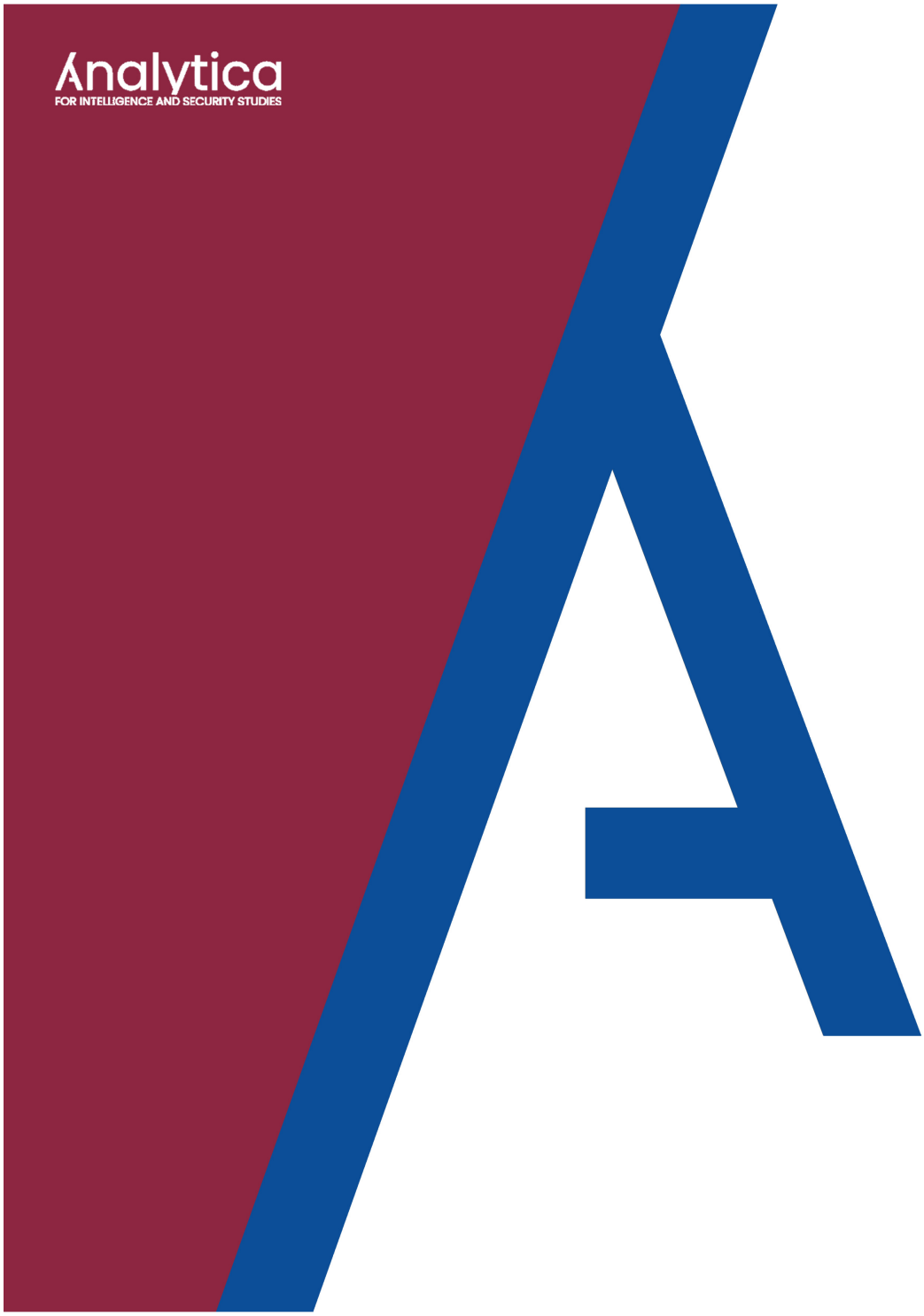

La revisione della Direttiva NIS ed il Perimetro di Sicurezza Nazionale.

Francesca Caravita

Analytica for intelligence and security studies

Paper Cyber security

La revisione della Direttiva NIS ed il Perimetro di Sicurezza Nazionale.

Francesca Caravita

Correzioni e revisioni a cura del Dottor PANEBIANCO Andrea

Torino, dicembre 2020

La situazione sanitaria attuale ha confermato l'importanza della tutela dei sistemi informatici ed informativi, rendendo la data e IT protection un elemento chiave per la sicurezza di qualsiasi organizzazione a prescindere dal settore di riferimento. Di conseguenza, mai quanto oggi le normative e le regolamentazioni esistenti in materia di sicurezza delle reti e dei sistemi diventano un punto di riferimento per tutte le imprese che intendono aumentare il loro livello di sicurezza e la consapevolezza riguardante le minacce e i rischi informatici. Casualità o meno il 2020, oltre ad essere l'anno della pandemia, è anche quello della revisione da parte della Commissione Europea della Direttiva NIS (Network and Information Technology), ovvero una messa in discussione dell'efficienza delle misure adottate e quello dell'avvio della prima fase di attuazione del Perimetro di Sicurezza Nazionale Cibernetica, un piano per la protezione delle reti e dei sistemi informatici nazionali.

Lo scopo di questo elaborato è quello di analizzare questi due eventi, che oltre ad essere estremamente attuali, tenendo conto dell'incremento della minaccia cyber dovuto alla riorganizzazione della nostra società a causa della pandemia, sono estremamente collegati ed interconnessi per quanto riguarda gli obiettivi e le modalità. Il primo capitolo analizza la Direttiva Europea NIS in ottica critica, cercando di valutarne i punti di forza e le criticità tenendo conto della Consultazione pubblica conclusasi ad ottobre; il secondo capitolo esplora invece il percorso italiano in materia di cyber security, evolutosi dall'attuazione della NIS fino alla definizione del Perimetro di Sicurezza Nazionale Cibernetica. Infine, la conclusione ha come obiettivo quello di capire la direzione verso la quale si stanno dirigendo entrambe le misure in modo da individuare i next steps.

2. La Direttiva NIS: un punto di partenza in evoluzione

La Direttiva Network and Information Security è uno dei primi tasselli del grande puzzle del progetto di Cyber Security europea; con l'adozione e la successiva entrata in vigore della Direttiva nel 2016, infatti, l'Unione Europea ha fornito un piano di misure e regolamentazioni comuni in materia di protezione delle reti e dei sistemi informativi, il cui scopo è quello di uniformare il livello di sicurezza cibernetica fra gli stati membri.

L'urgenza di identificare un framework di sicurezza digitale comune era dovuta a due fatti principali. Prima di tutto, l'evidente disomogeneità fra gli stati membri, infatti come per altri ambiti, anche in quello della cyber security non si era mai sviluppata una naturale linea comune fra gli stati, ma, al contrario, si notava chiaramente una notevole differenza a livello di sviluppo tecnologico ai fini della protezione informatica ed informativa e una disparità di metodologie ed approcci alla questione cyber. Questo disallineamento rendeva l'intera Unione un sistema vulnerabile sia da attacchi interni, che esterni. Secondo fattore, l'incremento esponenziale della minaccia cibernetica ai danni delle aziende private e pubbliche. Si pensi che solo in Italia, secondo il rapporto dell'Associazione Italiana per la Sicurezza Informatica CLUSIT, nel 2016 si assisteva ad un aumento del 30 % degli attacchi informatici rispetto all'anno precedente.[1]

In considerazione di questi fatti, vi era la necessità di definire un approccio comune alla materia che potesse ergersi come base solida per l'implementazione delle diverse diramazioni nazionali in base alle necessità particolari. La Direttiva ha, da un lato, predisposto l'obbligo giuridico secondo il quale tutti gli stati membri dovevano definire una strategia circa la sicurezza della rete e dei sistemi informativi, fornendo, allo stesso tempo, un sistema di cooperazione e scambio di informazioni comunitario necessario a sostenere gli stati nell'individuazione delle strategie nazionali. Come, ad esempio, il Gruppo di Cooperazione e il network CSIRT, ovvero un fora di incontro e condivisione dei computer security response incident team nazionali. Dall'altro, ha definito dei requisiti di sicurezza ben precisi da implementare obbligatoriamente per tutte quelle organizzazioni nazionali identificate come Operatori di Servizi Essenziali (OSE) e Fornitori di Soggetti Digitali (FSD), in modo da diffondere la cultura della sicurezza informatica fra quei settori chiave per lo sviluppo dell'economia e della società.

Si tratta di quelle aziende la cui business continuity risulta necessaria per lo svolgimento di attività primarie per la collettività, fra queste, vi rientrano infatti il settore energetico, bancario e finanziario, sanitario, dei trasporti, la distribuzione dell'acqua e quello delle infrastrutture digitali.

[1] https://www.key4biz.it/rapporto-clusit-2016-cyber-attacchi-in-aumento-del-30-nel-2015/151531/

L' eventuale interruzione dei servizi forniti da parte di questi soggetti, a causa di un incidente o attacco informatico, comporterebbero non solo disservizi gravi alla popolazione, ma anche una perdita di denaro ingente. L'impatto non sarebbe solo nazionale, ma avrebbe delle ripercussioni a livello europeo, motivo per il quale l'Unione ha legiferato in merito in modo da definire uno starting point comune.

Questa dunque una panoramica circa le intenzioni e il contenuto della Direttiva, che, ai sensi dell'Articolo 23 della stessa, è soggetta a una revisione periodica. Come detto in precedenza, è proprio questo l'anno in cui la Commissione Europea deve esaminare l'andamento della Direttiva e l'efficacia della sua applicabilità a livello nazionale ed esprimere un parere al Parlamento e al Consiglio Europeo proponendo le eventuali modifiche da adottare. In realtà la Commissione ha deciso di anticipare la scadenza della review, che originariamente era prevista a maggio 2021, per due ragioni. La prima è che la revisione della Direttiva rientra come obiettivo primario all'interno del progetto europeo "Europe fit for digital age", ovvero la strategia digitale della UE che ha come finalità ultima quella di realizzare la propria sovranità digitale[2].

La seconda motivazione è connessa alla situazione sanitaria che ha cambiato le "regole del gioco" di molti settori, rendendoli sempre più dipendenti dalle strutture e sistemi informatici. Di conseguenza, la minaccia di attacco informatico alle piattaforme diventa un rischio primario per l'Unione Europea. In questo contesto lo "stato di salute" della NIS risulta fondamentale tanto da giustificare l'anticipazione delle attività di verifica e controllo. Questa revisione si basa su una valutazione della funzionalità della NIS, congiunta ad una consultazione pubblica per collezionare pareri da parte di attori rilevanti e una verifica di impatto. Più nel dettaglio, ciò che deve essere analizzato è legato sia allo stato attuale del livello di sicurezza implementato dagli stati membri, sia all'adeguatezza della Direttiva alla luce dei cambiamenti ed evoluzioni tecnologiche.

[2] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_it

Quindi da un lato, è necessario condurre un'attività qualitativa e quantitativa delle misure implementate dagli stati in modo da verificare se la sicurezza nazionale è stata incrementata dall'adozione della NIS; dall'altro, è d'obbligo verificare se la NIS risulta essere coerente e adeguata allo "stato dell'arte", concetto ricorrente nell'aquis europeo che fa riferimento all'evoluzione e allo sviluppo tecnologico. La consultazione pubblica è stata avviata fra giugno ed ottobre 2020 e si tratta di un'iniziativa aperta a stakeholder di settore ed enti istituzionali aventi lo scopo di valutare il funzionamento della direttiva in scala sia nazionale che europea. La consultazione, conclusasi il primo di ottobre, si basava su un questionario valutativo con la possibilità di esprimere commenti e pareri in ottica di miglioramento. Alla luce dei feedback raccolti in questa occasione è stato possibile rilevare i punti di forza della Direttiva, ma allo stesso tempo, le criticità emerse in questi anni di attuazione delle misure di sicurezza.

Sicuramente il punto di forza principale della NIS è stato l'effetto catalizzatore che ha avuto sull'implementazione di strategie e normative legate all'ambito cyber adottate dagli stati membri. Infatti, la Direttiva ha messo in luce la severità e la pericolosità del rischio associato a un attacco informatico, spingendo gli stati ad avviare valutazioni circa il loro livello di preparazione in caso di attacco e i loro meccanismi di reazione e prevenzione. Questo ha portato gli stati ad accelerare la definizione e l'implementazione di manovre di sicurezza. Ma non si è trattato solo di evidenziare il problema del rischio cyber in sé e per sé, ma la NIS ha permesso di diffondere l'idea di "cultura della sicurezza informatica", concetto spesso sottostimato in alcune realtà aziendali e statuali. Questo ha permesso di attribuire una maggiore importanza al sistema di protezione delle reti e dei sistemi a tutti i livelli, in quanto le minacce cyber non riguardano solamente le grandi multinazionali o le aziende statali ma possono colpire facilmente anche le piccole e medie imprese private. Dal rapporto di CISCO[3] del 2019 emerge che, in Italia, il 43 % delle aziende vittime di attacchi informatici sono piccole e medie imprese, per le quali l'allocazione di investimenti nella protezione dei dati e dei sistemi informativi non è mai stata una priorità. Secondariamente, la Direttiva ha cercato di fornire una risposta al problema cibernetico, che fosse comunitaria, con lo scopo ultimo di definire una strategia europea in grado di individuare un livello minimo di sicurezza

[3] https://www.cisco.com/c/dam/global/it_it/solutions/small-business/pdf/security-essentials.pdf

valido per tutti gli stati a prescindere dalle differenze nazionali. Apprezzabile è dunque lo sforzo di armonizzare il benchmark di partenza. Inoltre, da considerare come punto di forza è il tentativo di creare un sistema di networking e cooperazione fra gli stati in modo da fornire supporto tecnico ed organizzativo all'interno del processo di adozione delle misure previste. Esempi di questa intenzione, i già citati network CSIRT e il Gruppo di Cooperazione NIS.

Se la Direttiva è sicuramente un ottimo punto di partenza al fine di realizzare la sovranità digitale europea e il mercato unico digitale, allo stesso tempo, presenta delle criticità emerse nel periodo di applicazione delle misure da parte degli stati membri. Queste problematiche, proprio perché considerate un possibile ostacolo agli obiettivi del progetto digitale europeo, sono oggetto della revisione da parte della Commissione, il cui scopo era proprio quello di evidenziare i punti deboli della Direttiva. Fra questi, si possono sintetizzare tre macro-aree critiche: il disallineamento nel processo di adozione da parte degli stati, il limite delle categorie di settori soggetti alle misure di sicurezza e, infine, le misure di sicurezza non adeguate allo stato dell'arte tecnologico. Prima questione, si tratta di una problematicità che è comune all'interno dell'Unione: la disarmonia fra gli stati membri.

Questo accade in quanto gli stati, nella ricezione della Direttiva, attuano una metodologia e un approccio di adozione diverso fra loro. Il problema sta nell'interpretazione della definizione di "operatori essenziali", dunque da cosa si intende per "servizio essenziale", in quanto la Direttiva fornisce sì delle linee guida, ma molto generali, lasciando un'ampia capacità di manovra di scelta da parte delle istituzioni governative. Questo ha portato ad una disomogeneità nell'interpretazione del panorama regolatorio, che ha avuto delle ripercussioni negative sia sulla protezione del livello di sicurezza delle aziende stesse, sia del loro business. Per esempio, è emerso il rischio che una singola azienda operante in due stati diversi, venga identificata come OSE in uno stato, ma non nell'altro. Questa circostanza, oltre ad essere un controsenso per la Direttiva stessa, arreca delle difficoltà organizzative per le aziende che si trovano ad operare in contesti legislativi diversi seppur tutti regolati dalla stessa Direttiva. Inoltre, si crea anche il rischio che alcune aziende, che necessitano un livello di protezione maggiore, vengano escluse dal panorama NIS proprio a causa di questa disomogeneità interpretativa delle norme definite.

Lo stesso discorso vale anche per i FSD, i cui criteri di identificazione non risultano chiari e troppo generali. Di conseguenza, quello che viene suggerito alla Commissione è di cercare di provvedere ad una definizione più stringente del concetto di OSE e FSD in modo da evitare interpretazioni ed applicazioni divergenti fra gli stati membri. La seconda criticità è direttamente legata a quanto appena descritto e riguarda i settori definiti nell'Annex 2 della NIS che descrive le categorie di OSE. Non solo non vi sono dei criteri ben definiti, ma i settori/sotto settori inclusi non coprono tutte le aree produttive o di servizi vulnerabili che necessiterebbero di una protezione maggiore. Se si analizzano i feedback rilasciati all'interno del sito della Commissione dedicato alla Consultazione Pubblica si possono rilevare analisi interessanti provenienti proprio dagli attori attivi nei settori di riferimento. Per esempio, secondo l'azienda Eurosmart, la NIS non include settori vitali come l'e-Governement e le telecomunicazioni[4]; oppure secondo Enel Italia, all'interno della sezione "Energia" manca il riferimento ai servizi legati a *"generation (distributed or centralised) and public lighting services"*[5]. Ancora, per quanto riguarda invece la categoria degli FSD, l'Organizzazione europea dei consumatori (BEUC) propone di includere anche i social network in quanto vengono identificati come fornitori di servizi digitali sempre più vulnerabili ad attacchi informatici[6]. In questo caso bisogna infatti considerare la quantità di dati personali potenzialmente vulnerabili detenuti da social network come Facebook o Twitter, il cui furto o manomissione potrebbe generare impatti estremamente negativi. La soluzione proposta a questa seconda criticità, quasi all'unisono, è dunque quella di ampliare la lista dei destinatari della NIS tenendo conto delle nuove minacce e dei nuovi scenari in ambito cyber. Infine, le terza problematica è legata all'adeguatezza della NIS allo sviluppo tecnologico. Infatti, in termini di tempo, cinque anni per lo sviluppo informatico sono un'enormità, tanto che lo stato dell'arte connesso alle minacce cyber è sicuramente molto diverso rispetto a quello dell'anno in cui è stata adottata la Direttiva.

[4] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F543293
[5] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F541131
[6] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F539550

Si è assistito a un cambiamento delle tecnologie disponibili da parte degli utenti malevoli e di conseguenza una modifica delle modalità di attacco. Si pensi solo a come si è evoluta la minaccia informatica in questo 2020 a causa della pandemia e della riorganizzazione del mondo del lavoro dovuta alla necessità di lavorare a distanza. Infatti, gli utenti malevoli sono stati in grado di plasmare la tecnologia a loro disposizione in modo da sfruttare le vulnerabilità emerse dallo smart working e questo ha portato ad uno spostamento dell'interesse della superficie di attacco[7] dai sistemi digitali (reti, connessioni etc.) ai sistemi fisici (dispositivi come tablet, pc e cellulare etc.) che risultano essere oggi le maggiori vittime dei cyber attack. In una situazione di questo tipo, dove la tecnologia e la pervasività degli attacchi è in continua crescita ed evoluzione, la Direttiva NIS deve essere in grado di fornire una protezione adeguata al nuovo panorama informatico.

Da un'analisi dei feedback rilasciati nel corso della Consultazione Pubblica emerge proprio questo aspetto, ovvero che la NIS non tiene conto di alcuni ambiti fondamentali nella definizione dei requisiti obbligatori per gli OSE e i FSD. Per esempio, la Eurosmart[8] riporta proprio che la NIS dovrebbe tenere in considerazione alcuni fenomeni appena nati come l'avvento del 5G e prevedere requisiti di security in grado di mettere in sicurezza i dispositivi mobili connessi a questa rete.

Anche Enel suggerisce che al fine di ampliare i settori di applicazione della NIS è necessario considerare lo sviluppo tecnologico, soprattutto in ambito rete 5G e Intelligenza Artificiale. Ugualmente l'azienda cinese Hangzhou Hikvision Digital Technology Co, suggerisce che la Direttiva dovrebbe considerare l'incremento esponenziale dell'impiego dei dispositivi Iot (Internet of things), ovvero smart object perennemente connessi ad internet, in ambito industriale e produttivo.

[7] Fortinet, Global Threat Landscape Report: A Semiannual report by FortiGuard Labs, Agosto 2020, pp. 10-11
[8] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F543293

L'aumento dell'utilizzo di questa tecnologia (il cui numero di dispositivi utilizzati da utenti aumenterà fino alla cifra di 50 milioni di unità entro il 2022[9]), unita all'incremento degli attacchi ai danni di questi (nel 2020 gli IoT costituiscono il 33% dei dispositivi infetti, rispetto al 16% del 2019[10]) fanno sì che la NIS si debba adeguare a questo fenomeno, attraverso l'inclusione di misure di sicurezza ad hoc a tutela degli IoT all'interno dei requisiti di sicurezza in modo da "creare un livello comune di sicurezza per tutti questi dispositivi"[11].

Perimetro di sicurezza nazionale cibernetica: la prima attuazione

Il percorso di difesa e tutela dello spazio digitale italiano è composto da numerosi traguardi legislativi che hanno poco a poco disegnato l'architettura della cybersecurity nazionale rendendola una delle priorità strategiche della sicurezza nazionale. Per meglio comprendere l'assetto cibernetico italiano è necessario focalizzarsi su alcuni passaggi chiave i quali si possono riassumere in quattro momenti: il Decreto Monti nel 2013, il Decreto Gentiloni nel 2017, il Recepimento della NIS nel 2018 ed infine la Legge 133 del 2019 inerente il Perimetro Cibernetico di sicurezza nazionale. Il Decreto Monti è il punto di avvio dal quale si definisce[12], per la prima volta, l'architettura istituzionale nazionale cyber. Il decreto prevedeva la razionalizzazione e il rafforzamento delle capacità cyber del paese al fine di tutelare la sicurezza informatica delle infrastrutture critiche materiali ed immateriali, attraverso la definizione dei meccanismi, delle procedure e degli organi individuati per raggiungere tal fine.[13]

Alla luce delle misure previste dalla NIS in ambito europeo nel 2016, l'anno seguente viene emanato il Decreto Gentiloni[14] che andrà a sostituire quello del 2013. Questo decreto delineava i nuovi assetti organizzativi dell'architettura cibernetica nazionale apportando alcune novità.

[9] https://www.microsoft.com/en-us/download/confirmation.aspx?id=101738
[10] https://pages.nokia.com/T005JU-Threat-Intelligence-Report-2020.html
[11] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F542933
[12] https://www.sicurezzanazionale.gov.it/sisr.nsf/comunicazione/decennale-intelligence/gli-anni-della-cybersecurity.html
[13] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2013/03/dpcm-24-01-2013.pdf
[14] https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-31-marzo-2017.html

La prima riguarda la volontà di affidare al Dipartimento Informazioni per la Sicurezza (DIS) un ruolo centrale all'interno dell'architettura cyber, infatti ottiene la gestione del Nucleo per la Sicurezza Cibernetica (Nsc) un organo di prevenzione e risposta ad eventuali situazioni di crisi che precedentemente ricadeva sotto l'Ufficio del consigliere militare. Inoltre, al Direttore Generale del DIS viene affidato il compito di definire le linee di azione che devono assicurare il livello di sicurezza necessario sia per il settore privato che per quello pubblico. Secondariamente, tenendo conto della NIS, viene rafforzato il ruolo del Comitato Interministeriale per la Sicurezza della Repubblica (CISR) che assume un compito attivo in caso di crisi e, inoltre, viene affiancato da un organo tecnico, il CISR tecnico.

Nel 2018, con il Decreto Legislativo n.65, viene recepita la disciplina della materia in ambito NIS, quindi le normative previste a livello europeo vengono adottate anche per l'Italia. A tal proposito, viene istituito presso la Presidenza del Consiglio dei ministri, più precisamente presso il DIS, il Computer Security Incident Response Team (CSIRT) italiano sostituendo i già esistenti Computer Emergency Response Team (CERT/ CERT PA), le cui attività, disciplinate nel DPCM del 2019 e avviate a partire da maggio 2020, vertono sulla gestione degli incidenti cyber e sul supporto fornito agli attori coinvolti sia privati che pubblici in caso di crisi. Il Decreto definisce, inoltre, le autorità competenti in ambito NIS che devono sia vigilare sull'applicazione delle misure, sia definire i soggetti rientranti nella categoria degli OSE. Infine, viene identificato sempre nel DIS il punto di contatto NIS (PoC), organo adibito alla cooperazione con gli altri stati membri e con le istituzioni europee.

Infine, l'ultimo tassello del disegno cibernetico italiano, che punta ad affermarsi come punto di riferimento d'avanguardia a livello europeo è il Perimetro Nazionale di sicurezza cibernetica, adottato nel 2019 con la Legge 133, il cui regolamento è entrato in vigore il 21 ottobre 2020 con il DPCM del 30 luglio 2020. Si tratta di un pacchetto di normative il cui scopo è quello di prevedere e fornire degli strumenti di difesa agli attori nazionali, privati e pubblici, a tutela della sicurezza delle reti, dei sistemi informativi ed i servizi informatici. La tutela degli interessi informatici delle istituzioni pubbliche e delle aziende italiane destinatarie della normativa ha un duplice significato che è alla base del Perimetro.

Da un lato, tutelare i loro sistemi informatici vuol dire contribuire alla sicurezza nazionale, questo perché i destinatari del Perimetro sono definiti come quelli "esercitanti funzioni essenziali allo stato in quanto assicurano un servizio essenziale al mantenimento di attività civili, sociali ed economiche fondamentali per gli interessi dello stato"[15] la cui un'interruzione a causa di un attacco cyber pregiudicherebbe la sicurezza nazionale. Dall'altro, fornire gli strumenti per la prevenzione e la risoluzione degli attacchi informatici alle aziende le rende più competitive sul mercato commerciale internazionale e di conseguenza arreca beneficio all'economia italiana su larga scala. Infatti, la competitività delle aziende oggi si basa anche sulla loro capacità di mettere in sicurezza i dati degli utenti da minacce esterne.

Il DPCM del 30 luglio ha dato l'avvio a questo progetto definendo prima di tutto i criteri di individuazione degli attori inclusi nel perimetro e secondariamente gli obblighi previsti al fine di tutelare le loro architetture informatiche. Per quanto riguarda il primo aspetto, il Decreto esplica che il perimetro deve essere applicato a tutti i soggetti che esercitano una funzione essenziale per lo stato, le cui attività sono necessarie per lo svolgimento dei lavori delle amministrazioni CISR (Presidenza del Consiglio e Ministeri individuati art.5 Legge 123/2007) e tutti i soggetti privati e pubblici che prestano un servizio essenziale per il mantenimento dell'attività civile, sociale ed economica del paese. Rientrano fra questi a parte il settore governativo, quello dell'interno, della difesa, dello spazio e aerospazio, dell'energia, delle telecomunicazioni, dell'economia e finanza, dei trasporti, dei servizi digitali, delle tecnologie critiche e gli enti previdenziali/lavoro. Interessante è analizzare i criteri di individuazione dei soggetti rientranti nel perimetro.

La normativa, definendo gli elementi che inquadrano l'"essenzialità" di un attore, esprime la volontà del legislatore di attribuire al concetto di sicurezza nazionale un significato più ampio. Infatti, considera come elementi arrecanti un danno alla sicurezza nazionale non solo l'interruzione della continuità operativa del servizio fornito, ma anche la compromissione della disponibilità, integrità e riservatezza dei dati coinvolti nel servizio stesso.

[15] https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg

Vengono, inoltre, considerate come aspetti discriminanti alcune variabili che valutano gli impatti di un eventuale attacco informatico su diverse dimensioni: la portata di un' eventuale interruzione del servizio/compromissione dei dati in termini territoriali e di numero di utenti coinvolti, la gravità degli effetti causati dall'interruzione/compromissione, che dovrà essere misurata in termini di analisi del rischio ed infine, il fattore temporale, ovvero il periodo di tempo necessario a ripristinare il normale svolgimento delle attività impattate. Sulla base di questi criteri, ogni amministrazione CISR deve stilare una lista di soggetti che dovrà essere esaminata dal CISR e dal CISR tecnico. Riguardante, invece, gli obblighi previsti, il Decreto stabilisce che ciascun soggetto scelto debba stilare un elenco di tutti i beni ICT (Information and Communication Technology) di competenza, che saranno poi l'oggetto delle misure di sicurezza in quanto elementi a rischio di attacco informatico. La normativa precisa le modalità di selezione di questi beni; prima di tutto chiarisce il significato di "beni ICT" intendendo un insieme di reti, sistemi informativi e servizi informatici, che vengono impiegati all'interno dello svolgimento di funzioni essenziali per lo stato o per l'erogazione di servizi essenziali. Inoltre, viene reso noto che questi beni devono essere individuati al termine di un'analisi del rischio condotta in modo da verificare l'impatto di un'eventuale interruzione/compromissione dovuto a un attacco cyber sui beni stessi. Infine, è richiesta ai soggetti destinatari la redazione di una descrizione della componentistica e dell'architettura relativa ai beni ICT individuati, secondo un modello redatto dal DIS e dal CISR tecnico. Tutta la documentazione redatta dovrà essere trasmessa al DIS attraverso una piattaforma digitale dedicata. Come ultimo elemento di analisi è necessario citare l'istituzione del cosiddetto "Tavolo Interministeriale", ovvero un organo di supporto al CISR tecnico per l'attuazione del perimetro. Il tavolo, gestito dal DIS e composto da membri della Sicurezza Nazionale, del CISR e dei Ministeri coinvolti, dovrà occuparsi delle questioni tecniche riguardanti le liste dei soggetti individuati e degli aspetti di competenza del CISR o del CISR Tecnico.

Alla luce delle manovre legislative descritte che hanno di fatto delineato l'assetto cibernetico del nostro paese è interessante valutare due aspetti: la presa di coscienza di una nuova realtà, quella cibernetica e la conseguente urgenza di razionalizzazione ed organizzazione del panorama istituzionale al fine di gestire questo nuovo contesto e il ruolo centrale affidato al DIS all'interno di questo progetto.

Per quanto riguarda la prima considerazione, il fatto che gli attori statuali debbano tener conto della realtà virtuale è ormai un'ovvietà che si è concretizzata su diversi livelli. In primis a livello europeo con l'adozione della NIS, del Cybersecurity Act e del GDPR, strumenti che hanno cercato di regolamentare su diversi aspetti, sia dal lato informatico sia dal lato privacy e tutela dei dati, il nuovo panorama digitale dal quale dipendono quasi tutti i settori produttivi e fornitori di servizi. Non si è trattato però solo di organizzare e regolamentare, ma anche di fornire gli strumenti necessari alla tutela dei sistemi informatici ed informativi considerando l'incremento costante delle minacce informatiche ai danni degli impianti digitali. Ugualmente, anche a livello nazionale, l'Italia è stata in grado di rilevare l'urgenza e l'attualità della questione cercando di adeguare, come descritto, il proprio assetto istituzionale di conseguenza, tenendo in considerazione l'impatto notevole che la minaccia cyber comporta a danno degli interessi del nostro paese. Infatti, come riporta la Relazione annuale del DIS al Parlamento *"l'arma cibernetica si è confermata anche nel 2019 strumento privilegiato per la conduzione di manovre ostili in danno di target, sia pubblici che privati, di rilevanza strategica per il nostro paese"*[16]. Per cui, la tutela degli asset sia pubblici che privati risulta di fondamentale importanza, motivo per cui abbiamo assistito negli ultimi anni ad uno sforzo rilevante da parte degli attori istituzionali che ha permesso de velocizzare il processo di implementazione della struttura cyber in linea con le best practices internazionali. La seconda considerazione è legata al ruolo conferito al DIS all'interno dell'assetto cibernetico. Ricordiamo infatti che il DIS risulta essere il centro di coordinamento delle attività all'interno del meccanismo di regolamentazione e di gestione delle questioni legate all'ambito cyber ed è infatti responsabile dello CSIRT, del PoC e del NSC, oltre ad essere coordinatore dell'implementazione del Perimetro Cibernetico.

[16] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2020/03/RELAZIONE-ANNUALE-2019-4.pdf

La centralità del Dipartimento è stata sicuramente rafforzata con la Legge 133/2012 (che andava ad integrare la normativa sul Sistema di informazione per la sicurezza della Repubblica) che prevedeva non solo il rafforzamento delle attività di informazione per la protezione delle infrastrutture critiche in ambito cibernetico e di sicurezza delle informazioni presso le agenzie del compartimento di sicurezza, ma attribuiva anche al DIS il ruolo di coordinamento dell'attività di ricerca informativa finalizzata alla protezione cibernetica ed informatica. Inoltre, la materia cyber necessita sicuramente di una gestione unitaria accentrata nelle mani di un solo attore che dirige tutti i soggetti coinvolti su vari piani e livelli. Infatti, la questione cibernetica si può definire "interdisciplinare" in quanto coinvolge tutti gli ambiti ed i settori e dunque ha un impatto rilevante su piani diversi che solitamente non risultano essere connessi. In più, il mondo cibernetico va di pari passo con l'innovazione tecnologica che cresce ad un livello esponenziale, per cui tutte le misure devono essere sempre aggiornate e adeguate allo stato dell'arte tecnologico. Per queste ragioni, è fondamentale che sia definito un solo soggetto in grado di tenere sotto controllo questi aspetti diventando il punto di riferimento dell'architettura cibernetica nazionale.

Conclusione

Nel corso di questo elaborato sono stati analizzati gli sviluppi della normativa in ambito cyber a livello europeo e a livello nazionale, ma quali sono i next steps della NIS e del Perimetro Cibernetico?

Per quanto riguarda la NIS si attende la Decisione finale della Commissione Europea relativa alle attività di valutazione e controllo condotte in questi mesi. Come punto di partenza per capire quale potrebbe essere l'indirizzo preso dalla Commissione si può considerare la Roadmap[17] fornita dalla Commissione stessa in occasione della Consultazione Pubblica avente lo scopo di informare i cittadini e gli stakeholder sui lavori in corso, in particolare sulle possibili modalità di intervento. Vengono descritti quattro possibili scenari di policy da implementare ai fini della revisione della NIS. La prima opzione prevede il mantenimento della situazione attuale aspettando la naturale evoluzione delle misure implementate fino ad ora a livello statale.

[17] file:///C:/Users/XP465HU/Downloads/090166e5d0c95543%20(1).pdf

La seconda propone invece di definire delle misure non legislative volte a chiarire gli aspetti critici della NIS, come per esempio la definizione e i criteri di identificazione degli OSE che hanno creato un disallineamento fra gli stati membri con lo scopo di eliminare la frammentazione nell'implementazione delle misure. La terza proposta consiste nella modifica della Direttiva esistente con lo scopo di aumentare l'armonizzazione delle misure. Si tratta dunque di un processo di emendazione e di aggiunta di definizioni e principi soprattutto, anche in questo caso, inerenti l'identificazione degli OSE e l'ampliamento della lista di settori che necessitano una protezione aggiuntiva. Infine, la quarta opzione propone la definizione e l'adozione di un nuovo atto legislativo che abrogherebbe la NIS fornendo normative più dettagliate ed esaustive al fine di limitare la frammentazione interna e ampliare i settori e servizi coinvolti.

In conclusione, ciò che emerge da queste policy è la volontà di portare chiarezza fra le norme e di dettagliare i criteri di individuazione dei soggetti OSE e FSD, oltre che di ampliare di settori di applicazione; ciò che invece ancora non è chiaro e, di difficile previsione, è la modalità con cui avverrà la revisione della Direttiva. Stando ai feedback rilasciati dagli stakeholder, la Commissione dovrebbe optare per l'opzione 3 o 4 in quanto considerate quelle più efficaci e adatte al panorama attuale.

Riguardante invece il Perimetro, l'appena approvato DPCM è il primo di una serie di provvedimenti legislativi che nel tempo, in modo graduale, andranno a definire nel dettaglio l'operatività del Perimetro Cibernetico. Allo stato attuale, si sta aspettando la pubblicazione della lista, per ora segreta, dei soggetti coinvolti nel programma e la successiva comunicazione da parte del DIS alle aziende ed amministrazioni destinatarie. A quel punto saranno queste a dover condividere la documentazione prevista dal DPCM. Il quadro normativo, seppur chiaro, risulta essere sicuramente complesso nelle sue fasi più operative, ovvero quelle di implementazione degli obblighi previsti.

§

Bisognerà vedere dunque quale sarà la reazione delle aziende e soprattutto quale la loro capacità operativa nell'adempiere alla stesura della lista dei beni ICT e della loro componentistica, sia a livello di tempistiche che a livello di esaustività del materiale fornito. In particolare, la preoccupazione maggiore verte sulle piccole e medie imprese, che si ricorda, possono rientrare fra i soggetti destinatari se identificate come di interesse nazionale, le cui risorse sia a livello di personale, che a livello di budget, sono limitate.

Di conseguenza, queste realtà potrebbero risultare le più penalizzate dal Perimetro, ostacolandone la produttività e la competitività sul mercato.