Amministrazioni al mondo dell'industria, dalla cittadinanza agli studenti. A quest'ultimo riguardo, il DIS ha patrocinato la "CyberChallenge.IT", organizzata dal Laboratorio Nazionale di Cybersecurity del Consorzio Interuniversitario Nazionale per l'Informatica, finalizzata alla creazione della prossima generazione di professionisti dalla sicurezza informatica, composta da giovani talenti da formare e, successivamente, impiegare nelle realtà strategiche del Paese.

L'edizione 2020 ha registrato la partecipazione di oltre 4mila studenti suddivisi su 28 sedi (di cui 26 università) e ha visto la vittoria della squadra dell'Università di Udine.

Il DIS, inoltre, in ragione del diffuso impiego di modalità lavorative "agili", accresciuto dall'emergenza Covid-19, ha predisposto un "Vademecum delle policy di sicurezza per le organizzazioni", volto a sensibilizzare gli OSE in primis, ma anche per la più ampia diffusione a livello nazionale, contenente alcuni accorgimenti necessari alla riduzione del livello di esposizione al rischio cyber associato al telelavoro.

Nel medesimo contesto, si è proceduto, in fattivo raccordo con il Ministro per l'Innovazione tecnologica e la Digitalizzazione - Dipartimento per la Trasformazione Digitale, ad assicurare l'osservanza dei principi di cybersecurity, nonché la formazione del personale e la promozione della consapevolezza, nell'ambito della norma di impulso alla digitalizzazione della Pubblica Amministrazione (D.L. n. 76/2020, cd. Decreto "semplificazioni", convertito, con modificazioni, dalla legge n. 120/2020).

TRASFORMAZIONE DIGITALE E SICUREZZA CIBERNETICA

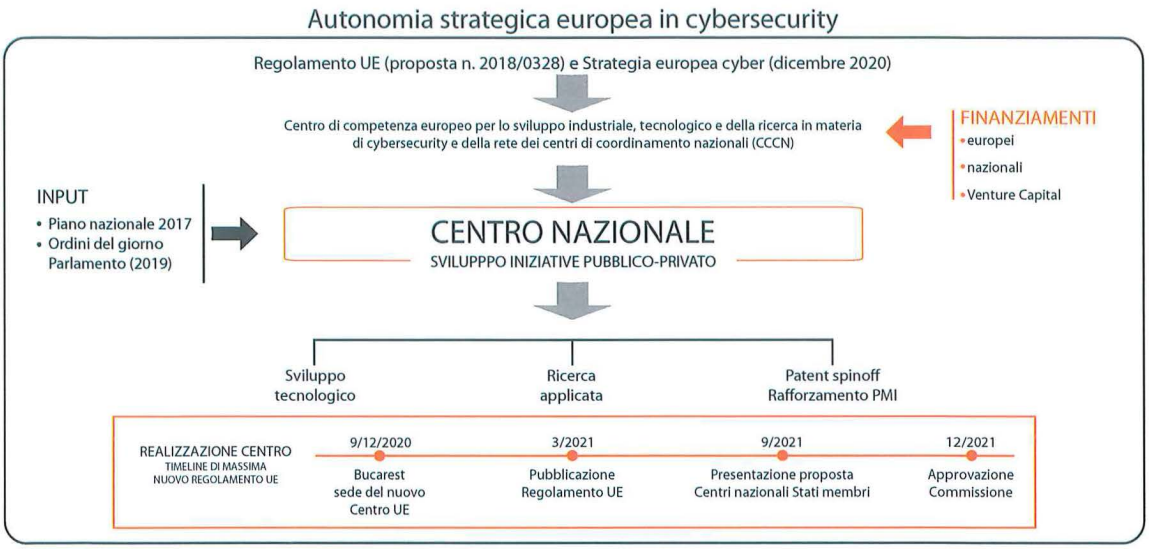
Dopo l'accelerazione del processo di trasformazione digitale imposto dalla pandemia Covid-19 che ha portato ad un sensibile aumento degli attacchi cibernetici, il programma di finanziamento "Next Generation EU" getta i presupposti per un'ulteriore fase di allargamento e velocizzazione di tale processo creando quindi contestualmente la necessità di aumentare la resilienza del Paese e dell'Europa rispetto agli attacchi. Il DIS ha mantenuto stretta sinergia con il Ministro per l'Innovazione tecnologica e la Digitalizzazione - Dipartimento per la Trasformazione Digitale, così da assicurare il rafforzamento degli investimenti in sicurezza cibernetica nel contesto delle attività di innovazione digitale della Pubblica Amministrazione e del settore produttivo, in coerenza con le normative nazionali in materia e con la "Strategia dell'UE per la cybersecurity nel decennio digitale". Tale Strategia invita gli Stati Membri ad allocare adeguate risorse del programma "Next Generation EU" per accrescere la resilienza delle infrastrutture e dei servizi critici, nonché la sovranità tecnologica e la leadership dell'Unione e dei suoi Stati Membri. Il perseguimento di tale scopo passa anche attraverso:

- la creazione di un "European Cyber Shield", ossia di una rete integrata di CSIRT nazionali, Security Operations Center (SOC) nazionali, Information Sharing and Analysis Centers (ISACs) settoriali, con le Autorità nazionali di cybersecurity;
- il supporto alla supply-chain industriale per garantire la sovranità tecnologica europea, avvalendosi di fondi, competenze, capacità tecnologiche e industriali. In tal senso, la Strategia assegna un ruolo chiave al Centro di competenza europeo per lo sviluppo industriale, tecnologico e della ricerca in materia di cybersecurity e alla rete dei Centri di coordinamento nazionali;
- la creazione di un mercato del lavoro europeo attrattivo per i giovani talenti nel settore della sicurezza cibernetica e la promozione di mirati programmi di formazione di personale specializzato.

Le menzionate azioni sono già state al centro di diverse iniziative avviate dal Comparto Intelligence nel corso del 2020, e che proseguiranno nel 2021, per elevare i livelli di sicurezza cibernetica del Paese e le capacità di prevenzione e risposta agli eventi cibernetici, rafforzando, in particolare, lo scambio di informazioni e l'analisi degli elementi tecnici grazie agli strumenti normativi messi in campo dalla normativa sul Perimetro di sicurezza nazionale cibernetica, nonché lo sviluppo di modelli matematici funzionali alla modellazione delle interdipendenze tra le infrastrutture ICT dei soggetti pubblici e privati più rilevanti per la sicurezza nazionale, così da poter meglio definire, in ottica previsionale, l'impatto degli incidenti cibernetici significativi.

REGOLAMENTO UE PER LA CREAZIONE DI UN CENTRO DI COMPETENZA EUROPEO PER LO SVILUPPO INDUSTRIALE, TECNOLOGICO E DELLA RICERCA IN MATERIA DI CYBERSECURITY E DELLA RETE DEI CENTRI DI COORDINAMENTO NAZIONALI

Entro sei mesi dall'entrata in vigore del Regolamento, ogni Stato Membro è chiamato a costituire un proprio Centro di coordinamento nazionale da individuare in un ente pubblico, o a maggioranza pubblica, e che abbia la capacità di: supportare e relazionarsi con il citato Centro UE e la connessa rete dei diversi Centri nazionali di coordinamento; gestire fondi; possedere o avere accesso diretto a capacità tecniche e di ricerca in materia di cybersecurity; coinvolgere e coordinarsi con i settori pubblico (incluse le Autorità NIS) e privato, con l'accademia, il mondo della ricerca e la società civile. Il Centro nazionale, creato per potenziare la capacità domestica industriale, di competenze e di ricerca in cybersecurity, per poter accedere ai fondi europei, dovrà essere accreditato al Centro UE dallo Stato Membro e, in questo senso, la Commissione avrà tre mesi di tempo per esprimersi. Il Centro UE e il Centro nazionale dovrebbero essere operativi a partire dalla fine del 2021. L'importanza di tale Centro è di tutta evidenza solo considerando la circostanza che, durante i lavori parlamentari relativi al citato "Perimetro di sicurezza nazionale cibernetica", il Parlamento stesso ha ritenuto di impegnare il Governo con tre ordini del giorno alla creazione di un Centro nazionale di ricerca e sviluppo in cybersecurity, anche in relazione alle nuove tecnologie.

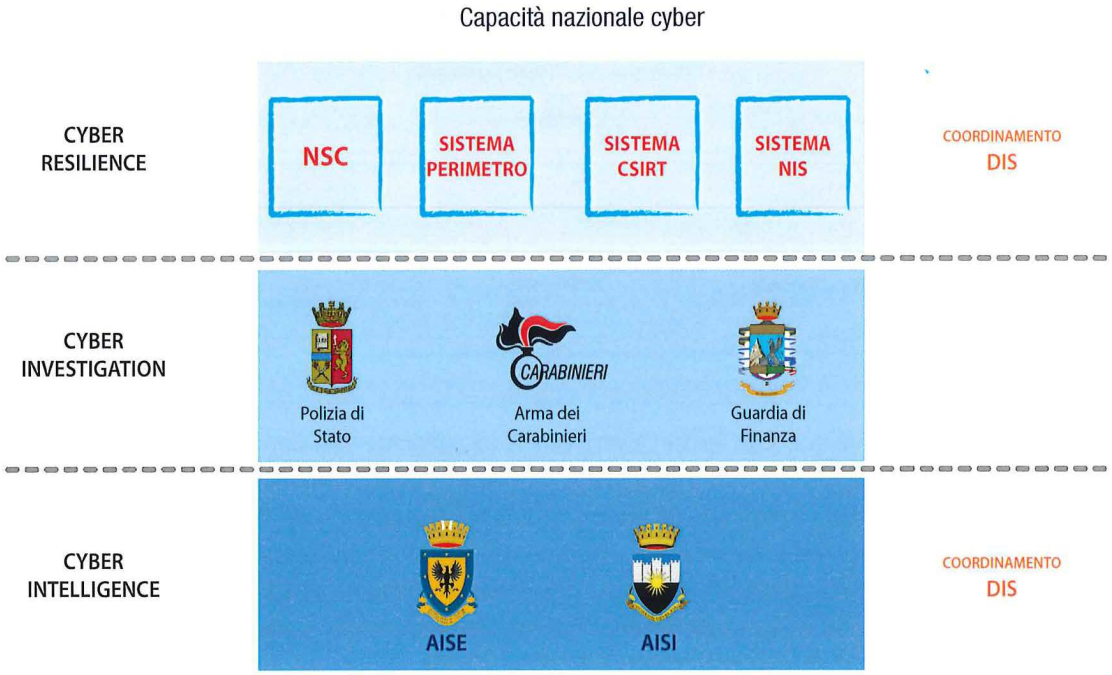


Sempre in questo contesto, inoltre, considerato che l'Italia sarà, in pochi mesi, chiamata a creare il proprio Centro di coordinamento nazionale, destinato ad operare in stretto raccordo con il sopra richiamato Centro europeo, il DIS ha condotto un approfondimento in merito all'organizzazione e alle funzioni che la nuova struttura sarà chiamata a svolgere, evidenziando l'esigenza che questo Ente assuma anche le funzioni di centro nazionale di ricerca e sviluppo in cybersecurity, in linea con quanto previsto dal Piano Nazionale per la protezione cibernetica e la sicurezza informatica (marzo 2017) e alla cui istituzione il Parlamento, come già accennato, ha impegnato il Governo, con tre ordini del giorno, in sede di conversione in legge del D.L. n. 105/2019 sul Perimetro di sicurezza nazionale cibernetica.

Il Centro avrebbe quindi l'obiettivo, da un lato, di favorire lo sviluppo e il potenziamento di una industria italiana ed europea competitiva, in grado di fornire tecnologie e servizi abilitanti ad elevato grado di sicurezza, con particolare riguardo all'ambito delle infrastrutture critiche digitali, alle principali filiere industriali nazionali e, dall'altro, di operare – in termini di supporto, studio e sviluppo – in stretta sinergia con i diversi soggetti che compongono l'architettura nazionale di sicurezza cibernetica.

La menzionata nuova struttura, inoltre, costituirebbe la naturale interfaccia dei Centri di competenza previsti dal Piano nazionale Impresa 4.0 – che fa seguito all'iniziativa della Commissione europea "Digitising European Industry" dell'aprile 2016, volta a promuovere la trasformazione digitale delle imprese, rafforzando i collegamenti tra ricerca e industria – oltre che dei Digital Innovation Hub, distribuiti sul territorio a supporto delle piccole e medie imprese e delle Pubbliche Amministrazioni locali per il relativo incremento delle capacità di prevenzione e di valutazione del livello di maturità digitale e tecnologica, nonché per l'accrescimento della consapevolezza.

In tal modo, si ritiene che possa essere definita l'architettura nazionale cyber per la parte connessa alla sicurezza nazionale, allo stato della vigente legislazione.



LISTA ACRONIMI

AgID – Agenzia per l'Italia Digitale
ANSSI – Agenzia nazionale francese per la sicurezza dei sistemi informatici
Blue OLEx – Blueprint Operational Exercise
CISR – Comitato Interministeriale per la Sicurezza della Repubblica
CMX – Crisis Management Exercise
CNAIPIC – Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
COR – Comando per le Operazioni in Rete
CERT – Computer Emergency Response Team
CSIRT – Computer Security Incident Response Team
CV – Centro di Valutazione
CVCN – Centro di Valutazione e Certificazione Nazionale
CyCLONe – Cyber Crisis Liaison Organisation Network
DDoS – Distributed Denial of Service
DORA – Digital Operational Resilience Act
DPCM – Decreto del Presidente del Consiglio dei Ministri
DSN – Documento di Sicurezza Nazionale
ENISA – Agenzia dell'Unione Europea per la cybersecurity
FIRST – Forum of Incident Response and Security Teams
FSD – Fornitori di Servizi Digitali
ICE – Infrastrutture Critiche Europee
ICT – Information and Communication Technology
IPCR – Integrated Political Crisis Response Arrangements
ISAC – Information Sharing and Analysis Center
ITU – International Telecommunication Union
MAECI – Ministero degli Affari Esteri e della Cooperazione Internazionale
MEF – Ministero dell'Economia e delle Finanze
MiSE – Ministero dello Sviluppo Economico
MIT – Ministero delle Infrastrutture e dei Trasporti
NATO – North Atlantic Treaty Organization
NIS – Network and Information Systems
NISCG – NIS Cooperation Group
NSC – Nucleo per la Sicurezza Cibernetica
OEWG – Open Ended Working Group
ONU – Organizzazione delle Nazioni Unite
OSE – Operatori di Servizi Essenziali
OSCE – Organizzazione per la Sicurezza e la Cooperazione in Europa
PoC – Punto di contatto unico NIS
PN – Piano Nazionale per la protezione cibernetica e la sicurezza informatica

RAN – Radio Access Network
RAT – Remote Access Tool
SOC – Security Operations Center
TELCO – Fornitori di reti e di servizi di comunicazione elettronica accessibili al pubblico
UdA – Unità per l'Allertamento
UE – Unione Europea
UN GGE – United Nations Group of Governmental Experts