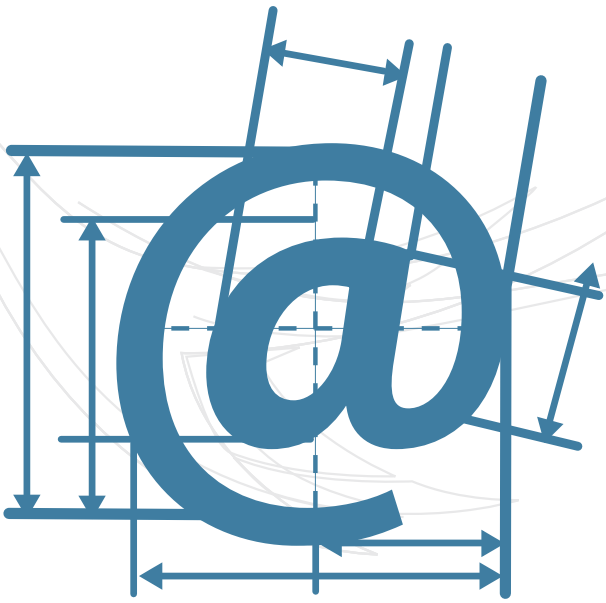
SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

DOCUMENTO DI SICUREZZA NAZIONALE



2019

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO
AI SENSI DELL'ART. 38, COMMA 1 BIS, LEGGE 124/2007

INDICE

Stato della minaccia cibernetica

Ambiti e attori

In ragione dell'elevata disponibilità di tool offensivi e della loro estrema pervasività e persistenza, 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**.

Il costante monitoraggio intelligence delle Tecniche, Tattiche e Procedure-TTP adottate dagli attaccanti ha consentito di rilevare il progressivo innalzamento della qualità e della complessità di alcune operazioni, confermando il crescente riutilizzo tanto di oggetti malevoli quanto di intere infrastrutture di attacco, le cui risorse sono state, talora, impiegate contestualmente, in modo più o meno consapevole, da diversi attori ostili. Tale modus operandi ha consentito ad alcuni gruppi Advance Persistent Threat-APT di acquisire elementi sulle capacità offensive dei "competitor" e di effettuare interventi sulle loro infrastrutture per minarne l'operatività ovvero per impiegarle per attività intrusive, cosi da occultare la reale provenienza dell'attacco.

Obiettivo primario dell'intelligence ha continuato ad essere il **contrasto delle campagne di spionaggio digitale**, gran parte delle quali riconducibili a gruppi strutturati di cui è stata ritenuta probabile – alla luce sia delle ingenti risorse dispiegate, sia della selezione dei target, quasi sempre funzionale al conseguimento di obiettivi strategici e geopolitici – la matrice statuale.

La principale finalità di tali campagne è stata infatti l'esfiltrazione di informazioni dalle infrastrutture informatiche riferibili ad Amministrazioni pubbliche centrali, volta a meglio comprendere la postura del nostro Paese sui dossier d'interesse per l'attaccante.

Ripetuti tentativi di intrusione sono stati effettuati anche nei confronti degli assetti cibernetici di operatori del settore petrolchimico, pure italiani, in quanto parte integrante della catena del valore di primarie realtà internazionali afferenti all'ambito Oil & Gas.

Nello sviluppo delle cennate operazioni, i gruppi APT hanno continuato a privilegiare la **compromissione dei sistemi di gestione e smistamento della posta elettronica**, in cui sono state inoculate sofisticate ed inedite versioni di artefatti malevoli. In tale ambito, l'intelligence ha avuto modo di rilevare come gli attaccanti abbiano monitorato le comunicazioni elettroniche scambiate da utenti del target – tra cui anche quelle di figure apicali – procedendo poi a sottrarre illecitamente i contenuti, il tutto in modo assolutamente "stealth".

Propedeutica allo svolgimento delle citate attività è stata la costituzione di **articolate reti di anonimizzazione**, realizzate compromettendo nodi tra loro eterogenei connessi ad internet ed esposti a vulnerabilità note (su tutti, i dispositivi di tipo Network Attached Storage-NAS), da impiegare per esfiltrare informazioni e gestire da remoto l'infrastruttura di Comando e Controllo nonché per sottoscrive-

re servizi IT commerciali (domini web, servizi di hosting, etc.) con provider localizzati in diverse regioni geografiche, in modo da rendere ancora più difficoltosi i tentativi di individuazione e attribuzione.

Le manovre di matrice hacktivista, operate prevalentemente da formazioni minori contigue al collettivo digitale "Anonymous Italia" (su tutte, AnonPlus ITA, AntiSec ITA e LulzSec_ITA), hanno fatto registrare – in un contesto di complessiva contrazione delle attività di tali sodalizi – l'avvio delle campagne "#OpLavoro" ed "#OpAngelieDemoni": la prima, contro le cosiddette "morti bianche", con azioni in danno di enti pubblici ed organizzazioni operanti nel mondo del lavoro; la seconda, tesa ad evidenziare presunte illiceità nel sistema di affido dei minori da parte di amministratori locali ed operatori dei servizi sociali.

Si è confermato marginale l'attivismo di individui e gruppi di matrice cyberterrorista.

Andamento della minaccia

Per una migliore comprensione dello scenario descritto, si riportano – in linea di continuità con quanto fatto in passato – elaborazioni statistiche concernenti le attività ostili perpetrate, attraverso il dominio cibernetico, ai danni degli assetti informatici rilevanti per la sicurezza nazionale. Ciò, sulla base degli elementi ricavati dalla raccolta informativa delle Agenzie ovvero acquisiti nell'ambito della partnership pubblico-privato e della cooperazione con i principali Servizi collegati esteri nonché presso i dedicati esercizi internazionali NATO e UE.

In punto di metodo – nel rammentare i tangibili progressi conseguiti in termini di detection degli attacchi cyber quale diretta conseguenza del costante potenziamento organizzativo e tecnologico perseguito dal Comparto (in un'azione di impulso che si estrinseca anche verso le Amministrazioni CISR) – si evidenzia come rigorose esigenze di riservatezza circa l'entità numerica delle minacce rilevate ne impongano la divulgazione solo in termini percentuali.

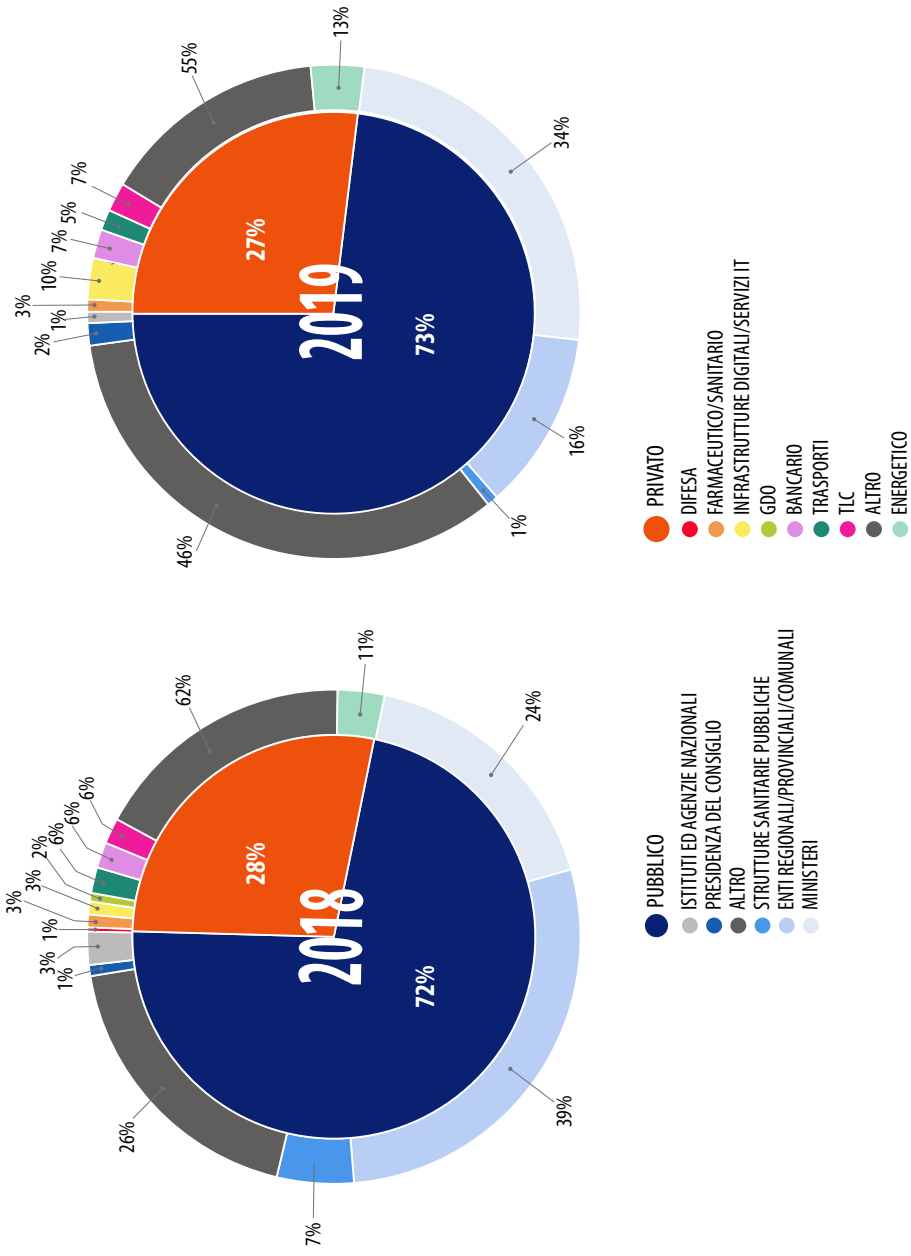
Tanto premesso, nel 2019 tali dati – espressivi dunque delle sole manifestazioni "critiche" del fenomeno – evidenziano un numero complessivo di azioni ostili quasi dimezzato rispetto al 2018, con ciò riportando, dopo il picco registrato nel raffronto 2017-2018, lo sviluppo tendenziale su valori maggiormente in linea con l'osservazione complessiva dell'andamento della minaccia.

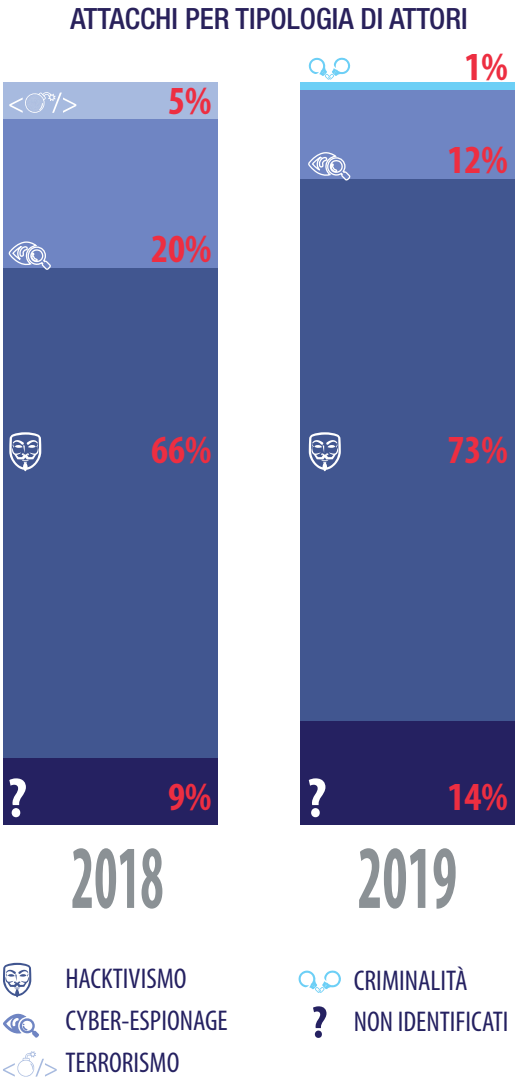
Tra i target privilegiati si sono confermati **i sistemi informatici di Pubbliche Amministrazioni centrali e locali** (73%).

La ripartizione degli attacchi in ambito pubblico ha visto in leggero aumento quelli diretti verso i principali Ministeri (+10%) ed in diminuzione quelli in danno di assetti IT di enti locali, che sono scesi al 16% del totale, facendo registrare una contrazione di oltre 20 punti percentuali.

Le risorse web di varie associazioni di categoria e sindacati (assimilati, ai fini della presente rilevazione, ai "soggetti pubblici" ed inseriti nella categoria "Altro", con percentuali anno su anno pressoché invariate) sono state interessate da azioni di matrice hacktivista nell'ambito della citata "#OpLavoro".

ATTACCHI PER TIPOLOGIA DI TARGET



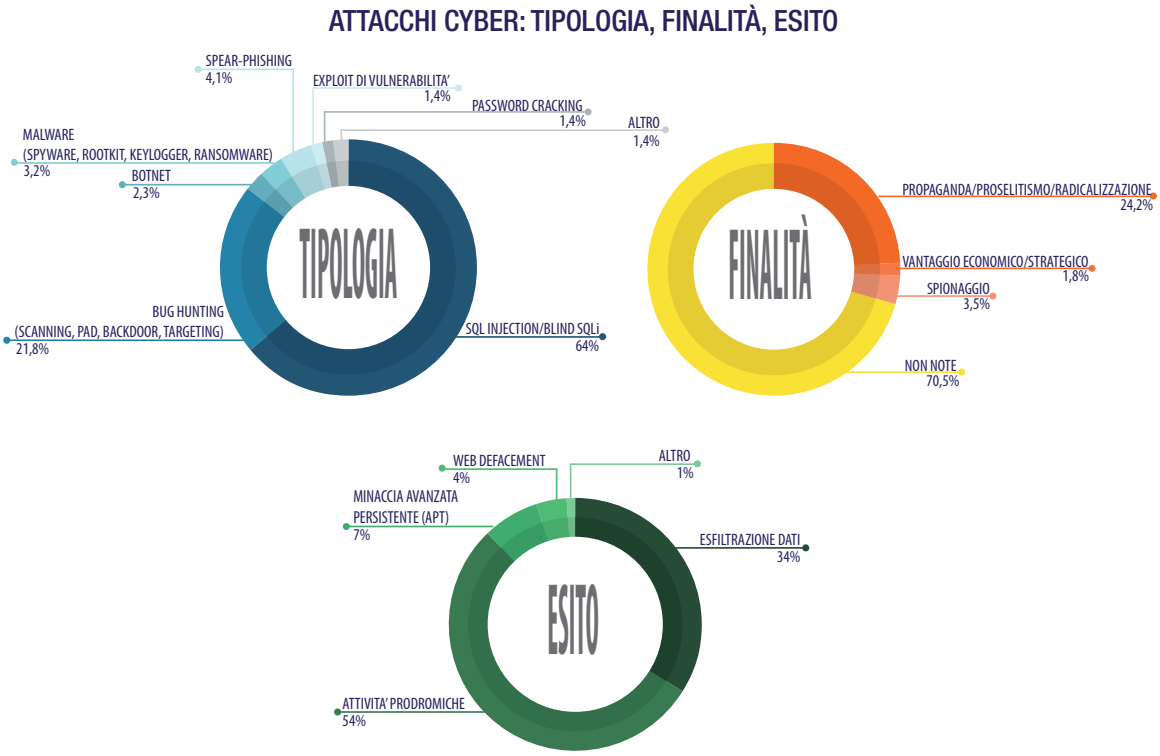


La maggioranza delle azioni ostili contro soggetti privati, è da ricondurre alle stesse formazioni hacktiviste (che le hanno poste in essere in concomitanza con l'annuale manifestazione di protesta "Million Mask March"), così come quelle nei confronti di piccole organizzazioni senza scopo di lucro (anch'esse annoverate nell'ambito della categoria "Altro"), attuate in occasione della campagna "#OpAngelieDemoni".

Guardando alla minaccia dalla prospettiva degli attori ostili, il 2019, nel confermare il trend degli ultimi anni, ha identificato l'**hacktivismo** come la **minaccia numericamente più consistente** (73%), seguito dalle campagne digitali di matrice statuale (12%), in leggero calo rispetto al 2018. Letta insieme all'incremento degli attacchi non immediatamente riconducibili alle categorie di attori in analisi (14%, in aumento di 5 punti percentuali), tale riduzione potrebbe tuttavia essere ascritta sia alle **aumentate capacità di offuscamento degli attori statuali** – che fanno ampio riscorso a tecniche cd. anti-forensics – sia alla crescente disponibilità nel dark web di impianti malevoli (molti dei quali di originaria fattura "statuale"), che contribuiscono entrambe a rendere arduo il processo di attribuzione.

Le **tipologie di attacco** rilevate hanno confermato il **predominante ricorso** dei gruppi antagonisti **a tecniche di SQL Injection** per violare le infrastrutture delle vittime (64% del totale), solitamente precedute da attività di scansione di reti e sistemi (cd. Bug Hunting, circa il 22%) alla ricerca di vulnerabilità da sfruttare nelle fasi successive dell'attacco. A tali tecniche si sono affiancate massive **campagne di spear-phishing** (4,1%), tese verosimilmente all'inoculazione di impianti malevoli (3,2%), quali web-shell e rootkit, di norma impiegati per acquisire il controllo remoto delle risorse compromesse.

In termini di esiti, si è assistito ad un'inversione di tendenza che ha decretato un rilevante **incremento di azioni prodromiche** a potenziali, successivi attacchi (54% del totale, in aumento di 30 punti percentuali) rispetto alle offensive tese a



sottrarre informazioni da assetti informatici effettivamente compromessi (34%).

Il citato aumento delle attività preparatorie è causa del corrispondente incremento delle iniziative alle quali non è stato possibile attribuire una chiara finalità (70,5%), che rappresentano nel 2019 la maggioranza assoluta, seguite dalle azioni ostili poste in essere per scopi di propaganda (24,2%), perlopiù di matrice hacktivista. Sono rimaste invece marginali, quantomeno in termini numerici, le campagne con finalità di spionaggio (3,5%), verso le quali, peraltro, si è mantenuta elevata l'attenzione del Comparto, attesa l'insidiosità di tale minaccia e l'esigenza di promuovere a beneficio dei target ogni utile azione di prevenzione e mitigazione.

Sul fronte della **minaccia ibrida** – caratterizzatasi, anche nel 2019, per il prevalente impiego di strumenti cyber per indebolire la tenuta dei sistemi democratici occidentali – è proseguita l'azione di coordinamento del Comparto a livello sia nazionale (con l'avvio di dedicati raccordi interistituzionali volti a mettere a sistema e potenziare le capacità di risposta del nostro Paese) sia internazionale, con l'obiettivo di seguire ed orientare in modo favorevole ai nostri interessi gli sviluppi sulla materia, nei molteplici esercizi dove la stessa è trattata.

In linea con quanto fatto in passato – ed in parallelo con la dedicata iniziativa promossa al riguardo dalla UE – il Comparto ha riattivato, in concomitanza con le operazioni di voto per il rinnovo del Parlamento europeo del 26 maggio,

il monitoraggio dei possibili canali di propagazione della minaccia: dalla dimensione cibernetica, impiegata per la conduzione di operazioni di influenza online, alle manovre di tipo convenzionale.

Iniziative internazionali in materia di disinformazione e minaccia ibrida

Tra gli esercizi internazionali in materia di disinformazione e minaccia ibrida cui partecipa il Comparto si annoverano:

- il Rapid Alert System dell'Unione Europea, finalizzato alla condivisione di informazioni tra gli Stati membri per prevenire/contrastare eventuali attività di disinformazione;
- l'Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats, operante in seno al Consiglio dell'Unione Europea, il cui obiettivo è facilitare il coordinamento sulle minacce ibride per aumentare la consapevolezza e la resilienza dell'Unione e dei singoli Stati Membri;
- lo European Centre of Excellence for Countering Hybrid Threats di Helsinki, hub internazionale di esperti intergovernativi sulla materia, operante alla stregua di un "in-house think tank" per NATO e UE, a beneficio delle quali produce analisi strategiche ed eroga training specialistico;
- il Rapid Response Mechanism del G7, che impegna i Paesi del Gruppo a rafforzare la cooperazione internazionale attraverso un maggiore scambio informativo, così da identificare e rispondere alle molteplici minacce poste ai processi democratici.

Potenziamento della resilienza cibernetica del Paese

Reti di nuova generazione (5G)

L'anno trascorso – in cui **gli sviluppi tecnologici e le correlate sfide** hanno assunto una **inedita dimensione geopolitica e geostrategica**, confermando come il sistema di protezione cibernetica vada inteso in senso ampio, fino ad includere la sicurezza della supply chain – ha richiesto un particolare impegno del Comparto sul fronte delle minacce potenzialmente connesse con l'implementazione delle reti di nuova generazione nel nostro Paese. Nei confronti del 5G – che avrà impatti significativi su contesti industriali evoluti e su infrastrutture critiche per le quali lo stesso 5G sarà una tecnologia abilitante – l'intelligence ha cominciato ad operare a valle dell'assegnazione delle frequenze agli operatori di telecomunicazione attivi sul nostro territorio, conclusasi nell'ottobre 2018.

L'elevata attenzione degli Organismi informativi va ricondotta alla circostanza che all'avvento del 5G ha fatto (e continuerà a fare) da sfondo **un contesto caratterizzato dal predominio tecnologico di alcuni attori e dalle preoccupazioni di altri rispetto al rischio di abuso delle nuove infrastrutture per finalità ostili**.

Hanno confermato la portata globale di questa sfida gli interventi posti in essere dalla Commissione Europea con l'emanazione, il 26 marzo, di una Raccomandazione che ha chiamato gli Stati Membri ad effettuare un'analisi dei rischi di sicurezza del 5G a livello nazionale. Gli esiti di tale analisi, dai quali è stato

ricavato l'assessment europeo (approvato ad ottobre), hanno costituito il punto di riferimento per la definizione di mirate misure di mitigazione (il cd. toolbox), finalizzate in dicembre e rese pubbliche il 29 gennaio 2020.

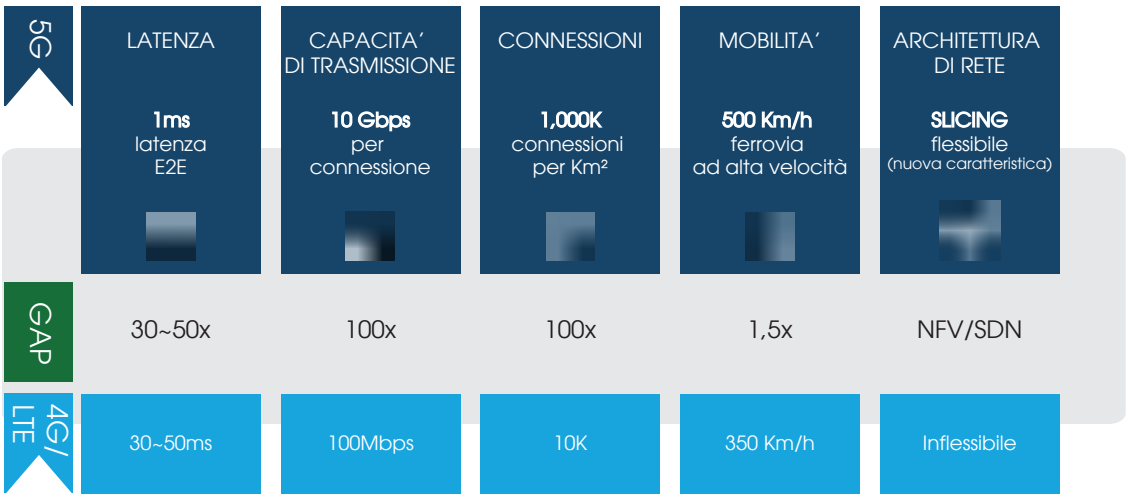
Nel **risk assessment nazionale** – elaborato dal Comparto, in raccordo con Ministero dello Sviluppo Economico-MiSE ed AGCOM e con il rilevante ausilio degli operatori assegnatari di frequenze – sono stati prima identificati gli asset più rilevanti dell'architettura 5G e poi analizzati i profili di rischio rispetto a intenzioni, mezzi e capacità degli attori ostili.

Il nostro Paese ha adottato dunque un **approccio basato su parametri oggettivi** – connessi, cioè, alle caratteristiche della nuova tecnologia – individuando

Caratteristiche delle reti di nuova generazione

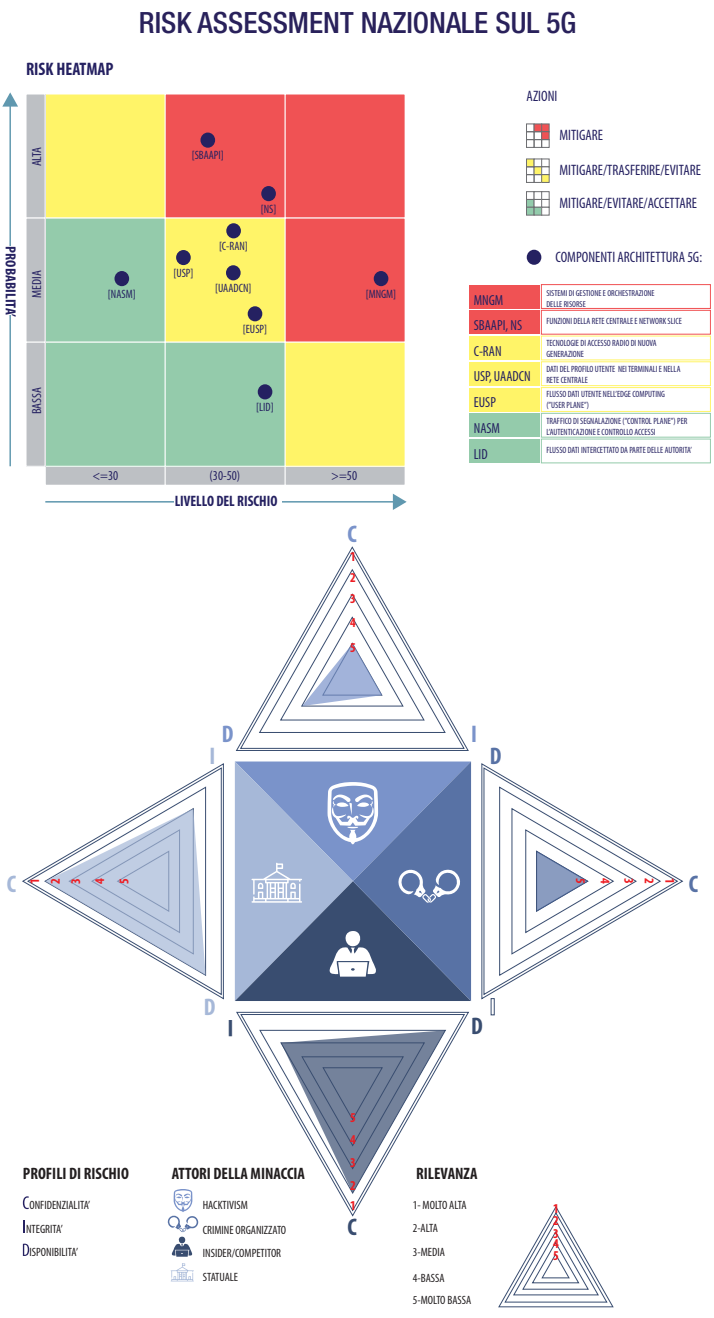
Con il 5G si passerà, in sostanza, dall'uso di architetture e sistemi dedicati – in cui componenti hardware e software coesistono in uno stretto rapporto di interdipendenza – a un modello estremamente più fluido, dove gli elementi fondamentali della rete assumono la forma di moduli software che possono essere messi in esecuzione all'interno di sistemi virtualizzati, basati su piattaforme hardware le cui risorse sono allocabili dinamicamente in base ai livelli di servizio desiderati. Si tratta del paradigma del cloud computing al quale siamo ormai abituati, che ora viene però applicato anche alle funzioni di rete. In questo senso, si parla infatti di "reti programmabili", di "softwarizzazione" della rete e di "network slicing". Da questo dinamismo deriva anche la possibilità di dislocare la potenza di calcolo, di solito accentrata nelle strutture "core", verso la periferia, in modo da erogare servizi complessi con tempi di risposta minimi, secondo il modello noto come "edge computing".

La tecnologia 5G prevede specifici casi d'uso in cui la rete è servente alla comunicazione automatizzata tra oggetti dislocati massivamente sul territorio: essa sarà dunque la "dorsale" dell'"Internet delle cose", che innerverà la comunicazione massiva tra macchine. Inoltre, le caratteristiche di bassa latenza e altissima affidabilità offerte dal 5G saranno impiegate dai sistemi a guida autonoma e di telemedicina, rivoluzionando, tra gli altri, i settori del trasporto e della salute.



strumenti idonei a fronteggiare i rischi per la sicurezza nazionale.

Si è, in primo luogo, intervenuti estendendo al 5G l'ambito dei poteri speciali attribuiti al Governo nei settori strategici (cd. **Golden Power**), prescrivendo agli operatori di notificare i contratti per l'acquisizione di beni e servizi connessi a quelle reti conclusi con fornitori extra-europei, inclusi quelli che, pur avendo sede legale in Europa, sono controllati da società site al di fuori dell'UE. In tale



contesto, il Governo può opporre il veto all'acquisizione o imporre prescrizioni di sicurezza, la cui attuazione è oggetto di specifico monitoraggio.

L'esperienza maturata in questo breve lasso di tempo ha visto diversi operatori effettuare notifiche, rispetto alle quali sono state **prescritte stringenti misure di sicurezza**.

In base alla disciplina dettata dalla legge istitutiva del "Perimetro di sicurezza nazionale cibernetica" (vedi infra), tali prescrizioni potranno essere aggiornate a seguito dell'entrata in vigore dei regolamenti attuativi della predetta normativa, laddove fosse necessario adeguarne il contenuto rispetto alle nuove disposizioni e ai livelli di sicurezza da queste previsti.

Nodali sono stati, anche in questo ambito, i rapporti con il settore privato intrattenuti in seno al **Tavolo Tecnico Imprese** (TTI), che ha visto crescere, tra l'altro, il numero dei suoi partecipanti, confermando ancora una volta la **centralità della collaborazione tra istituzioni ed operatori privati strategici** in materia di tutela della sicurezza nazionale cyber. In occasione di eventi che hanno interessato singole imprese appartenenti al Tavolo o settori determinati, si è provveduto a fornire ausilio mirato in formato bilaterale, a supporto delle azioni di rilevazione, mitigazione ed eradicazione di specifiche minacce. Ciò mentre, sul piano più generale, il TTI ha continuato a rappresentare la sede privilegiata per lo scambio di informazioni di natura tecnica sulle campagne ostili nonché per la condivisione di briefing di taglio analitico volti a contestualizzare l'attivismo nel dominio cibernetico dei principali interpreti della minaccia.

Perimetro di sicurezza nazionale cibernetica

Lo **sviluppo più significativo** registrato dall'ecosistema cyber nazionale è stato l'**istituzione del cd. "Perimetro di sicurezza nazionale cibernetica"** (Legge 18 novembre 2019, n. 133), iniziativa promossa dal Comparto al fine di consentire al Paese di fronteggiare adeguatamente le sfide poste dall'evolversi della minaccia cibernetica nelle sue molteplici forme, a partire da quelle di matrice statuale. Una minaccia accresciuta dalla sempre maggiore interconnessione dei sistemi e dall'avvento di nuove tecnologie – in primis il 5G e quelle rispetto alle quali il 5G sarà, come detto, fattore abilitante, inclusa l'Intelligenza Artificiale – che, se da un lato forniranno soluzioni native in grado di proteggere in modo ancora più incisivo i dati e le comunicazioni, dall'altro pongono delicati problemi sul fronte della sicurezza, e non solo sul versante tecnico.

A livello globale si sta infatti giocando **una partita strategica nella quale sicurezza cibernetica e sicurezza nazionale sono indissolubilmente legate**. In questo contesto la mancanza di autonomia tecnologica, che caratterizza il mercato digitale italiano ed europeo in genere, ha determinato l'esigenza di prevedere meccanismi di tutela che facciano leva contestualmente su screening degli investimenti e screening tecnologico.

In questo senso, l'adozione della Legge n.133/2019 di conversione, con modificazioni, del Decreto Legge 21 settembre 2019, n. 105, recante "disposizioni

urgenti in materia di perimetro di sicurezza nazionale cibernetica", ha finalizzato un processo, avviato nel 2018 a seguito di deliberazione del Comitato Interministeriale per la Sicurezza della Repubblica (CISR), frutto della necessità e urgenza, rilevate dal Governo, non solo di disporre del "sistema perimetro" in tempi rapidi, ma di prevedere altresì:

- il raccordo con la normativa sul cd. Golden Power in materia di apparati e tecnologie 5G, per gli aspetti relativi alla valutazione tecnica dei fattori di vulnerabilità, affidata al Centro di Valutazione e Certificazione Nazionale (CVCN), istituito presso l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del MiSE con Decreto del Ministro del 15 febbraio 2019;
- l'**assegnazione al Presidente del Consiglio di strumenti d'immediato intervento** che consentano, su deliberazione del CISR, di affrontare con la massima efficacia e tempestività situazioni di rischio grave e imminente per la sicurezza nazionale in ambito cyber.

Nell'architettura disegnata dalla citata Legge 133/2019, il DIS – in coerenza con il mandato di supportare il Presidente del Consiglio dei Ministri nell'esercizio delle sue funzioni di alta direzione e responsabilità generale della politica dell'informazione per la sicurezza anche nel dominio cyber – è stato investito del compito di garantire il raccordo con le Autorità e i soggetti "perimetrati", così da assicurare la coerenza e l'unitarietà di indirizzo nell'implementazione della norma. Per tali motivi, il CISR tecnico – presieduto dal Direttore Generale del DIS e composto dai Direttori degli Organismi informativi nonché da dirigenti di vertice dei Ministeri rappresentati nel Comitato – ha anche assegnato al Dipartimento il coordinamento delle attività che Presidenza del Consiglio dei Ministri, Amministrazioni CISR e Comparto intelligence devono porre in essere per l'elaborazione

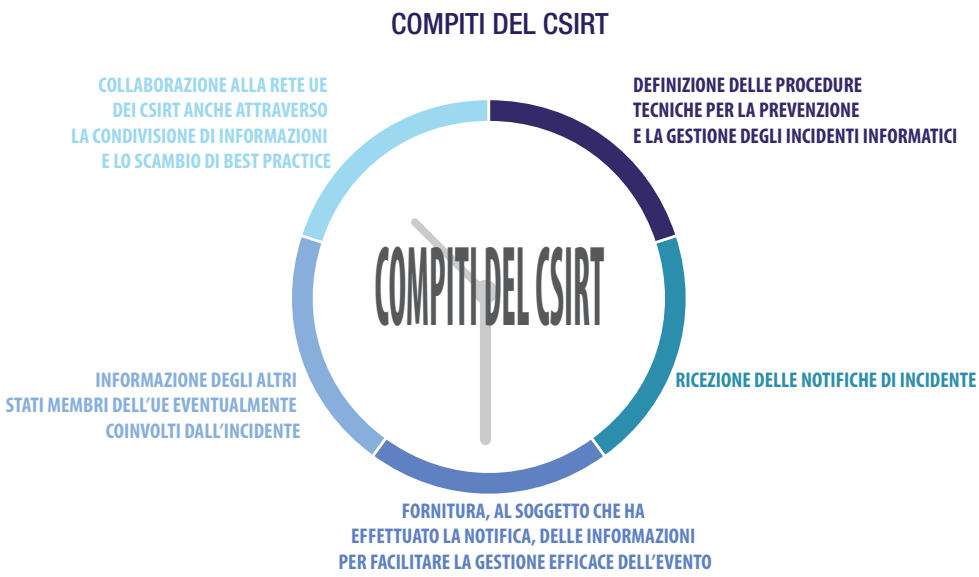
della disciplina attuativa della legge, che porterà entro la fine del 2020 alla piena operatività del "sistema perimetro".

IL "PERIMETRO" IN PILLOLE	
A chi si applica	Soggetti nazionali pubblici e privati che – impiegando reti, sistemi informativi e servizi informatici – esercitano una funzione essenziale dello Stato ovvero assicurano un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato
A cosa si applica	Reti, sistemi informativi e servizi informatici dei soggetti inclusi nel "perimetro" dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale
Cosa prevede	• Notifica degli incidenti, così da assicurare un immediato flusso di informazioni a favore delle strutture deputate alla prevenzione, preparazione e gestione degli eventi cyber (in particolare CSIRT e Nucleo per la Sicurezza Cibernetica, entrambi incardinati nel DIS) • Misure di sicurezza relative a organizzazione, processi e procedure, anche in relazione al procurement ICT • Screening tecnologico degli approvvigionamenti ICT appartenenti a categorie specifiche, destinati agli asset inclusi nel "perimetro". La procedura prevede che il soggetto che intenda procedere a tali acquisizioni ne dia comunicazione al Centro di Valutazione e Certificazione Nazionale (CVCN), che, entro un massimo di 60 giorni, può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software • Attività ispettiva e sanzionatoria a cura di Presidenza del Consiglio dei Ministri e MiSE, rispettivamente per i soggetti pubblici e per quelli privati "perimetrati" • Norme di coordinamento con il Decreto Legislativo n. 65/2018, di recepimento della Direttiva NIS, e con il Codice delle Comunicazioni Elettroniche per i soggetti sottoposti contestualmente ad una di queste discipline e alla legge sul "perimetro"
Poteri d'emergenza	In presenza di un rischio grave ed imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, il Presidente del Consiglio – ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione – può disporre, previa deliberazione del CISR, la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati

Ulteriori evoluzioni dell'ecosistema cibernetico nazionale

Un ulteriore, significativo sviluppo si è poi registrato con la **costituzione presso il DIS** – disposta dal DPCM 8 agosto 2019 – **del Computer Security Incident Response Team (CSIRT) italiano**, struttura che si affianca al Nucleo per la Sicurezza Cibernetica (NSC) e al punto di contatto unico NIS, anch'essi istituiti presso il Dipartimento e con i quali il suddetto Team è chiamato ad interfacciarsi.

Il DPCM prevede che la nuova struttura inizi ad operare entro maggio 2020, assumendo i compiti sin qui assolti da CERT-N e CERT-PA rispetto a cittadini, imprese e amministrazioni pubbliche. A tal fine, sono state intraprese le opportune iniziative per assicurare in tempi contenuti l'operatività del CSIRT a partire dalla definizione



delle procedure per la prevenzione e la gestione degli incidenti informatici, la ricezione delle relative notifiche e la partecipazione alla rete UE dei CSIRT.

Il combinato disposto della legge sul "perimetro" e del DPCM istitutivo del CSIRT conferisce **ulteriore centralità e valenza alle attività dell'NSC**, facendone lo **snodo dei livelli politico, operativo e tecnico**.

Tale organismo collegiale – presieduto dal Vice Direttore Generale del DIS con delega al cyber – si è riunito con cadenza mensile agendo in chiave di prevenzione, preparazione, risposta e ripristino rispetto ad eventuali situazioni di crisi cibernetica, con l'obiettivo di rafforzare le capacità di difesa del Paese.

Nel corso del 2019, l'NSC ha tra l'altro: verificato lo stato di attuazione delle misure di coordinamento interministeriale per la gestione delle crisi cyber; supportato le Amministrazioni partecipanti nell'implementazione di progetti volti ad incrementare le rispettive capacità di difesa e prevenzione; promosso e coordinato la partecipazione nazionale ad esercitazioni cyber (meritano particolare menzione, in proposito: la "Blue OLEx 2019", volta a definire procedure operative condivise in ambito UE per la gestione di incidenti cibernetici su vasta scala; la "EU ELEx 2019", promossa nell'ambito del Gruppo di Cooperazione NIS con l'obiettivo di testare le capacità del livello operativo delle autorità deputate alla gestione del processo elettorale europeo; la "G7 Cyberincident Cross-border Coordination Exercise", per testare la resilienza del settore finanziario dei Paesi del G7).

Pure di rilievo, le attività svolte – in stretto raccordo con il MAECI – nell'ambito della **International Cooperation Strategy**, tesa a valorizzare le eccellenze industriali nazionali e a propiziare rapporti di collaborazione con primari partner esteri.

Sono proseguite, inoltre, le attività di implementazione degli indirizzi previsti dal "Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico" e

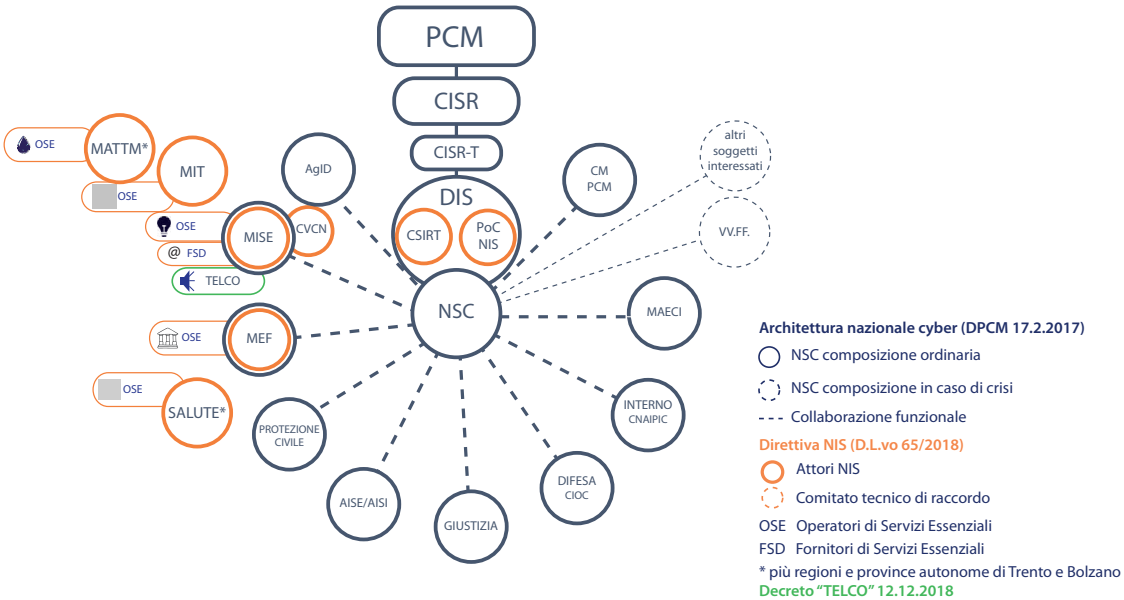
delle linee operative declinate nel "Piano Nazionale per la protezione cibernetica e la sicurezza informatica" anche attraverso:

- la promozione e supervisione di un dedicato gruppo di lavoro per elevare i livelli di sicurezza ICT delle forniture pubbliche. L'esercizio, cui hanno partecipato le Amministrazioni NSC e Consip, si è concluso con l'elaborazione, sotto il coordinamento di AgID, di dedicate **"linee guida per la sicurezza nel procurement ICT"**;
- il patrocinio della **Cyberchallenge.it**, il programma di formazione organizzato dal Consorzio Interuniversitario Nazionale per l'Informatica (CINI) rivolto a giovani talenti destinati ad integrare la prossima generazione di professionisti della sicurezza informatica, che ha raccolto 3.500 iscrizioni in 18 Atenei italiani.

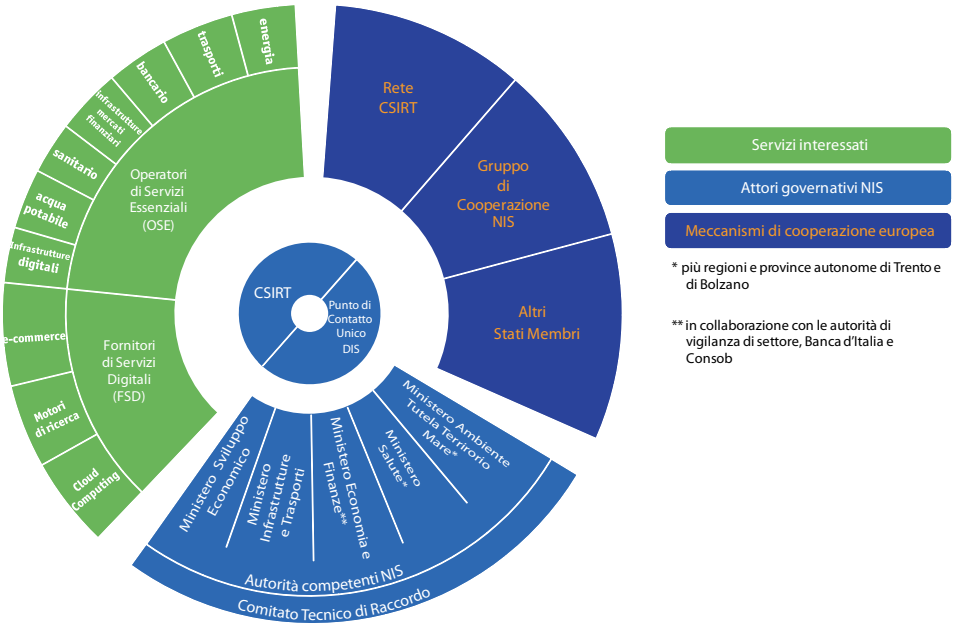
Fitti e costanti sono stati **i raccordi** promossi **con le Autorità competenti NIS e con CERT-N e PA**, per assicurare una coerente, armonica implementazione del Decreto Legislativo n. 65/2018 di attuazione della **cd. Direttiva NIS**. Un formato interistituzionale che ha consentito la definizione coordinata delle soglie per la notifica degli incidenti cibernetici con impatti rilevanti nonché l'elaborazione, sulla base del framework sviluppato dal CINI in materia di cybersecurity e di data protection, delle linee guida recanti le misure di sicurezza che gli Operatori di Servizi Essenziali-OSE sono tenuti a rispettare.

Il DIS ha, altresì, assicurato la partecipazione alla rete dei CSIRT e al Gruppo di Cooperazione NIS – foro di discussione all'interno del quale i Paesi membri si confrontano su tematiche di taglio politico-strategico connesse con l'implementazione della Direttiva NIS – fornendo un apporto significativo alla

ECOSISTEMA CYBER ITALIANO



GLI ATTORI DELLA DIRETTIVA NIS



definizione delle procedure di risposta coordinata a crisi e a incidenti cibernetici su scala europea (cd. Blueprint).

Sviluppi registrati a livello europeo: dalla resilienza alla deterrenza

Continuativa è stata la partecipazione ai principali consessi UE, NATO, G7 e OSCE, nell'ambito dei quali è stata seguita la negoziazione dei principali atti normativi e documenti di policy in materia cyber.

A livello UE sono in particolare proseguite le attività volte ad assicurare il conseguimento degli obiettivi previsti dalla Comunicazione congiunta della Commissione europea e dell'Alto Rappresentante dell'Unione per gli Affari Esteri e la Politica di Sicurezza al Parlamento europeo in tema di "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE" (cd. "**Cybersecurity Package**" del 13 settembre 2017).

Per quel che concerne il potenziamento della resilienza della UE rispetto ad attacchi cyber, di rilievo sono l'entrata in vigore (27 giugno) del Regolamento (cd. "**Cybersecurity Act**") che introduce un quadro europeo di certificazione per le tecnologie ICT e rafforza il mandato dell'Agenzia per la cybersecurity (ENISA) nonchè l'adozione di un primo set di procedure di risposta coordinata a crisi e a incidenti cibernetici su scala europea.

Nel medesimo contesto si colloca la "Proposta di Regolamento per la creazione di un Centro europeo per lo sviluppo industriale, tecnologico e della ricerca in materia di cybersecurity e della rete dei Centri di coordinamento nazionali",

Il cyberdiplomacy toolbox

Le "Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities" (cd. Cyberdiplomacy toolbox), elaborate nell'ambito dell'Horizontal Working Party on Cyber Issues del Consiglio dell'UE, sono state approvate dal Comitato Politico e di Sicurezza l'11 ottobre 2017. Il documento – che ha quale presupposto una situational awareness condivisa e concordata tra tutti gli Stati Membri – individua le possibili misure che le Istituzioni europee e gli Stati Membri della UE possono implementare in risposta ad attività cyber malevole poste in essere da un attore statuale. Le misure di cui al toolbox – preventive, restrittive, di cooperazione, di stabilizzazione, finalizzate a segnalare situazioni di preoccupazione e a sensibilizzare parti terze – possono essere adottate indipendentemente l'una dall'altra, in maniera sequenziale, o parallela, in ogni caso funzionale a un approccio strategico volto a mitigare le minacce cyber, prevenire l'insorgere di conflitti e promuovere la stabilità dello spazio cibernetico a livello globale. Alcune delle misure previste dal toolbox richiedono l'attribuzione quale presupposto per la loro applicazione.

volta a conseguire una sovranità tecnologica dell'Unione – intesa come la capacità di sviluppare nuove tecnologie in alcuni specifici settori (tra cui crittografia, quantum computing e Intelligenza Artificiale), così da acquisire una maggiore autonomia nel dominio digitale – attraverso un migliore coordinamento degli sforzi a livello nazionale ed europeo in materia cyber.

Sul piano del conseguimento di un'efficace deterrenza cibernetica, é da considerarsi di assoluto momento il varo – nell'ambito dell'implementazione del cd. Cyberdiplomacy Toolbox – della Decisione e del Regolamento del Consiglio istitutivi di un **regime sanzionatorio** contro attacchi cibernetici che minacciano l'Unione o i suoi Stati Membri.

IL REGIME SANZIONATORIO UE	
In quali casi si applica	In caso di attacchi cibernetici, inclusi quelli tentati, con potenziali effetti significativi che costituiscono una minaccia esterna nei confronti dell'UE e dei suoi Stati Membri. Le misure restrittive possono essere applicate anche in risposta ad attacchi cibernetici con effetti significativi ai danni di Stati terzi e organizzazioni internazionali, se funzionali al raggiungimento degli obiettivi della Politica Estera e di Sicurezza Comune (PESC)
A chi si applica	Persone fisiche o giuridiche, entità o organismi stabiliti o operanti al di fuori del territorio dell'Unione, ritenuti responsabili di attacchi informatici
Come si applica	L'applicazione del regime viene decisa all'unanimità su proposta di uno Stato Membro o dell'Alto Rappresentante dell'Unione per gli Affari Esteri e la Politica di Sicurezza. L'elenco delle persone fisiche o giuridiche, delle entità o degli organismi cui si applicano tali misure è soggetto a periodico riesame su base almeno annuale
In cosa consiste	Configurabile sotto forma di "travel ban" e "asset freeze", prevede che gli Stati Membri adottino le misure necessarie rispettivamente per: impedire l'ingresso o il transito nel loro territorio di persone fisiche responsabili di attacchi informatici tentati o conclusi, nonché di coloro che sono a queste associati, che forniscono sostegno o che sono altrimenti coinvolti in tali azioni; disporre il congelamento di tutti i fondi e le risorse economiche da questi detenuti o controllati