Audizione Informale nell'ambito dell'esame del Disegno Di Legge C.1717 Governo, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

Roma, 22 Marzo 2024

Premessa

AIAD è la **Federazione**, membro di Confindustria, in rappresentanza delle **Aziende Italiane per l'Aerospazio, la Difesa e la Sicurezza**.

Il 21 novembre dello scorso anno si è costituito in ambito AIAD il Comitato Cyber di cui fanno parte le aziende federate: Grandi Aziende, PMI e start up Italiane, che sviluppano tecnologia proprietaria o che quanto meno hanno al loro interno competenze in diversi ambiti di quello che più comunemente viene chiamato Cyber Space.

Tra gli obiettivi di questo comitato ci sono:

1) la creazione di una **tassonomia** comune all'interno dei pilastri tecnici-operativi così come definiti nel documento "Strategia Nazionale di Cybersicurezza" dell'Agenzia per la Cybersicurezza Nazionale, in particolar modo si fa riferimento alla:

    - Cyber Resilience
    - Cyber Space Operations
    - Cyber Intelligence
    - Cyber Crime Prevention and Repression

2) La definizione di una **mappatura** delle capacità progettuali, manifatturiere e dei servizi delle realtà industriali del comitato stesso, funzionale in ottica di **sovranità tecnologica nazionale.**

3) La disseminazione della **cultura dell'autonomia strategica** valorizzando e tutelando gli interessi nazionali industriali, obiettivo quest'ultimo del tutto in linea con quelli del DDL Cyber che al CAPO I parla esplicitamente di un contesto connesso alla tutela degli interessi nazionali strategici.

Fatta questa doverosa premessa Presidente, si ritiene che l'evoluzione del panorama normativo in materia di cybersecurity sia un chiaro segno di maturità istituzionale e sancisce un nuovo punto di partenza.

Tuttavia è doveroso da parte nostra segnalare alcuni punti di interesse.

Punti di interesse

ART. 11 (Modifiche al codice penale)

Nella seconda parte del Disegno Di Legge, è relativa all'incremento delle pene per i reati di cyber crime, crea delle nuove fattispecie di reato. Tra queste particolarmente rilevante è il tema di cui all'articolo 1, lettera p) che introduce un nuovo articolo nel Codice Penale, 635 quater.1, che introduce il reato di Detenzione, installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

L'articolo in questione pone una serie di questioni di tipo interpretativo e rischia di determinare, nel suo drafting attuale, alcuni paradossi.

Innanzitutto, sotto il profilo interpretativo è necessario che venga meglio chiarito e specificato il concetto espresso dall'avverbio "abusivamente". Cosa significa esattamente, quale fattispecie precisa individua? In particolare, nell'articolato esso è presente nella identificazione delle condotte oggetto di reato in questi termini "…abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa…". L'avverbio "abusivamente" è da leggersi come intrinsecamente giustapposto a ciascuna di queste singole fattispecie? Vale a dire "abusivamente si procura, [abusivamente] detiene, [abusivamente] produce… (etc..)" ? Oppure esclusivamente alla fattispecie cui è esplicitamente associato "abusivamente si procura"? L'incertezza interpretativa potrebbe portare ad effetti pratici paradossali. Ad esempio alla non occorrenza del reato quando la pratica delittuosa sia portata attraverso uno strumento informatico detenuto legittimamente, ma usato illegittimamente. Al contrario, è possibile, soprattutto nell'ambito di talune fattispecie, che il concetto di "abusività" sia difficilmente circostanziabile. Se ben chiaro è il significato di "abusivamente si procura" (evidentemente relativo ad una appropriazione in qualche modo indebita o in violazione di leggi vigenti), non è chiaro cosa dia vita ad una abusiva detenzione, ad una abusiva produzione (non essendo la professione di sviluppatore una professione regolata o il cui esercizio è sottoposto al possesso di un particolare titolo), "abusiva consegna" o "abusiva messa a disposizione di altri".

Sempre ragionando in tema di interpretazione, tale nuovo reato si verifica sotto la condizione che i fatti in oggetto si verifichino "allo scopo di danneggiare illecitamente un sistema informatico". Per cui la semplice occorrenza delle fattispecie prima descritte non integra da sola la dinamica delittuosa ma deve essere "asservita" all'intentum (al solo intentum, non è necessario che il danno si manifesti, basta "lo scopo di…") malevolo di "danneggiare illecitamente".

A tal proposito è necessario sottolineare, anche in questo caso, si pongano dei dubbi interpretativi nella comprensione del sintagma "danneggiare illecitamente", che indurrebbe a pensare che esista -e che quindi sia scriminata- l'ipotesi di "danneggiare lecitamente".

Interpretare in questo senso è auspicabile, poiché in molti casi l'attività di cybersecurity potrebbe portare a svolgere talune delle attività di sopra richiamate, ma non a scopo malevolo, bensì a scopo difensivo. Tuttavia se questo era l'intento del proponente, la formulazione non è certamente delle più chiare ed immediate, soprattutto se pensiamo al fatto che, nell'ordinamento italiano, non è prevista la legittima difesa cibernetica.

Proprio questo può essere il punto di svolta del provvedimento: il riconoscimento del legittimo ricorso all'uso del mezzo informatico per difendersi da una azione violenta che metta a rischio la sicurezza del singolo o di altri ovvero i beni ovvero il domicilio, sebbene digitale.

Poiché nel Diritto Penale non si procede per analogia è necessario intervenire in tal senso per disporre esplicitamente a vantaggio dei cittadini il diritto di difesa, già previsto nella vita cinetica, anche in quella cibernetica, agendo sull'articolo 52 del Codice Penale nelle forme che il Parlamento riterrà più opportune.

Senza questo intervento l'effetto paradossale del nuovo Art. 635 quater.1 del Codice, ma anche di molti degli altri articoli che vengono modificati con inasprimento delle pene, potrebbe essere quello di porre nella condizione gli attori malevoli (hacker) di denunciare i soggetti che operano nell'ambito della cyber resilience e che, attraverso specifiche attività, potrebbero compiere una delle azioni indicate dal nuovo articolo come delittuose.

L'esempio concreto è quello di un Red Team (difesa attiva) che agisca per far cessare un attacco informatico, potrebbe incorrere nel reato -non essendo disposta la fattispecie del "danneggiamento lecito"- per danneggiamento illecito delle capacità dell'hacker. Ancora, il servizio di Cyber Threat Intelligence che recupera nel dark web informazioni che consentono di sventare un attacco informatico potrebbe incorrere nella fattispecie dell' "abusivamente si procura", non essendo definito quando sia invece consentito il "procurarsi" dati, informazioni etc..

ART. 14
(Modifiche al decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203)

Si desidera esprimere apprezzamento per la disposizione recata dall'articolo 14 del Disegno Di Legge, con la quale si riconosce il ruolo e l'efficacia delle sofisticate tecnologie fornite dal comparto delle intercettazioni legali, impiegate come mezzi per la ricerca della prova nel contrasto dei fenomeni criminali, qui confermate come strumento essenziale per il perseguimento di specifici delitti che presuppongono, in capo ai presunti autori, un'elevata capacità informatica.

A questo proposito, giova ricordare che le aziende associate AIAD operanti nel settore del *lawful interception*, per tecnologie proprietarie ed elevatissima specializzazione del personale impiegato, rappresentano un'eccellenza hi-tech dell'industria nazionale al fianco delle Istituzioni, che fa dell'incessante innovazione il suo tratto distintivo.

Si ritiene pertanto, al fine di consentire agli Organi dello Stato di poter continuare a disporre dei dispositivi di cyber investigation ed intelligence adeguati al crescente livello della minaccia posta da organizzazioni criminali sempre più attive nel domino cibernetico, che sia indispensabile individuare specifiche policies per stimolare investimenti a supporto della componente Ricerca & Sviluppo in tale delicato settore, strategico per il Paese.

ART. 18 (Disposizioni finanziarie)

Infine è necessario soffermarsi sull'articolo 18. Le disposizioni finanziarie, che attengono ad entrambi le parti del provvedimento. Un provvedimento molto ambizioso che però deve essere attuato "a costo zero" o meglio "a risorse disponibili". Ciò è semplicemente impossibile. Un nuovo e più ampio sistema di norme sulla cyber resilienza con obblighi ed impegni cogenti ed un rafforzato sistema di contrasto al cyber crime, necessitano di adeguate risorse aggiuntive. In particolare vanno richiamate quelle citate dalla Strategia di Sicurezza Nazionale Cibernetica fissate in una quota annuale pari almeno all'1,2% degli investimenti pubblici. Senza raggiungere quella cifra, con un investimento serio e urgente che faccia arrivare la spesa pubblica del bilancio statale circa a 2 miliardi di euro annui per la cyber, ne le imprese ne le pubbliche amministrazioni potranno avere le possibilità di dotarsi delle soluzioni adeguate o richieste obbligatoriamente da questa o altre normative in arrivo.

Conclusioni

Per garantire la sicurezza di oggi bisogna anticipare le minacce di domani anche attraverso forti partnership pubblico-privato per sviluppare prodotti e soluzioni resilienti nazionali

AIAD è a disposizione per ogni approfondimento necessario a sviluppare questo tipo di partnership volto a raggiungere tutti gli ambiziosi obiettivi del Disegno Di Legge in un contesto connesso alla tutela degli interessi nazionali strategici, coscienti che un'industria d'eccellenza in questo settore, rappresenterà sicuramente un ulteriore volano per l'export.

A.I.A.D.
Federazione Aziende Italiane per l'Aerospazio, la Difesa e la Sicurezza

Via Nazionale 54 – 00184 Roma