Cybersecurity connect

La disciplina europea della Direttiva NIS2

a cura di
CECILIA CAVACEPPI e ALFONSO CONTALDO

prefazione di Donato A. Limone

contributi di Tiziana Barzanti, Cecilia Cavaceppi, Alfonso Contaldo, Claudia Frisani, Giuseppe Gorga, Michele Gorga, Matteo Lucchetti, Sofia Marchiafava, Maddalena Valli

UNIVERSITÀ

tab edizioni

viale Manzoni 24/c
00185 Roma
www.tabedizioni.it

Prima edizione maggio 2024
ISBN versione cartacea 978-88-9295-897-5
ISBN versione digitale 978-88-9295-898-2

Indice

Premessa

L'importanza della cybersecurity nelle strutture di reti

di Alfonso Contaldo

1. Cenni per una sommaria definizione di cybersecurity e di cyber-defence

La parola *cybersecurity* deriva dalla crasi di due parole, *cyberspace* e *security*, ognuna delle quali possiede una propria definizione, consolidata nel tempo e sicuramente meritoria di una autonoma ed elaborata analisi semantica, che però non affronteremo. Ciò su cui ci concentreremo è il nuovo concetto, quasi un neologismo, che risulta da questa crasi e che si è andato imponendo negli ultimi anni: la "cybersecurity"[1]. Secondo una prima ricostruzione, tale definizione richiamerebbe l'idea di «sistema di sicurezza che protegge la rete telematica di uno Stato o di altro ente (privato o pubblico) da eventuali intrusioni perpetrate per via informatica»[2]. In realtà, però, tale definizione, a nostro avviso, benché corretta sembrerebbe non del tutto pregnante.

Analogamente non sembra del tutto assorbente neppure la, seppur corretta, definizione coniata da altre autorevoli fonti che la definiscono come «ways of protecting computer systems against threats such as viruses»[3].

Sembra, forse, più opportuno ricondurre la cybersecurity a quell'insieme di tecnologie, programmi, processi e tecniche concepiti e messi in atto per proteggere dispositivi, dati e reti informatiche.

1. Cfr. R. Marchetti, R. Mulas, *Cybersecurity: Hacker, terroristi, spie e le nuove minacce del web*, Luiss Press (formato Kindle), Roma 2017, pp. 42 ss.

2. Cfr. A. Teti, *Cyber espionage e cyber counteintelligence. Spionaggio e controspionaggio cibernetico*, Rubbettino, Soveria Mannelli 2018, pp. 45 ss.

3. Cfr. F. Kaplan, *Dark Territory: The Secret History of Cyber War,* Simon & Schuster Inc., New York 2016, pp. 62 ss.

Si noti che nella nostra definizione intendiamo richiamare un triplice concetto: da un lato la protezione dei contenuti, dei dati, delle informazioni; un secondo concetto relativo alla protezione hardware (quindi gli elementi fisici dei dispositivi quali PC, smartphone, mainframe, server ecc.); una terza protezione relativa agli aspetti software intesi quali programmi, reti, database, archivi digitali ed altre impostazioni informatiche similari.

Quindi, già da queste linee prodromiche di approccio alla questione, si evince che la demarcazione dei confini della cybersecurity appare piuttosto rarefatta e, teoricamente, in possibile espansione[4]. D'altronde non possiamo immaginare se le nuove tecnologie che esploderanno nel giro di pochi anni potranno essere oggetto di attacchi informatici (ad esempio si ipotizzi un futuro ed eventuale attacco ai meccanismi di ricarica wireless di dispositivi informatici in grado di approfittare dei sistemi elettromagnetici ad induzione per prendere il controllo di informazioni protette).

Orbene risulta, quindi, determinante ragionare sulla c.d. *soglia di tollerabilità* e ciò apre ad inquietanti scenari che pongono l'attenzione su di un fatto *sui generis*: una sicurezza informatica totale non è possibile.

In realtà, tuttavia, occorre stemperare tale forzatura sottolineando che questa è una analogia anche con il mondo non digitale. Una sicurezza totale da ogni forma di aggressione è, oggettivamente, impossibile. La grande, fondamentale distinzione fra mondo analogico e digitale, comunque, emerge anche in questo caso in maniera subdola.

Se è vero che i sistemi di sicurezza fisici del mondo digitale hanno avuto una evoluzione nel corso dei secoli, alcuni di essi risultano comunque sempre utili ed adeguati in talune situazioni relativamente semplici (ad esempio per interdire l'accesso ad un luogo si può utilizzare un lucchetto). Ciò non è precisamente vero in ambito di sicurezza dei sistemi informatici e telematici. Infatti utilizzare strumenti di protezione obsoleti non si riesce a garantire alcuna forma di protezione (ad esempio usare un antivirus con una definizione dei virus del 1995).

Quindi, in ambito di cybersecurity è sempre e comunque necessario un costante aggiornamento delle tecniche e delle metodologie di protezione.

4. Cfr. A. Teti, *Cyber espionage e cyber counteintelligence. Spionaggio e controspionaggio cibernetico*, cit., pp. 85 ss.

Non si potrà evocare un meccanismo paragonabile al vecchio "lucchetto" del mondo analogico che poteva, entro certi limiti, proteggere un archivio nel 1930 così come nel 2023.

Il senso è che la sicurezza informatica non può essere e non sarà mai totale. Al lavoro di aggiornamento e perfezionamento delle tecniche anti-hacking corrisponde il parallelo progresso delle tecniche di hacking, anzi, sono proprio i progressi fatti dagli hacker e dai creatori di virus a determinare la crescita qualitativa dei sistemi di protezione. Non esiste un sistema di difesa, insomma, che una volta montato renda il nostro computer o le nostre reti sicure per sempre. Si può tentare di fare un parallelismo con il mondo biologico, identificando la preda (il sistema attaccato) ed il predatore (il criminale informatico) e ricordando che l'evoluzione porta ad un perfezionamento delle armi di entrambi senza riuscire, peraltro, a far dominare nessuno dei due. Laddove ciò accadesse, si andrebbe verso l'estinzione di una specie e, nel nostro caso, di una branca della sicurezza informatica o delle tecniche di aggressione digitali.

Il secondo concetto che ci preme analizzare in questa sede riguarda la *cyberdefense* che, in base alle indicazioni rilasciate dal CCDCOE[5] è definita come «misura proattiva per rilevare od ottenere informazioni su un'infrazione informatica, attacco informatico o imminente operazione informatica ovvero per determinare l'origine di un'operazione che comporta l'avvio di una contromisura preventiva o informatica contro la fonte d'aggressione»[6].

La sottile sfumatura che differenzia questo ambito dalla impostazione della cybersecurity è da individuarsi nell'oggetto tutelato. Tipicamente, le dinamiche legate alla cyberdefense sono intimamente connesse a meccanismi di difesa nazionali, sistema militare o paramilitare e protezione delle istituzioni di enti ed organizzazioni governative.

La difesa informatica, in questa accezione, si concentra sulla prevenzione, il rilevamento e la fornitura di risposte tempestive agli attacchi o alle minacce, in modo che nessuna infrastruttura o informazione venga manomessa. Con la crescita del volume e la complessità degli attacchi informatici, la difesa in-

5. Acronimo del Cooperative Cyber Defence Centre of Excellence della Nato, avente sede a Tallin in Estonia.

6. Trad. dall'originale Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America (2013).

formatica è essenziale per la maggior parte delle entità al fine di proteggere le informazioni sensibili e salvaguardare le risorse.

Questa differente accezione, quindi, si dispiega dalla comprensione dell'ambiente specifico, la difesa cibernetica analizza le diverse minacce possibili per l'ambiente dato. Il programma di sviluppo di tecnologie e strumenti adatti a garantire la cyberdefense è basato sull'assunto di ideare e guidare le strategie necessarie per contrastare attacchi o minacce concrete a strutture che, per le loro peculiarità strategiche, potrebbero, laddove aggredite con successo, esporre a gravi minacce di sicurezza interna ed internazionale[7]. Ciò detto, se ne rileva che una vasta gamma di attività diverse è coinvolta nella difesa cibernetica per proteggere l'entità interessata e per la risposta rapida a un panorama di minacce. Queste potrebbero includere tecniche atte a favorire la riduzione di possibili aggressori, la comprensione delle posizioni critiche e delle informazioni sensibili, nonché l'adozione di controlli preventivi per assicurare che gli attacchi non abbiano successo.

In questo ambito, in particolare, è indispensabile una costante operatività ed una efficiente vigilanza ininterrotta con elevatissime capacità di rilevamento ed applicazione di contromisure agli attacchi. Sicché

> l'ampia gamma di azioni ostili può andare dallo spionaggio agli attacchi veri e propri, con finalità di inibire, alterare o addirittura distruggere dati, hardware, reti o eventuali servizi e sistemi ad essi connessi. Generalmente possono essere rivolte ad assetti governativi, economico-finanziari, imprese, infrastrutture critiche o servizi dedicati alla società civile. I possibili effetti da essi generati possono facilmente divenire strategicamente rilevanti oppure influenzare comportamenti, azioni e documentazione collegati anche ad operazioni militari in corso. I protagonisti possono essere entità statuali, gruppi terroristici, organizzazioni criminali o semplici individui dediti alla ricerca di informazioni o alla distruzione/danneggiamento dei sistemi informatizzati e dei dati in essi contenuti.[8]

7. Cfr. A. Teti, *Cyberespionage e cyber counterintelligence. Spionaggio e controspionaggio cibernetico*, cit., pp. 72 ss.

8. Cfr. N. De Felice, *Strategia di difesa nel cyberspazio quale contributo alla tutela degli interessi nazionali*, in Gori U., Germani L.S. (a cura di), *Information Warfare 2011, La sfida della Cyber Intelligence al sistema Italia dalla sicurezza delle imprese alla sicurezza nazionale*, FrancoAngeli, Milano 2012, p. 76.

Ancora una volta, dunque, ne emerge che le minacce potenzialmente realizzabili appaiono nettamente attivabili in maniera del tutto trasversale ai vari ambienti strategici ed operativi. Per la delicatezza di tale vicenda resta essenziale tenerne conto nell'ambito della pianificazione generale.

Orbene la predisposizione di attività di cyberdefense rimangono pressoché interamente devolute ad attività realizzate con piena operatività del comparto della difesa militare.

Pertanto prende sempre più vigore e rilevanza che:

> L'elemento determinante è la conquista della superiorità informativa che, da un lato, assicura a tutti gli elementi della forza amica l'accesso illimitato e tempestivo all'informazione e, dall'altro, nega la stessa capacità all'avversario. Al riguardo si rendono necessari alcuni passi fondamentali: sviluppare capacità e dottrina tali da poter mantenere aggiornata la Situational Awarness (SA) e operare anche nell'ambiente cibernetico al fine di guadagnare e mantenere un sufficiente vantaggio sugli opponenti, proteggere le proprie reti e le proprie infrastrutture critiche cibernetiche, al fine di produrre effetti di dissuasione e di resilienza ad eventuali attacchi.[9]

Sembra doveroso ricordare che, tuttavia, l'ambito applicativo della cyberdefence, nel suo complesso, è decisamente molto diverso da quello della cybersecurity.

Infatti l'esigenza di attività militari comprende anche aspetti molto lontani dal tradizionale ambiente informatico includendo, infatti, anche attività più tradizionali quali, a mero titolo esemplificativo, «l'utilizzo di porte di accesso blindate congiuntamente a sistemi di identificazione personale per l'accesso fisico a locali protetti [...] assicurando la manovra ai comandanti di tutti i livelli, generando libertà d'azione, minimizzando gli effetti di eventuali attacchi e, nel contempo, limitando la manovra avversaria»[10].

9. Cit. Centro Alti Studi per la Difesa, Istituto Superiore di Stato Maggiore Interforze, 17° corso, 1° gruppo di lavoro 1ª sezione, *L'evoluzione della capacità Cyber: da Cyber defence a Cyber Warfare,* lavoro collettaneo di Ten. Col. Pizzuti P.; C.F. Podico P., Ten. Col. Pagani S., Napolitano I., Ten. Col. Pfister L., Capuano G., Magg. D'Altorio L., Ten. Col. De Paolis A., Ten. Col. Iossa D., Magg. Magazzù S., C.C. Marzi F., Musto C., Magg. Peretto R., Magg. Saturnino P., Ten. Col. Stanojevic B., Ten. Col. Tavone D., 2015, pp. 2 ss.

10. *Ibidem.*

Questo contesto conduce alla forma di una differente organizzazione che fa riferimento alla c.d. *Computer Network Operations*[11]. Si rileva che

> le CNO si basano sullo sviluppo capacitivo di tre pilastri fondamentali: a) la Computer Network Defence (CND): una serie di azioni tese a proteggere da attività cibernetiche ostili le info-strutture del CIS e gli assetti della Difesa. Questa attività si sostanzia nella difesa, analisi e sfruttamento dei dati; b) la Computer Network Exploitation (CNE): quella serie di azioni tese ad acquisire ed analizzare dati e informazioni contenute su computer e network d'interesse, al fine di ottenere un vantaggio. Si tratta di una capacità che, se sviluppata adeguatamente, consente anche una più puntuale pianificazione delle operazioni; c) il Computer Network Attack (CNA): le azioni volte a rendere inaccessibili, degradare o distruggere informazioni contenute in un computer o in rete, oppure la rete di computer stessa degli avversari. Questi attacchi necessitano di un preventivo avallo politico, di regole d'ingaggio, nonché della tutela di un quadro normativo e legislativo appropriato.[12]

1.1. *L'implementazione in ambito dell'UE delle policies in materia di cybersecurity*

A seguito degli attentati terroristici di Madrid dell'11 marzo 2004, in ambito europeo, si è iniziato a ragionare in tema di sviluppo di strategie nazionali di cybersecurity, la cooperazione ed il rafforzamento delle capacità dei vari CSIRT[13], ma anche studi sull'adozione sicura del cloud. Affrontando, così, que-

11. Per approfondimenti vedi: P. Shakarian, J. Shakarian, A. Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach*, Syngress, New York 2013; B. Valeriano, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, Hurst, New York 2015; B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*, RAND Corporation, Washington 2016; J.L. Caton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, Strategic Studies Institute, Washington 2016; K. Friis, J. Ringsmose, *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, McGraw Hill, London 2016; U. Gori, S. Lisi (a cura di), *Cyber warfare 2016. Dalle strategie e tecnologie cyber contro il terrorismo all'IoT e Impresa 4.0*, FrancoAngeli, Milano 2017; C. Guitton, *Inside the Enemy's Computer: Identifying Cyber Attackers*, Hurst & Co. Publ., London 2017; M. Taddeo, L. Glorioso (Eds), *Ethics and Policies for Cyber Operations. NATO. Cooperative Cyber Defence Centre of Excellence*, Springer, London 2017; A.A. Tsirigotis, *Cybernetics, Warfare and Discourse: The Cybernetisation of Warfare in Britain*, Springer, London 2017.

12. Cfr. A. Teti, *op. et loc. supra cit*.

13. Sono i Gruppi di intervento per la sicurezza informatica in caso di incidente (*Computer Security Incident Response Team*). Del funzionamento degli stessi ci occuperemo in modo più approfondito nel corso dell'ultimo capitolo del presente lavoro.

stioni relative alla protezione dei dati, tecnologie di protezione della vita privata e della privacy nelle tecnologie emergenti, della eID[14] e della fiducia nei servizi digitali e identificando il panorama delle minacce informatiche.

Si deve inoltre, ricordare che il giorno precedente agli attentati, l'Unione aveva approvato il Regolamento[15] che istituiva l'Agenzia europea di sicurezza delle reti e dell'informazione (ENISA) che ha lo scopo «di assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito della Comunità e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione»[16].

Nel giugno del 2004, anche alla luce dei pericoli legati alla cybersicurezza[17], il Consiglio Europeo ha richiesto la preparazione di una strategia globale per la protezione delle infrastrutture critiche e la Commissione europea, nell'ottobre del 2004, ha adottato una Comunicazione in materia di protezione delle infrastrutture critiche nella lotta contro il terrorismo[18] nella quale, auspicando il «dialogo tra il settore pubblico e quello privato sulle questioni di sicurezza», si elencavano una serie di misure per aumentare la prevenzione, la preparazione e la risposta a livello europeo in caso di attentati contro le infrastrutture critiche[19].

14. Al riguardo ci si permette di rinviare a G. Cassano, A. Contaldo, *Internet e tutela della libertà di espressione*, Giuffrè, Milano 2009, pp. 162 ss. ed alla bibliografia colà citata.

15. Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio del 10 marzo 2004. Ci si permette di rinviare a A. Contaldo, F. Dainotti, *Diritto e tecnologie delle reti di informazione*, Simone, Napoli 2005, pp. 272 ss.

16. Regolamento (CE) n. 460/2004 del 10 marzo 2004 che istituisce l'ENISA, art. 1. Sul punto cfr. A. Contaldo, *L'ENISA e le competenze comunitarie per la cibersicurezza,* in «Rivista di polizia», n. 6, 2018, pp. 452 ss.

17. A tal riguardo si ritiene utile ricordare che la loro correlazione con le infrastrutture critiche è in progressivo aumento, infatti, «In un anno le minacce informatiche contro le infrastrutture critiche nazionali italiane si sono moltiplicati per cinque, con gli alert che nel 2017 hanno toccato quota 28.500, e i veri e propri attacchi che sono arrivati a 1.006. A certificarlo tracciando un bilancio dell'anno appena trascorso è la Polizia postale, confermando così le crescenti preoccupazioni sulla sicurezza informatica di Pubblica amministrazione e imprese e la necessità di implementare con attenzione e regolarità tutte le misure di sicurezza e di protezione», cit. A. Salerno, *Cybersecurity: più di mille attacchi alle infrastrutture critiche in un anno,* in «Corriere comunicazioni», n. 9, 2018, fonte: https://www.corrierecomunicazioni.it/cyber-security/2017-della-cybersecurity-piu-mille-attacchi-infrastrutture-critiche/ (ultimo accesso il 23 aprile 2018).

18. Cfr. COM. 2004/698 del 20/10/2004, Comunicazione della Commissione al Consiglio e al Parlamento europeo, *Prevenzione, preparazione e risposta in caso di attacchi terroristici.*

19. Cfr. L. Franchina, M. Carbonelli, L. Gratta, M. Crisci, *Infrastrutture Critiche: lo stato dell'arte. Direttiva Europea e situazione nazionale*, PCM Segreteria di Coordinamento Interministeriale per le Infrastrutture Critiche, Convegno ICSA, Roma 2010.