Cyber Warfare 2018

Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche

a cura di Umberto Gori

FrancoAngeli

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con

La versione completa dell'e-book (a pagamento) è leggibile con Adobe Digital Editions. Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta cliccando qui le nostre F.A.Q.

Collana di Scienza Politica e Relazioni Internazionali, diretta da Umberto Gori

Il progresso delle scienze sociali è strettamente legato alla ricerca interdisciplinare. Tale indirizzo non ostacola però l'applicazione di un approccio e di un metodo rigorosamente unitari. L'approccio è quello dei sistemi, il metodo è quello della scienza politica più avanzata. L'uno e l'altro mirano a conoscere il reale nella sua complessità, a partire da dati e variabili fattuali, con l'ausilio, anche, di discipline diverse, teorie empiriche e quindi previsioni aventi valore probabilistico.
C'è una fortissima domanda, oggi, di strumenti aggiornati atti ad interpretare fenomeni complessi e talora privi di precedenti ed a consentirne la previsione, data l'accelerazione dei tempi storici.
A questa domanda la «Collana di Scienza Politica e Relazioni Internazionali» si propone, ambiziosamente, di rispondere, cercando anche di rimuovere, in misura progressiva, le resistenze, ancora vive nel nostro Paese, dovute al tradizionale convincimento che il campo sociale non sia coltivabile con gli strumenti euristici che hanno determinato lo sviluppo eccezionale delle scienze della natura.
La denominazione della collana si giustifica per due aspetti: primo, perché di solito quando si parla di scienza politica si pensa al quadro interno e qui invece si vuole accreditare la tesi che anche il sistema internazionale è analizzabile in tale prospettiva; secondo, perché anche per l'analisi corretta del sistema interno è ormai impensabile non fare un sistematico riferimento al contesto internazionale (e viceversa).
La collana svilupperà sia una parte di metodologia e di tecniche analitiche, sia una parte teorica e di ricerca sugli aspetti di sostanza del vasto campo preso in considerazione. Contribuiranno all'una e all'altra metodologi e scienziati politici, sociologi della politica e studiosi dell'amministrazione, comparatisti e cultori di relazioni internazionali.
La collana ha essenzialmente un taglio operativo. I suoi naturali destinatari saranno quindi, oltreché gli specialisti, anche tutti coloro che, ai diversi livelli, sono detentori di responsabilità decisionali. Scopo ultimo è infatti la progressiva «modernizzazione» dell'Italia nel campo della valutazione scientifica dei fatti politici, interni ed internazionali, che è premessa insieme di razionalizzazione dei processi decisionali e di un corretto funzionamento delle istituzioni e della vita democratica del Paese.

Cyber Warfare 2018

Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche

a cura di Umberto Gori

FrancoAngeli

L'evento ha avuto luogo a Milano il 12 dicembre 2018 presso il Centro Congressi Palazzo delle Stelline. La conferenza è stata promossa dal Centro Universitario di Studi Strategici, Internazionali e Imprenditoriali (CSSII), Centro Studi Difesa e Sicurezza (CESTUDIS), CIS Università La Sapienza, Istituto per gli Studi di Previsione (ISPRI), European Center for Advanced Cyber Security (EUCACS) e d'intesa con InTheCyber – Intelligence & Defense Advisors.

Il curatore del volume sente l'obbligo di ringraziare Daria Vernon De Mars, esprimendo il più alto compiacimento per la sua intelligente, paziente e costante collaborazione alla revisione dei testi e all'editing dei presenti Atti.

Indice

Prefazione

di *Paolo Lezzi*[*]

È sempre con grande emozione e stupore che mi accingo ogni anno ad aprire queste conferenze ed a scrivere poi queste poche righe di prefazione, per l'attenzione e la partecipazione ed il seguito che permane negli anni. Ci sentiamo una grande responsabilità nel tipo di temi che ogni anno cerchiamo di proporre, innovativi e delicati. Siamo giunti quest'anno a pubblicare gli atti della nona edizione, ed in procinto di lanciare la decima. Sono quindi passati ben dieci anni dalla prima Conferenza di Roma. Mi sento in dovere di ricordare che c'è stata una pre-edizione, un NATO Advanced Research Workshop[1] all'Arsenale di Venezia nel 2009, al termine del quale è nata l'idea di far nascere queste conferenze. Quindi innanzitutto il mio più grande ed affettuoso ringraziamento va al Professor Umberto Gori per la dedizione con cui ha portato e porta avanti il suo compito di Direttore Scientifico sia della CWC che di EUCACS. Sono poi grato agli altri componenti del Board: il Professor Colajanni e l'Amm. Sanfelice di Monteforte. Ma un ricordo particolarmente affettuoso va al Senatore Generale Luigi Ramponi, nostro entusiasta componente del Board della Conferenza e Primo Presidente, e tale rimarrà nel tempo, di EUCACS, che abbiamo costituito poche settimane prima della sua scomparsa. Invito ancora una volta, chi non lo avesse ancora fatto, a leggere la sua autobiografia[2], perché fa vedere lo spessore di un uomo dedito alla passione ed al servizio per il suo Paese che pochi hanno. Non dobbiamo dimenticare che è stato il vero padre del Piano Cibernetico Nazionale, forse senza la sua passionale esistenza non si sarebbe arrivati a procedere in

[*] Chairman CWC, Vicepresidente Esecutivo EUCACS, CEO & Founder InTheCyber Group.

[1] NATO Advanced Research Workshop (ARW) *Operational Network Intelligence: Today and Tomorrow*, 6-7 febbraio 2009, Arsenale di Venezia. Atti nel volume *Modelling Cyber Security: Approaches, Methodology, Strategies*, a cura del Prof. Umberto Gori per IOS Press, Nato Science for Peace and Security Series E: Human and Societal Dynamics – Vol. 59.

[2] L. Ramponi, *Val la pena di vivere*, Aracne Edizioni, Febbraio 2016.

tal senso. È proprio in sua memoria che, dopo l'*impasse* generato dalla sua repentina scomparsa, abbiamo voluto dare un nuovo impulso ad EUCACS, chiedendo al Prof. Michele Colajanni di assumerne la carica di Presidente. L'impegno primario sarà rivolto alla *cyber education*, necessità vitale per la Difesa del Paese, come più volte ripetuto nelle CWC ed in questi Volumi. È fondamentale un'ampia collaborazione tra persone, associazioni, aziende, università ed istituzioni perché si arrivi da una parte ad una awareness diffusa tra tutti i cittadini di quella che è la minaccia cyber e dall'altra, che si arrivi ad una conoscenza specifica, multidisciplinare per poter dare corpo a quelli che sono i cosiddetti "operatori cyber", a qualsiasi livello essi siano: a livello civile, a livello governativo o a livello militare. Abbiamo bisogno di persone che non siano puramente tecniche, che non siano puramente dei letterati, ma che abbiano la capacità di discernere realmente all'interno di questo sfaccettato mondo della minaccia cyber per la difesa del Paese.

La CWC svoltasi a Milano il 12 Dicembre 2018 ha affrontato un tema estremamente delicato "Dalla Difesa Passiva alla Risposta Attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche". Un tema anche molto ardito, perché se ne parla tra le righe, ma fino ad ora questa è la prima conferenza che lo ha affrontato in maniera aperta. È un tema sì estremamente sensibile, ma è un tema che diventa irrimandabile per la situazione contingente e che va in ogni caso affrontato, qualsiasi decisione poi si prenderà, e discusso a fondo per capirne tutte le possibili sfaccettature. La minaccia Cyber è sempre più presente ed incombente in tutte le varie sfaccettature più o meno sofisticate, ma che sicuramente impattano ormai sui conti economici delle aziende, sui loro valori patrimoniali e anche direttamente sui PIL dei Paesi. Si contano ancora facilmente i veri e propri attacchi cyber, quelli con conseguenze cinetiche, quindi quelli che si differenziano dagli attacchi puramente informatici o informativi. Ma siamo tutti consapevoli di quanto questa tipologia di attacchi sia possibile, sia tecnicamente fattibile e alla quale siamo ancora esposti. Le nostre infrastrutture, i nostri sistemi, sia a livello aziendale che a livello governativo, che a livello militare non sono ancora totalmente sicuri da questo punto di vista. Certi attacchi possono avere conseguenze anche drammatiche, anche superiori agli attentati di tipo tradizionale. Abbiamo quindi da questo punto di vista una estrema responsabilità nel portare in atto tutte le misure possibili e necessarie per alzare il livello di difesa, questo vale sia per le aziende che per le istituzioni, che per qualsiasi tipologia di entità. Non si tratta più di comprare qualche tecnologia di protezione informatica o di far realmente evolvere alla massima tecnologia disponibile la difesa cibernetica, ma di attivare dei veri e propri processi di presidio continuativo della Cyber Security Avanzata: tramite programmi continuativi di *assessment*, di

simulazioni di attacco, di vere e proprie esercitazioni che coinvolgono sia le tecnologie che gli uomini che sono preposti al loro controllo.

Urge sempre più l'attivazione e la costruzione di veri e propri Centri di Difesa Cyber in modalità PPP (public-private-partnership), non solo puramente a livello centrale, ma a livello regionale, a livello locale, a livello di filiera, in puntuale coordinamento con il livello centrale statuale. Solo così si potrà avere una reale percezione e discernimento su quello che può o sta avvenendo, di capire se più eventi contemporanei, distribuiti sul territorio sono casuali o sono un attacco sistemico. Solo in questo modo potremmo raggiungere un miglioramento continuativo, come continuamente migliora e diventa più sofisticata la minaccia. Ma anche qualora fossimo così bravi da attuare tutto questo, ad attivare efficacemente tutto questo, e dobbiamo farlo rapidamente e con l'approvazione di tutti, rimane questa questione finale: chi, come, dove, quando e se dobbiamo o possiamo agire per individuare, analizzare, depotenziare o neutralizzare la minaccia? Con questo dilemma si stanno confrontando tutti i Paesi. Alcuni hanno già preso posizione, altri hanno già messo in atto misure asimmetriche cinetiche in risposta ad attacchi Cyber. In tutto questo la difficoltà nel processo di attribuzione resta il punto centrale.

Questo è il compito arduo che è stato dato alla CWC2018. I diversi prestigiosi relatori ci hanno sicuramente aiutato in un primo importante approfondimento, che è, però, solo l'inizio di un percorso che è da affrontare a più livelli, ma sicuramente a livello del Sistema Paese nel suo complesso e dei suoi massimi vertici. La costruzione di una capacità Cyber Nazionale, frutto delle migliori risorse del Paese è doverosa e possibile. In finale ringrazio l'On. Ing. Angelo Tofalo, Sottosegretario alla Difesa, ed il Gen.B.A. Francesco Vestito, Comandante del Centro Interforze Operazioni Cibernetiche, che da anni partecipano attivamente ai lavori della CWC.

Riconoscimenti

Promotori

European Center for Advanced Cyber Security (EUCACS)
Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII)
Centro Studi Difesa e Sicurezza (Cestudis)
CIS Università La Sapienza
Istituto per gli Studi di Previsione (ISPRI)
European Center for Advanced Cyber Security (Eucacs)
Centro Studi Grande Milano

Ideato d'intesa con InTheCyber- Intelligence & Defense Advisors

Con la sponsorship di

CA Technologies
ORACLE

Con la collaborazione di

CLUSIT
CERSA

Prolusione

di *Angelo Tofalo*[*]

Partecipo per il quarto anno alla Cyber Warfare Conference, che reputo sempre una grande opportunità di scambio di informazioni sul tema cyber. A differenza delle precedenti occasioni, che mi hanno visto nella veste di deputato e di tecnico ed ingegnere, partecipo a questa 9° edizione nazionale nell'incarico di Sottosegretario di Stato alla Difesa e, in virtù di ciò, intendo offrire una panoramica di più ampio respiro su quello che io, e il governo in generale, stiamo portando avanti per affrontare nel modo migliore le nuove sfide del dominio cibernetico.

A livello globale un passo in avanti è stato compiuto al Summit della NATO 2016 di Varsavia (e che sia accaduto soltanto nel 2016, a mio parere, è da considerarsi tardivo), dove è stato riconosciuto ufficialmente il dominio cibernetico come il quinto dominio operativo in campo militare. La NATO quindi riconosce il dominio cibernetico, dopo quelli terrestre, marittimo, aereo e spaziale, come un "campo" militare a tutti gli effetti operativo. Conseguentemente a ciò gli Stati membri hanno messo in atto le proprie azioni. In Italia è stato costituito il CIOC, il Comando Interforze per le Operazioni Cibernetiche, la cui creazione era prevista nel Piano Nazionale per la Sicurezza Cibernetica del 2013 (all'epoca veniva denominato COCI, Centro Operativo Cibernetico Interforze).

Una riflessione più generale voglio farla evidenziando che, storicamente, l'uomo ha sempre cercato di definire quelli che sono stati e che sono tutt'oggi i modelli di società. Senza andare troppo indietro nel tempo abbiamo ad esempio sentito parlare di società del rischio (Beck) e di società liquida (Bauman). Sono questi temi di profonda attualità, ragion per cui in prima persona sto partecipando ad un tavolo, quello di Rousseau Academy, all'interno del

[*] Sottosegretario di Stato alla Difesa con delega Cyber.

quale – insieme a diversi esperti, professori e scienziati di livello internazionale, docenti del MIT, ricercatori che arrivano da tutte le parti del mondo e con il contributo anche di grandi aziende che operano con i Big Data – stiamo cercando di definire quella che sarà la società futura.

È evidente, infatti, che la società di domani sarà sempre più digitale. Questo comporta un approccio totalmente diverso, che ovviamente si ripercuote in ogni settore, anche in quello della Difesa.

La Difesa Nazionale è priorità per ogni Paese sovrano, è strategica perché si occupa di proteggere quelli che sono i confini, seppur tuttavia, quando ci muoviamo nello spazio cibernetico, è difficile anche solo parlare di linee di demarcazione.

Nella società digitale, le istituzioni, il mondo accademico, i docenti, le famiglie hanno difficoltà a stare al passo dei giovani e giovanissimi. È in atto una sorta di inseguimento generazionale, ed è talmente veloce che può esser paragonato a un'onda che cresce sempre di più e noi dobbiamo evitare di farci travolgere.

Come classe dirigente, come istituzione e come persone che sentono forte questa responsabilità, ritengo dobbiamo governare questi cambiamenti piuttosto che subirli.

Purtroppo anche in Italia più di una volta si sono verificati episodi che hanno causato disagio e sofferenza fino a spingere giovanissimi a commettere gesti estremi.

In altre parole il dominio cibernetico ha ripercussioni concrete nella nostra società a livello globale.

Per quanto riguarda lo scenario europeo l'UE ha approvato la NIS 2018, che invita i Paesi membri a uno sforzo maggiore per aumentare il livello di sicurezza. Non sarà semplice concretizzarne i contenuti, ma deve essere impegno prioritario.

Questo mio contributo coincide esattamente con i primi sei mesi dalla mia nomina a Sottosegretario. Fin da subito ho voluto mettere le mani all'interno del Ministero della Difesa che, devo dire, è notevolmente avanti rispetto a tutta la Pubblica Amministrazione italiana nel settore cibernetico.

In relazione a quello che ho riscontrato finora, l'indicazione politica che sto dando è quella di cercare di far parlare un'unica lingua cibernetica al Ministero della Difesa: mi riferisco alle varie Forze armate, l'Esercito, l'Aeronautica, la Marina, l'Arma dei Carabinieri, all'interno delle quali spesso ciascuno tende ad utilizzare, ad esempio, una piattaforma o un software diverso, per le stesse funzioni e gli stessi servizi.

Nell'ambito del Ministero della Difesa, dove per la prima volta è stata assegnata una delega specifica alla sicurezza cibernetica proprio per evidenziare la sensibilità del governo sulla materia, lo sforzo è volto a ottimizzare l'organizzazione, creando una maggiore interoperabilità fra i vari dispositivi e sistemi utilizzati dalle diverse Forze Armate.

È un percorso che stiamo portando avanti interagendo con gli altri Dicasteri. L'attuale quadro normativo italiano conferisce alla Presidenza del Consiglio e al Dipartimento dell'Informazione per la Sicurezza, al DIS, il compito di fare da regia per quanto riguarda la sicurezza cibernetica di tutto il Sistema Paese. Il cuore di tutto è l'NSC (Nucleo di Sicurezza Cibernetica), il tavolo dove siedono tutti i Ministeri, il DIS e le Agenzie.

La nostra architettura consente di gestire ogni genere di minaccia, stiamo lavorando per fare sempre meglio ed essere più sicuri.

Ogni giorno sempre più persone sono connesse alla rete, siamo sull'ordine di 4-5 miliardi e ci sono sempre più oggetti interconnessi.

Ricollegando tutto ciò alle nuove tecnologie, come la blockchain, come l'intelligenza artificiale, all'Internet of Things, l'Internet del tutto, spesso mi chiedo: se da qui a qualche anno un "alieno" dovesse guardare il pianeta Terra e decidesse di comunicare con noi, proverebbe a contattare i 7 miliardi di umani o i 100, 200, 300 miliardi di oggetti collegati alla rete e comunicanti tra di loro?

Nei più grandi laboratori del mondo si immaginano già da diversi anni sensori di ogni genere; si parla ad esempio di albero intelligente che comunica i dati ricevuti dall'ambiente e dall'aria, quindi foreste e fiumi intelligenti, così se pensiamo all'intelligenza artificiale, ci rendiamo conto che andiamo verso un mondo che sarà dominato dagli algoritmi. Ma questi algoritmi chi li scrive?

Un mio professore portava sempre l'esempio dell'auto intelligente: all'improvviso si presenta per l'auto un problema di security, di fronte a un ostacolo quale decisione verrà presa? Ci sarà un codice, un algoritmo che deciderà da che parte andare, magari calcolando il danno minore. Questo è il mondo che sta arrivando ad alta velocità.

Personalmente sento forte la responsabilità di provare a governare questo cambiamento e non subirlo. In Italia, e qui introduco una riflessione politica, abbiamo risorse fuori dal comune: spesso abbiamo meno risorse finanziarie degli altri, ma proprio per questo ci ingegniamo il doppio riuscendo a trovare soluzioni migliori di chi dispone dei capitali.

Tuttavia questa è una partita che da soli non si può giocare: bisogna fare squadra quanto meno in Europa e non solo.

In questa partita sicuramente l'industria della Difesa può essere uno strumento per rendere più forte il vecchio continente e permetterci di avere una voce in capitolo, per quanto piccola, in materia cibernetica, che rappresenta la grande sfida di oggi e di domani.

Nuovi approcci alla sicurezza cibernetica: la diplomazia preventiva come strumento di difesa attiva

di *Umberto Gori*[*]

Sono solo due i modi per contrastare un attacco, cinetico o cibernetico che sia: difesa od offesa, diplomazia o forza militare.

L'epoca storica in cui viviamo vede una sempre maggiore attività conflittuale nell'unico spazio creato dall'uomo, attività che aumenta pressoché esponenzialmente in quantità e qualità.

L'esperienza ci insegna che chi attacca è sempre un passo avanti rispetto a chi cerca di difendersi a causa delle caratteristiche dello spazio cibernetico, le quali consentono operazioni aggressive senza preavviso, ad impatto immediato, di difficile attribuzione e a basso costo.

Tutti gli Stati, nessuno escluso – secondo un rapporto sui trend nella sicurezza informatica nel 2019 della società FireEye – si stanno attrezzando per causare danni cibernetici. In testa alla classifica, oltre agli USA, troviamo Cina, Iran, Corea del Nord e Russia[1].

Dobbiamo quindi chiederci se le difese puramente reattive fin qui privilegiate non debbano essere sostituite da azioni proattive, da azioni, cioè, che presuppongano attività d'intelligence, di previsione e di modellizzazione dei vari tipi di attacco al fine di precostituire risposte che rendano più difficili e più costose le attività di aggressione.

È necessario, inoltre, indagare su quanto praticabili e lecite siano eventuali forme di deterrenza. Il nuovo dominio conflittuale non è infatti, ad oggi, come accade invece nei quattro domini naturali, oggetto di regolamentazione giuridica o consensuale. Le divergenti concezioni del mondo risultano a questo proposito ostative, così come le differenti interpretazioni di concetti base e i contrastanti interessi delle potenze maggiori.

---

[*] Emerito Università di Firenze, Presidente CSSII e Direttore ISPRI

[1] Cfr. ISPI, *Confronting an 'Axis of Cyber'? China, Iran North Korea, Russia* (F. Rugge Ed.), Introduction by Massolo G., Milano, 2018.

In questa breve introduzione si cercherà di delineare un'idea di risposta a queste domande.

La prima necessità è di formulare una definizione non equivoca di alcuni concetti-base come: "difesa attiva", "hacking back" e "diplomazia preventiva".

La difesa attiva (*active defense*) si contrappone innanzitutto alla "difesa reattiva". È, infatti, l'impiego di attività limitatamente offensive e di contro-attacchi per impedire all'avversario di raggiungere i suoi obbiettivi. Questa definizione non specifica se si riferisca ad attività cinetiche o cibernetiche.

La definizione che la NATO propone di *active defense* è la seguente: «a pro-active measure for detecting or obtaining information as to a cyberintrusion, cyberattack, or impending cyber operation for determining the origin of an operation that involves launching a pre-emptive, preventive, or cyber counter-operation against the source».

In area cyber la difesa attiva può significare "difese asimmetriche", ossia difese che aumentano il costo agli attaccanti, riducendo quello dei difensori.

Un esempio di ciò è la tecnologia Moving Target Defense (MTD), utilizzata da Cripto Move per spezzettare di continuo, replicare, ri-criptare, comprimere e mutare codici e parole chiave al fine di creare una protezione ridondante e sicura, per poi assemblare nuovamente tutto su propria autorizzazione. In futuro l'unico problema potrebbe essere dato dai computer quantistici, nonostante, comunque, già circolino idee su come neutralizzarli.

Un ulteriore esempio è costituito dalle tecnologie di cyber deception, denominate anche 'honeypot', come 'Illusive Networks', 'TrapX', 'Cymmetria', 'Attivo', etc., oppure strategie tipo 'Moving Target Defense', già illustrate dal sottoscritto in una precedente Conferenza.

Una forma più radicale di difesa attiva è quella definita "*pre-emptive*", ovvero anticipatoria di un attacco nel caso in cui questo sia ritenuto certo ed immediato. Nella lingua italiana non esiste un concetto equivalente, la traduzione di *pre-emptive* con 'preventivo' distorce il senso del primo. In inglese, invece, si differenzia fra 'preventive' e 'pre-emptive': un'azione preventiva si risolve in un attacco vero e proprio, e cioè in un'azione offensiva; un'azione pre-emptive, invece, è un attacco difensivo, necessitato dalla consapevolezza di una imminente aggressione avversaria.

Gli Stati Uniti d'America, ad esempio, con la Presidential Policy Directive del 20 ottobre 2012, rivelata da Snowden, prevedono non solo attacchi *pre-emptive*, in previsione di imminenti attacchi avversari, ma anche operazioni offensive a difesa di interessi nazionali non specificati[2].

[2] Martin Libicki, uno dei maggiori studiosi della materia, dubita che la deterrenza possa funzionare in ambito cyber, anche nell'ipotesi di un'attribuzione certa. La deterrenza, infatti,

Nello stesso tempo, però, il DoD riteneva importante utilizzare lo strumento diplomatico per arrivare ad un accordo sulle regole di comportamento in ambito cyber. È grande, infatti, la preoccupazione che nel processo di militarizzazione del ciberspazio prevalga la strategia offensiva.

Sul punto sono arrivate per prime la Russia e la Cina che, insieme a Tagikistan e Uzbekistan, hanno presentato una proposta all'Assemblea Generale delle Nazioni Unite, nel settembre 2011, intitolata International Code of Conduct for Information Security, da considerare politicamente impegnativa e non giuridicamente vincolante al fine di rendere più agevole un assenso americano.

Il contenuto, tuttavia, era ambiguo a causa dell'assenza di definizioni concordate sui concetti base. La Cina ha proposto alcuni princìpi, fra i quali l'uso di "*active preventive diplomacy*" e la "sovranità cibernetica", come naturale estensione della sovranità dello Stato sul ciberspazio.

Nella storia delle relazioni internazionali una situazione di anomia come quella esistente nel quinto dominio, non si era mai verificata.

È, dunque, impellente la necessità che l'Occidente reagisca e cerchi di pervenire ad un idem sentire, anche se il cammino non sarà semplice. L'assenza di norme di condotta può portare al disastro.

Le ciberdifese proattive comprendono azioni riconducibili a forme di Information Warfare Operations. Le operazioni cibernetiche offensive di norma necessitano di autorizzazioni e sono riservate ai vertici politici degli Stati.

È un esempio di ciò il cosiddetto *hacking back*: il processo di individuazione degli attacchi e, possibilmente, identificandone l'origine, per operare essenzialmente in modalità pre-emptive. Solo quando le tecnologie per l'attribuzione delle responsabilità saranno più avanzate l'*hacking back* potrà diventare un normale strumento di difesa. Ad oggi l'hacking back può causare solo danni collaterali.

La difesa attiva, del resto, è spesso confusa proprio con l'hacking back, nonostante vi siano importanti differenze quanto ad etica, legalità ed efficacia.

La difesa attiva non è di per sé offensiva, né necessariamente pericolosa. Non nuoce a terzi, è legale ed è efficace. Al contrario, l'hacking back è aggressivo, illegale e non sempre efficace.

Un esempio che traggo dall'«Harvard Business Review» del 21 maggio 2018 (Scott Berinato) può ulteriormente chiarire la principale differenza fra

---

«è nella mente del nemico». Libcki M., *Would Deterrence in Cyberspace Work even with Attribution?*, «Georgetown Journal of International Affairs», April 2015.