Cyber Warfare 2019-2020

Dall'evoluzione della Warfare alla resilienza al Covid-19

a cura di Umberto Gori, Daria Vernon De Mars

FrancoAngeli

FrancoAngeli
Edizioni La passione per le conoscenze

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con **Adobe Acrobat Reader**

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 2019-2020

Dall'evoluzione della Warfare alla resilienza al Covid-19

a cura di Umberto Gori,
Daria Vernon De Mars

FrancoAngeli

L'evento, articolato nell'anno 2019 in due edizioni, ha avuto luogo a Roma il 9 luglio 2019, presso la Nuova Aula del Palazzo dei Gruppo Parlamentari – Camera dei Deputati, e a Milano il 12 dicembre 2019, nella Sala della Vittoria Antica presso l'Aeronautica Militare – Comando 1ª Regione Aerea. Nell'anno 2020 l'evento si è tenuto in un'unica edizione interamente online, con seminari settimanali susseguitesi dal 12 maggio 2020 fino al 30 giugno 2020.
La conferenza è stata promossa dal Centro universitario di Studi Strategici, Internazionali e Imprenditoriali (CSSII), Centro Studi Difesa e Sicurezza (CESTUDIS), Istituto per gli Studi di Previsione (ISPRI), European Center for Advanced Cyber Security (EUCACS), Cyber Academy, Associazione Italiana Professionisti Sicurezza Informatica (AIPSI), Associazione Italiana Professionisti Security Aziendale (AIPSA) d'intesa con InTheCyber Group.

Indice

Edizione di Milano
12 dicembre 2019

Edizione 2020
Maggio - Giugno
La Resilienza Nazionale di fronte al Covid-19
Dicembre
Covid e Cyber Security: dalla reazione all'emergenza pandemica al cambiamento strutturale

Prefazione

di *Paolo Lezzi*[*]

Questo volume ricomprende gli atti delle edizioni 2019 e 2020 della Conferenza Nazionale sulla Cyber Warfare. Le prime a Roma il 9 luglio 2019, presso la Sala Gruppi della Camera dei Deputati, e a Milano il 12 dicembre 2019, presso la Sala della Vittoria Atlantica dell'Aeronautica Italiana a Milano, hanno avuto entrambe per tema "Evoluzione e Nuove Frontiere della Warfare (Information, Cyber e Hybrid) – Una Storia di Dieci Anni".

L'edizione 2020 si è svolta totalmente online, uscendo straordinariamente dal tema cyber stretto, sollecitata dalla situazione contingente, e si compone di una iniziale Web Conference del 12 maggio 2020 dal tema "La Resilienza Nazionale di fronte al Covid-19", cui seguono 6 WebRoundTable settimanali sino al 30 giugno 2020 sulla "Ripartenza Nazionale" affrontata da diversi aspetti.

Nel momento di andare in stampa ci ritroviamo nel pieno della seconda ondata del Coronavirus che sta nuovamente mettendo a dura prova le istituzioni e le popolazioni di tutto il mondo, non solo sotto il profilo sanitario, ma anche della tenuta sociale ed economica. In tali frangenti, forze ostili possono approfittare per mettere a punto le loro strategie malevoli sfruttando tutti i mezzi. È pertanto di fondamentale importanza non abbassare la guardia rispetto alla sicurezza nazionale.

Confidiamo che lo sforzo comune e la stretta collaborazione pubblico-privato tra tutte le risorse del Paese permetta di superare anche questa prova.

Un particolare ringraziamento e tributo sono rivolti al professor Umberto Gori che da oltre dieci anni cura con estrema premura, non solo la direzione scientifica della Conferenza, ma soprattutto permette di lasciare traccia del nostro lavoro con la redazione degli Atti della Conferenza stessa.

[*] Vicepresidente Esecutivo EUCACS, CEO InTheCyber Group.

Riconoscimenti

Promotori

European Center for Advanced Cyber Security (EUCACS)
Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università di Firenze (CSSII)
Centro Studi Difesa e Sicurezza (Cestudis)
Istituto per gli Studi di Previsione (ISPRI)
European Center for Advanced Cyber Security (Eucacs)
Cyber Academy
Associazione Italiana Professionisti Sicurezza Informatica (AIPSI)
Associazione Italiana Professionisti Security Aziendale (AIPSA)

Ideato d'intesa con InTheCyber Group

Con la sponsorship di

Akamai
Cisco
Cybereason
Radware
RSA
SonicWall
TIM
Google

Con il patrocinio di

Ministero della Difesa

Con la collaborazione di

CLUSIT
CERSA

Edizione 2019

Evoluzione e nuove frontiere della Warfare (Information, Cyber e Hybrid)

Una storia di dieci anni

Prolusione

di *Paolo Lezzi*[*]

È sempre, forse sono ripetitivo, per me una grande emozione ogni anno dichiarare aperta la Conferenza Nazionale sulla Cyber Warfare. Sono passati dieci anni ed è un tempo importante, vuol dire che questa iniziativa vive, è maturata, quindi l'intuizione iniziale non era solamente una chimera.

Dodici anni fa, come molti sanno, ho conosciuto il professor Gori e da lì è nata l'idea di fare, poco dopo, su sua provocazione, un Advanced Research Workshop della NATO all'Arsenale di Venezia. Quello può essere definito il primordio di quella che poi è diventata la Conferenza. A tale evento hanno partecipato una settantina di ufficiali di almeno 20 paesi della NATO, abbiamo discusso, 11 anni fa, di come rispondere alla minaccia Cyber a livello militare. Non si parlava ancora di quinto dominio, non si parlava ancora di risposta attiva, però già si poneva una domanda che a quei livelli era già un oggetto di discussione.

All'esterno sembrava fantascienza, così poi è cominciato il giro delle conferenze. Devo ammettere che solo le nostre forze armate, nella fase iniziale, avevano già compreso quanto fosse critica e importante questa tematica e quanto questo potesse essere di incidenza sulla sicurezza nazionale, al punto da essere poi riconosciuto come quinto dominio o quinto *battlefield*.

Abbiamo sempre cercato, ogni anno, di vedere in anticipo, di cogliere sul nascere aspetti non ancora affrontati e posti in discussione a livello nazionale. Abbiamo voluto, in questi anni, essere di pungolo e di stimolo nei confronti delle istituzioni, nei confronti di tutta l'arena della società italiana, dalle Forze Armate all'intelligence, alle imprese, alle accademie, con il coinvolgimento di tutti. Abbiamo cercato di toccare tutti gli aspetti del domino cyber, con le sue conseguenze psicologiche, sociali, cinetiche, con l'aiuto di relatori, devo dire, sempre di altissimo livello ed ai quali va permanentemente il mio ringraziamento. Un particolare ringraziamento per il lavoro assiduo ed appassionato è rivolto al professor Gori, che in questi dieci anni si è dato senza limiti e senza sosta a questa iniziativa e senza il quale, come è

[*] Vicepresidente Esecutivo EUCACS, CEO InTheCyber Group.

noto, non saremmo arrivati a questo traguardo. Il nostro Paese ha sicuramente fatto dei passi significativi nei confronti della minaccia cyber. È di alcuni anni orsono il primo Piano Cibernetico Nazionale, fortemente voluto dal nostro caro e compianto Generale Ramponi, il quale, come sapete, è sempre stato un appassionato componente del nostro comitato scientifico e che è stato tra i fondatori di EUCACS. Sono stati fatti tanti passi da quel momento in poi a livello istituzionale, sono stati creati organismi, messe a punto infrastrutture, per poter essere sempre più preparati rispetto alla minaccia cyber. Tuttavia, tanto, tantissimo è ancora da fare e non può essere fatto solo a livello puramente istituzionale. Questo è il principale motivo per cui è stato fondato EUCACS: per stimolare, valorizzare, la nascita di iniziative e partnership pubblico-privato. Questo è un aspetto fondamentale per lo sviluppo del Paese in tutti gli aspetti, ma in particolare in un aspetto come il dominio cyber. L'Italia ha un potenziale enorme di risorse, di iniziativa privata che è incomparabile, di capacità creativa, riconosciuta in tutto il mondo. Su questo dobbiamo cambiare paradigma, nel senso che se non c'è un reale sostegno a queste iniziative, a questa capacità, questa si disperde. In Italia spesso la creatività non viene valorizzata, mentre vediamo che appena un italiano fugge all'estero immediatamente emerge. Perché? Perché è presente dentro un'anima che è inalienabile, ma bisogna tornare a valorizzarla tutti assieme. L'Italia deve essere una potenza cyber sotto tutti i profili, può e deve diventare ciò. Non ha la possibilità di essere mega potenza su diversi aspetti, ma sul cyber, c'è tutto lo spazio, per raggiungere l'obiettivo. Gli investimenti sono relativi per poterlo fare, ma devono essere intrapresi tutta una serie di passi propedeutici importanti.

Provo ad esprimere di seguito cinque punti, che poi verranno ripresi, sicuramente in maniera più approfondita, dalle relazioni che seguono:

1. La consapevolezza globale: ovvero è necessario un piano di *cyber education* a tutti i livelli, questo lo sottolineiamo sempre, ma diventa sempre più urgente. Anche qui sono stati fatti dei passi avanti, sono nati tanti corsi specifici, le aziende cominciano a muoversi, ma questo deve andare avanti ancora di più. Sicuramente la Cyber Academy del professor Colajanni è un esempio di come i giovani possano essere valorizzati su questi aspetti. Abbiamo pensato prossimamente, oltre alla Conferenza, di fare dei workshop ristretti, molto ristretti, in Chatham House, così che si possa interloquire liberamente di che cosa vuol dire affrontare la minaccia, con tecnici, non tecnici, amministratori a tutti i livelli, provocando su determinati scenari, per far proprio crescere o nascere una naturalezza nell'affronto preventivo e difensivo di situazioni ed eventi sempre più frequenti e sempre più gravi.
2. La messa a punto di una cyber difesa reale ed efficace di tutte le infrastrutture pubbliche e private, elemento che ancora non si è concretizzato. Significa realizzare un circolo virtuoso di "*test&enhance*" per andare a

rinforzare sempre di più il livello di protezione. Attualmente le nostre imprese, come le nostre istituzioni, sono al 99% vulnerabili, al 90% passibili di attacchi sofisticati da parte di cybercrime avanzato, di spionaggio, di terrorismo, attacchi semi-statuali e financo statuali.

3. La capacità di individuazione e neutralizzazione degli attacchi ovvero quello che il NIST definisce come "*detection & response*". Tale capacità è ancora relativamente bassa, inizia ad essere presente nelle grandi realtà ma è totalmente mancante in tutto il resto del Paese. Dobbiamo costituire, lo predico ormai da diversi anni, dei centri di difesa cyber territoriali, con il preciso scopo di rilevare, neutralizzare sul nascere possibili attacchi. Non possono e non devono essere puramente istituzionali. Tali centri possono essere costituiti abbastanza rapidamente se pensati coinvolgendo e valorizzando le miglior risorse già presenti sul territorio a livello d'impresa, accademie ed apparati dello Stato. Non possiamo andare, e lo sottolineo perché già avvengono fenomeni di questo tipo, a sottrare ai team di quelle poche realtà veramente preparate sulla difesa cyber, personale formato negli anni sul campo, per metterlo in centri istituzionali, perché questo distrugge e depaupera una storia. Valutiamo attentamente la validità e la competenza di un team nonché la sua affidabilità istituzionale e coinvolgiamo, al fine di inserirlo in un meritevole, serio progetto cyber nazionale, diffuso sul territorio ma attentamente coordinato da un centro di difesa cyber nazionale. Tale centro nazionale dovrà anche coordinare le attività sul campo ai fini dell'attribuzione dell'origine di un attacco, e se del caso in coordinamento con le F.F.A.A. valutare, quando il Paese deciderà di avere una capacità offensiva tattica, se è opportuno arrivare a neutralizzare la fonte originante l'attacco stesso. Solo così possiamo renderci conto se un certo numero di realtà è attaccato in contemporanea e poter verificare se si tratta o meno di un attacco sistemico al Paese in tempo zero.

La Sicurezza Nazionale non può essere un problema esclusivo delle istituzioni preposte a occuparsene, ma deve essere una sensibilità diffusa nella popolazione, a maggior ragione nelle imprese. Quando un individuo si trova a casa o in azienda, se il suo PC è coinvolto, se lui è coinvolto, se qualcosa che lui porta addosso è coinvolto, può essere un problema non solo per il soggetto, ma per i suoi familiari, per la sua impresa. Se un'impresa è attaccata, non è un problema dell'impresa, è un problema di tutto il paese, perché se più imprese, lo ripeto sino alla noia, sono attaccate in contemporanea potrebbe essere oggettivamente un problema di sicurezza nazionale.

4. Il laboratorio deve validare/certificare le tecnologie acquisite per la pubblica amministrazione, previsto dal relativo decreto. Auspico anche su questo aspetto che sia realizzato coinvolgendo attraverso un processo di selezione simile a quello del punto precedente: le migliori capacità di *cyber testing* presenti in imprese private ed accademiche, realizzando in pochissimo tempo una potenza di fuoco inimmaginabile.

5. I sistemi di difesa adottati, tecnologie e uomini, devono essere continuamente esercitati, messi alla prova, perché altrimenti non conosciamo la capacità di reazione all'attacco, questo le nostre forze armate lo sanno bene. Quindi vanno messi alla prova, mezzi, tecnologie, processi e uomini, non esiste l'acquisto di tecnologia che salvi l'azienda o l'istituzione senza uomini totalmente capaci di gestirlo, non solo a livello militare, ma anche a livello dell'infrastruttura economica del paese. Sono quindi necessari dei veri e propri piani di esercitazioni cyber a tutti i livelli della società e della popolazione.

La NATO, come altre realtà, ha già sancito da alcuni anni il diritto alla risposta asimmetrica convenzionale rispetto ad un attacco cyber ma sino al 2019 non è giunta alcuna notizia ufficiale del suo impiego. Israele, essendo stata attaccata dal punto di vista cibernetico presso il suo MoD, dopo pochi minuti ha raso al suolo la palazzina da cui si originava l'attacco. Viceversa, gli USA hanno messo fuori uso via cyber il sistema missilistico iraniano che aveva attaccato alcune petroliere. Da questo momento ci posiamo aspettare che asimmetrie di questo tipo od in generale ibridità nelle tattiche militari diventino la prassi.

La Difesa italiana nel piano di ammodernamento continuo delle sue F.F.A.A. deve rapidamente affiancare alla sue già elevate capacità convenzionali e di guerra elettronica, capacità tattica cyber a tutti i livelli per concorre concretamente alla protezione del Paese ed al suo ruolo all'interno della NATO e dei diversi scenari di missione internazionale.

La CWC 2019 vuole comprendere, o meglio ri-comprendere, l'evoluzione di questi dieci anni, i cambiamenti della warfare nel suo complesso: non possiamo limitarci a parlare di information warfare o cyber warfare. parliamo ormai come detto di hybrid warfare.

Siamo accompagnati in questo percorso, nelle due edizioni di Roma e Milano, da relatori di tutto rispetto che ringrazio sinceramente per il loro contributo.

Nell'edizione milanese abbiamo poi introdotto due tavole rotonde, condotte dal professor Colajanni, per avere meglio il polso su come le imprese hanno vissuto questa evoluzione anche a partire dai risultati del Barometro Cyber Security 4.0 (iniziativa di EUCAS, NetConsulting3 ed InTheCyber Group) che fa il punto dello stato del maturity model della principali aziende pubbliche e private italiane dei diversi settori rispetto ai pilastri del NIST ed al GDPR.

Ringrazio tutti quelli che hanno contribuito alla realizzazione di questa iniziativa, in primis il Direttore Scientifico, il professor Gori ed il Presidente di EUCACS il professor Colajanni, perché con me hanno condiviso la partenza anche della CWC2019, ed il nostro staff che ha lavorato alacremente dietro le quinte e davanti alle quinte, gli sponsor e gli enti organizzatori e promotori tutti.

Un ringraziamento speciale va all'Areonautica Militare per averci voluto ospitare il 12 dicembre nella storica sede di Piazza Novelli a Milano, nelle persone del Generale Frigerio, Comandante della Prima Regione Aerea e del Comandante Vestito, già Comandante del CIOC ora Comandante delle Forze di Combattimento Aereo.