Information Warfare 2011

La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale

a cura di Umberto Gori
e Luigi Sergio Germani

FrancoAngeli

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.

Information Warfare 2011

La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale

a cura di Umberto Gori
e Luigi Sergio Germani

FrancoAngeli

La Conferenza è stata ideata dal Centro universitario di Studi Strategici e Internazionali dell'Università degli Studi di Firenze, dalla Link Campus University, dal Centro Studi "Gino Germani", dall'Istituto di Studi di Previsione (ISPRI), d'intesa con Maglan Europe, realtà leader internazionale nell'auditing e consulting per la difesa delle informazioni in ambito civile, militare e governativo

Un ringraziamento va alla dottoressa Serena Lisi per l'editing del volume

Indice

Prefazione

di *Vincenzo Scotti*[*]

Sono particolarmente lieto di introdurre gli atti di questa Conferenza dal titolo "La Sfida della Cyber Intelligence al Sistema Italia", promossa da CSSI, ISPRI, Link Campus University, Centro Studi "Gino Germani"; si tratta del secondo appuntamento dell'importante lavoro avviato – tra gli altri - dal Prof. Umberto Gori e dal Prof. Sergio Germani, ai quali sono molto grato.

Link Campus University, su questi temi, è impegnata da molti anni, sia a livello formativo (siamo giunti alla settima edizione del Master in Intelligence e Security) che sul piano della riflessione pubblica, con il coinvolgimento costante dei massimi livelli istituzionali ed accademici.

Link Campus University, su questi temi, è impegnata da molti anni, sia a livello formativo (siamo giunti alla settima edizione del Master in Intelligence e Security) che sul piano della riflessione pubblica, con il coinvolgimento costante dei massimi livelli istituzionali ed accademici.

Il tema di fondo di questa seconda Conferenza è, da un lato, capire quali sono le minacce e le opportunità per la sicurezza nazionale e per la sicurezza delle imprese derivanti dalla cyber intelligence e, dall'altro lato, come potenziare le capacità di cyber intelligence e network intelligence del sistema Italia.

Nel corso della conferenza si è discusso della sfida della cyber intelligence sotto diversi profili della sicurezza nazionale: la sicurezza militare, la sicurezza interna dello Stato, la stabilità e coesione sociale e politica, la sicurezza e competitività del sistema economico e delle imprese.

[*] Sottosegretario di Stato, Ministero degli Affari Esteri e Presidente della Link Campus University

Vorrei soffermarmi brevemente su quest'ultimo punto, in particolare sul concetto di sicurezza economica nazionale e sulla crescente importanza dell'intelligence economica.
Perché la tematica è molto rilevante per il dibattito attuale sulla crisi italiana?

La tematica della conferenza è particolarmente rilevante nella fase critica che attualmente attraversa il nostro Paese. La crisi del debito sovrano, infatti, rischia di avere ripercussioni negative sulla sicurezza e la stabilità del sistema Paese. La chiave per poter gestire e superare la crisi del debito è la crescita, l'innovazione, la modernizzazione dell'apparato produttivo. Questo concetto viene sottolineato costantemente nel dibattito sulla crisi.
In una economia globalizzata, in cui la conoscenza è il principale motore di crescita, le informazioni rivestono una valenza strategica, e la capacità di acquisirle, analizzarle e proteggerle è cruciale per la sopravvivenza e per la crescita dei sistemi-Paese e delle imprese.

Pertanto, una strategia tesa a rilanciare la crescita e la modernizzazione dell'economia italiana non può prescindere da due componenti: (1) una politica di tutela della sicurezza del sistema economico, delle imprese e degli Istituti di ricerca scientifica nei confronti di attività di spionaggio avversario, che vengono effettuate con il ricorso sempre più frequente a strumenti di aggressione cibernetica; (2) una politica tesa a potenziare l'intelligence economica come strumento di tutela della sicurezza economica nazionale e di sostegno alla crescita e alla competitività del sistema Paese.

L'intelligence economica a sostegno della crescita e della competitività del sistema Paese

L'intelligence economica è stata definita come "la raccolta e l'analisi di informazioni utili per le decisioni di governo riguardanti le strategie di sostegno del sistema Paese nella competizione sui mercati internazionali".
Essa comprende diverse tipologie di attività, tra cui: la protezione del patrimonio scientifico, tecnologico e industriale del Paese mediante il contrasto allo spionaggio avversario; il monitoraggio globale dello sviluppo dell'alta tecnologia e della ricerca scientifica (ad esempio, in settori quali informatica, biotecnologie, nanotecnologie, energia alternativa, chimica, neuroscienze); l'acquisizione di informazioni preventive a sostegno della competitività delle imprese italiane nelle diverse regioni geopolitiche.

Oggi la OSINT – l'intelligence delle Fonti Aperte – rappresenta uno strumento di crescente importanza sia per l'intelligence economica istitu-

zionale sia per la business intelligence. Ciò soprattutto grazie alla disponibilità sul web di una vasta gamma di fonti informative "aperte" e alla disponibilità di nuovi strumenti tecnologici per la raccolta e l'analisi di notizie OSINT.

Per concludere, una politica nazionale finalizzata al potenziamento dell'intelligence economica dovrebbe promuoverne lo sviluppo sia in ambito istituzionale sia nel mondo dell'impresa. Una tale politica dovrebbe parallelamente sostenere, nel settore privato, la diffusione di una più robusta cultura della cyber sicurezza e di specifiche politiche aziendali di protezione delle informazioni nei confronti dello spionaggio economico- industriale.

Lascio ora alla lettura degli importanti contributi che si sono succeduti durante la Conferenza, un appuntamento rivelatosi decisivo in relazione sia alla qualità dei partecipanti che al valore dei contenuti e che, soprattutto, per prospettive e per strategie tracciate.

Riconoscimenti

Medaglia di Rappresentanza del Presidente della Repubblica

Patrocini

Senato della Repubblica
Camera dei Deputati
Presidenza del Consiglio dei Ministri
Ministero degli Affari Esteri
Ministero della Difesa
Ministero dell'Interno
Ministero dello Sviluppo Economico
Ministro per la Pubblica Amministrazione e l'Innovazione
Polizia di Stato

Promotori

Link Campus University
Centro universitario di Studi Strategici e Internazionali (CSSI)
Centro Studi "Gino Germani"
Istituto per gli Studi di Previsione e le Ricerche Internazionali (ISPRI)

Ideata d'intesa con Maglan - Information Defense & Intelligence

con il contributo di IBM

con la sponsorship di Finmeccanica

Medaglia di Rappresentanza, con firma del Presidente della Repubblica Giorgio Napolitano, inviata al Prof. Umberto Gori, direttore scientifico della Conferenza, in segno di apprezzamento per *l'iniz*iativa

Riflessioni propedeutiche alla cyber intelligence

di *Umberto Gori*[*]

È stato Buckminster Fuller, noto scienziato e filosofo statunitense che, nel 1938, coniò il termine di efemeralizzazione con il quale intendeva riferirsi all'uso delle risorse tecnologiche per ottenere il miglior risultato con il minimo sforzo, per «fare sempre di più con sempre meno peso, tempo ed energia per ogni dato livello di prestazione funzionale». Secondo Fuller, tale concetto rappresenta una costante nella storia dello sviluppo umano. In altre parole, in natura tutti i progressi vanno dal materiale all'astratto. Fuller riteneva, già allora, che anche i problemi sociali potessero essere risolti con l'adattamento alle nuove tecnologie.

Nel bene e nel male, oggi, il maggior contributo alla trasformazione delle operazioni militari, industriali, commerciali e finanziarie - per non citarne che alcune - viene dall'utilizzo sempre più intenso di tecnologie digitali.

Anche la cyber intelligence (CybInt), cui è specificatamente dedicata questa seconda Conferenza nazionale sulla information warfare, è un esempio lampante di come si sia trasformato, secondo le intuizioni di Fuller, "il secondo più antico mestiere del mondo".

Con il processo di efemeralizzazione, in una parola, si può ottenere sempre di più con un uso sempre più limitato di risorse. È l'effetto crisalide, l'ascesa al livello superiore. Per riferirsi solo alle tecnologie militari, l'innovazione è funzionale a vincere le guerre prossime venture, ma anche ad evitarle perché - come insegna Sun Tzu - il sommo dell'abilità è sottomettere l'avversario senza combattere, rectius senza distruggerlo.

L'innovazione si basa sulla compressione di fattori fisici (spazio, tempo, materia ed energia) e sulla contestuale espansione dell'informazione. Pro-

[*] Professore Emerito, Università di Firenze, Presidente del CSSI, Direttore dell'ISPRI, Direttore Scientifico della Conferenza.

prio quello che succede nel caso della information warfare e delle operazioni net-centriche.

Per fare innovazione occorre immaginare, e saper costruire, scenari diversi dalla situazione presente. Solo a questa condizione le tecnologie saranno in grado di risolvere problemi, ottimizzare processi e risorse di ogni genere.

Ma, come sempre è accaduto e come sempre accadrà nella storia dello sviluppo di nuove tecnologie, queste ultime possono essere foriere di benefici progressi e, contemporaneamente, di grandi preoccupazioni.

La cyber intelligence non fa eccezione.

E allora domandiamoci, senza pretesa di essere esaustivi: come utilizzare l'intelligence nello spazio virtuale, questa quinta dimensione della conflittualità? I metodi, le norme e le regole operative tradizionali sono applicabili a tale spazio, o si deve procedere a modifiche? Come si conducono le operazioni tipiche dell'intelligence nel cyber spazio? Ad esso sono applicabili le covert actions? Come? etc. Tutte domande che hanno una risposta, ma sulle quali è opportuno meditare, aprendo una discussione fra ambienti eterogenei, pubblici e privati, operativi e intellettuali o di ricerca.

Anche perché le minacce cibernetiche alla sicurezza delle istituzioni, delle imprese e degli individui sono un problema troppo grande per essere gestite in solitudine. Il tema non può costituire una specializzazione di un solo settore: problemi continui e multidimensionali richiedono, in tutta evidenza, strategie e soluzioni condivise. In particolare, con riserva per le questioni classificate, occorre superare la contrapposizione civile-militare.

La definizione tradizionale di minaccia prende in considerazione le capacità e le intenzioni. Per la nuova definizione, adatta ai tempi della rivoluzione informatica, non sono più sufficienti le capabilities (includenti gli strumenti e la capacità di accesso) e le intenzioni, cioè le motivazioni che spingono alla minaccia: occorre, in più, la conoscenza, un know how specifico e sofisticato, capace di operare all'interno di un sistema e di una rete dopo averne guadagnato l'accesso. Solo così si possono effettuare minacce di grande spessore. Ovvio affermare che anche la cyber counter intelligence deve basarsi su un know how altrettanto, se non più, sofisticato.

Basta pensare a tutto ciò che occorre cercar di conoscere attraverso una analisi sistematica e a largo raggio delle attività su Internet, necessaria ad individuare modelli di comportamento, collegamenti fra gruppi terroristici, criminali e servizi segreti - sfruttando anche le conoscenze derivanti dai molti siti dell'e-jihadismo, come, ad esempio, www.terrore.com, www.jihadunspun.com, o www.khilafah.com. - analisi di eventi, indicatori di pronta allerta (early warning), etc. e a comprendere, valutare e prevedere le conse-

guenze politiche, economiche, sociali e tecnologiche di determinati atti di spionaggio, sabotaggio e arresto o distruzione di asset critici e strategicamente rilevanti.

Unica certezza è che tutto diventerà più difficile: la complessità crescente dei sistemi IT aumenterà le vulnerabilità. Inoltre, le tendenze che emergono ci dicono che ci sarà un uso crescente di algoritmi crittografici sempre più sofisticati e che verranno sfruttate anche le asimmetrie giurisdizionali fra i diversi Stati. Ciò ci insegna che, come in altri settori della vita internazionale, una normazione condivisa può promuovere stabilità e ridurre i conflitti, evitando malintesi e facilitando la prevedibilità dei comportamenti statuali. È quindi imperativo cooperare a livello internazionale per aumentare la sicurezza collettiva nel settore del cyber spazio. Internet è globale, come globali - Stati, imprese, individui - sono gli autori degli attacchi. Ergo, la risposta deve essere globale.

Così come un ideale Stato di diritto assicura libertà, democrazia e pace sociale, così un cyber space non anomico favorisce la sicurezza e la pace.

Il diritto internazionale dovrà essere adattato a questo nuovo sistema internazionale virtuale, astrazione, nel senso di Fuller, del vecchio sistema che tutti conosciamo e che tuttavia persiste, restando destinatario di effetti assolutamente concreti, così come dovranno essere riconsiderati alcuni paradigmi interpretativi delle relazioni internazionali.

Anche in questo nuovo sistema si affrontano valori contrapposti: da una parte, ostruzionismi, divieti e censure; dall'altra, dalla parte cioè dei Paesi democratici, rispetto per le libertà e i diritti fondamentali, libero flusso delle informazioni con il solo limite della sicurezza pubblica, limite - peraltro - che deve essere ben definito dal punto di vista giuridico.

Insomma, lo spazio virtuale non può essere un sistema senza regole. Al contrario, sono le regole (norme) che tutelano i diritti e le libertà di tutti; è la cooperazione internazionale che sola può tutelare la sicurezza di comunità e di singoli.

Le conseguenze dei cyber attack sono gravissime anche dal punto di vista economico. I Ministri delle Finanze del G8 ritengono che i crimini informatici costino 80 miliardi di dollari all'anno.

Alcune domande impongono un'attenta riflessione: quali sono i costi, reali e potenziali, di tali attacchi? Quanto frequentemente dobbiamo aspettarceli? Possiamo quantificare tutto ciò in maniera tale da informarci sull'ammontare ottimale della spesa che le istituzioni e le imprese dovrebbero affrontare per difendersi? Quanto efficace sarebbe tale spesa?

Risposte precise a tali domande per ora non ce ne sono. Mancano metodologie standard per il calcolo di tali costi e l'analisi sulla frequenza degli attacchi è resa difficile dalla ritrosia delle entità colpite a rendere pubbliche le loro vulnerabilità. Ad oggi, insomma, tutte le stime sono soltanto valutazioni "a braccio". Ma non c'è dubbio che i costi siano, a livello mondiale, dell'ordine di svariate decine di miliardi di dollari o euro, soprattutto se si considera che la quantità dei costi dipende da cosa si prende in esame: il tempo perso, la produttività sospesa o ridotta, i "falsi positivi" (es. business perduti), spese per misure ostative, etc.

Anche le assicurazioni, di solito, sono a dir poco restie a coprire i rischi derivanti dai cyber attacchi, anche per la mancanza di dati empirici che consentano di costruire tavole attuariali.

Gli attacchi "cyber", invece, sono vantaggiosi in termini di costi, la loro azione è immediata e inaspettata, godono di anonimato, hanno capacità di colpire globalmente, rischiano pochissimo, utilizzano strumenti relativamente facili da usare, etc.

E veniamo adesso, molto brevemente, alla questione definitoria. Il lessico in materia lascia a desiderare e non sempre ad un termine corrisponde un solo significato. Ad esempio, quando si parla di "attacco", non è chiaro se si intende hackeraggio, oppure spionaggio, interruzione di servizio od altro ancora. Porsi il problema dell'armonizzazione delle definizioni è in particolar modo necessario ai fini del funzionamento della cooperazione internazionale in materia e funzionale all'efficacia dell'azione multilaterale. Un'analisi comparata fra documenti ufficiali statunitensi ed europei mostra significative discrepanze nell'uso dei vari termini. Ad esempio, il termine cyber crime risente delle differenze delle diverse legislazioni nazionali. Fortunatamente, il problema è trattato a livello militare, dove il processo di standardizzazione è più sentito ed applicato, come dimostra il fatto che la questione "terminology/taxonomy nel cyber domain" è presa in considerazione nel Multinational Experiment 7 - Access to the Global Commons (MNE 7), di cui il cyberspazio è una parte significativa.

Così come andranno più accuratamente definite attività come cyber intelligence e network intelligence, distinguendone i campi di applicazione anche per individuare i contorni delle professionalità necessarie e dell'addestramento relativo.

La cyber intelligence può essere definita come il complesso di attività programmate ed applicate per identificare, seguire, misurare e monitorare informazioni sulle minacce digitali, nonché dati sulle intenzioni e attività di entità avversarie. Tali attività, che si svolgono con strumenti cibernetici nel cyberspazio, hanno una particolarità, a differenza delle altre forme di intel-

ligence, e cioè condividono con lo spazio fisico l'uso di Humint, l'intelligenza umana.

Intelligenza umana che si manifesta, in misura ancor più accentuata, per lo meno nella fase di pianificazione, nella network intelligence (NetInt) che si basa su concetti e principii di programmi tipo Deep Packet Inspection (DPI), capaci di identificare in tempo reale i protocolli utilizzati e i metadati (dati sui dati) ed estrarre i contenuti informativi che corrono sulla rete, analizzandone nel contempo le relazioni reciproche.

Per le imprese e per la loro politica di business e corporate security intelligence, tale tecnologia costituisce un formidabile strumento euristico. Identico vantaggio, se non maggiore, anche a fini di counter cyber intelligence hanno gli Stati che utilizzano per varie funzioni questi programmi così potenti e utili al punto che molti fra essi sono classificati.

È ovvio che con tali capacità ricognitive la cyber e la network intelligence possono contribuire in misura significativa all'attività di early warning e di previsione che è inerente ad ogni forma di intelligence.

Oggi, infatti, non soccorre più la mentalità di rispondere quando attaccati. Oggi le istituzioni e le imprese debbono ristrutturarsi per essere resilienti, e quindi flessibili; debbono essere - come usa dire oggi - "proattivi" nella protezione dei propri asset. La lista delle vulnerabilità non può più basarsi sugli eventi pregressi, ma dinamicamente aggiornata in funzione delle minacce emergenti e del profilo di rischio effettivo e mutevole dell'organizzazione.

Una prospettiva concreta, in futuro, potrà venire dal Progetto CRASH (Clean-slate design of Resilient, Adaptive, Secure Hosts) della Defense Advanced Research Projects Agency (DARPA) che mira a costruire sistemi computerizzati basati sulla biologia, traducendo le strategie del sistema immunitario in termini computazionali, capaci di monitoraggio continuo, di resilienza e di riparazione contestuale dei danni provocati dagli attacchi.

L'uso combinato della cyber analytics e della cyber forensics permetterà, con l'individuazione di schemi e correlazioni, di *connect the dots* e prevedere attacchi futuri. Prezioso ausilio verrà anche dalla cyber logistics che si curerà, fra l'altro, della sicurezza della catena che va dai fornitori al background del personale.

Come ho avuto modo di precisare più a fondo in altra sede, persino gli «eventi inaspettati» possono essere in qualche modo gestiti. Occorre prestare attenzione ai segnali deboli e monitorare costantemente la situazione.

Un solo accenno all'Italia e non è ottimistico. Mi riferisco al decreto legislativo approvato dal Consiglio dei Ministri il 7 aprile 2011 e pubblicato sulla G.U. n. 102 del successivo 4 maggio. Il decreto è in attuazione della direttiva 2008/114/CE sull'individuazione e designazione delle infrastrutture critiche europee (ICE) e la valutazione della necessità di migliorarne la protezione. A parte il ritardo di tre anni con il quale la direttiva è stata recepita, il decreto si preoccupa subito di far salve le competenze di una trentina di Ministeri, enti e commissioni varie e solo successivamente si occupa della questione in oggetto, creando ulteriori strutture: il NISP - Nucleo interministeriale situazione e pianificazione, nonché una "struttura responsabile" a sostegno del NISP stesso. Il NISP, a sua volta, deve acquisire il preventivo parere del Ministero dell'Interno che si avvale, a tal fine, per gli aspetti connessi con la difesa civile, anche della Commissione interministeriale tecnica, costituita con proprio decreto.

Dopo tutte queste consultazioni, è solo da sperare che i "cattivi" attendano un po' a sferrare l'attacco.

Concludo: in futuro, gli attacchi tramite la Rete non potranno essere evitati al 100%. Ma il combinato uso degli strumenti che la cyber e la network intelligence mettono a disposizione, insieme con una vigilanza attenta e continua, consentiranno di contenere i danni, rivelandoci - almeno in parte - la fonte delle minacce. E le lezioni via via apprese (le *lessons learned*) potranno tradursi in protocolli di controllo capaci di prevenire, sempre di più, attacchi futuri.

Come diceva Napoleone - la citazione mi sembra appropriata - «vi sono solo due poteri al mondo: la spada e l'intelligenza. A lungo andare la spada è sempre battuta dall'intelligenza».

Verso una nuova forma di guerra economica: il cyber spionaggio industriale pilotato da servizi d'intelligence

di *Luigi Sergio Germani*[*]

1. Una minaccia alla sicurezza e alla competitività del sistema Italia

Lo spionaggio industriale e scientifico – ossia la ricerca informativa occulta tesa all'acquisizione di segreti industriali e proprietà intellettuale da imprese e centri di ricerca – é un fenomeno in forte espansione in tutto il mondo. Praticato sia da Stati che da attori non-statali, esso viene condotto sempre più di frequente nello spazio cibernetico e mediante le nuove tecniche di intrusione informatica (*computer network exploitation* o *cyber-exploitation*), tra cui quelle più sofisticate, come la *Advanced Persistent Threat* (APT).

Il fenomeno insidia, in primo luogo, la supremazia economica e tecnologica degli USA, ma costituisce un problema crescente per tutti i paesi occidentali, e anche per il nostro Paese. Esso va considerato una minaccia alla sicurezza economica e alla competitività del sistema Italia sui mercati internazionali. Si tratta di un attacco all'economia italiana meno visibile e conosciuto rispetto alla speculazione finanziaria sui bond, ma altrettanto insidioso.

La più recente relazione semestrale sulla politica dell'informazione per la sicurezza, predisposta comunità d'intelligence italiana, annovera lo spionaggio industriale come una delle principali minacce alla sicurezza economica nazionale, resa più insidiosa a causa della crisi economica: «La congiuntura ha reso più vulnerabile il tessuto imprenditoriale italiano anche rispetto al fenomeno dello spionaggio industriale, che rischia sia di depauperare il potenziale produttivo e innovativo nazionale, che di

[*] Link Campus University e Direttore del Centro Studi "Gino Germani" e di Eurasia Strategy - Centro di Ricerche Strategiche sull'Eurasia, Condirettore Scientifico della Conferenza.