Cyber Defense
Un nuovo fattore critico di successo nell'ambito della politica di sicurezza

ten col Stefano Giedemann

TENENTE COLONNELLO STEFANO GIEDEMANN

Il contributo vuole fornire una visione generale del tema volta a favorire la comprensione della materia oggetto di una mattinata di studio e confronto con esperti selezionati nell'ambito di un evento specificatamente organizzato dall'Associazione della Rivista Militare della Svizzera di lingua italiana (ARMSI) presso l'**Auditorium BancaStato, sabato 17 ottobre 2015.** Il documento è sviluppato in base ad una personale prospettiva e conoscenza diretta del tema. Lo stato delle informazioni è al 15 luglio 2015.

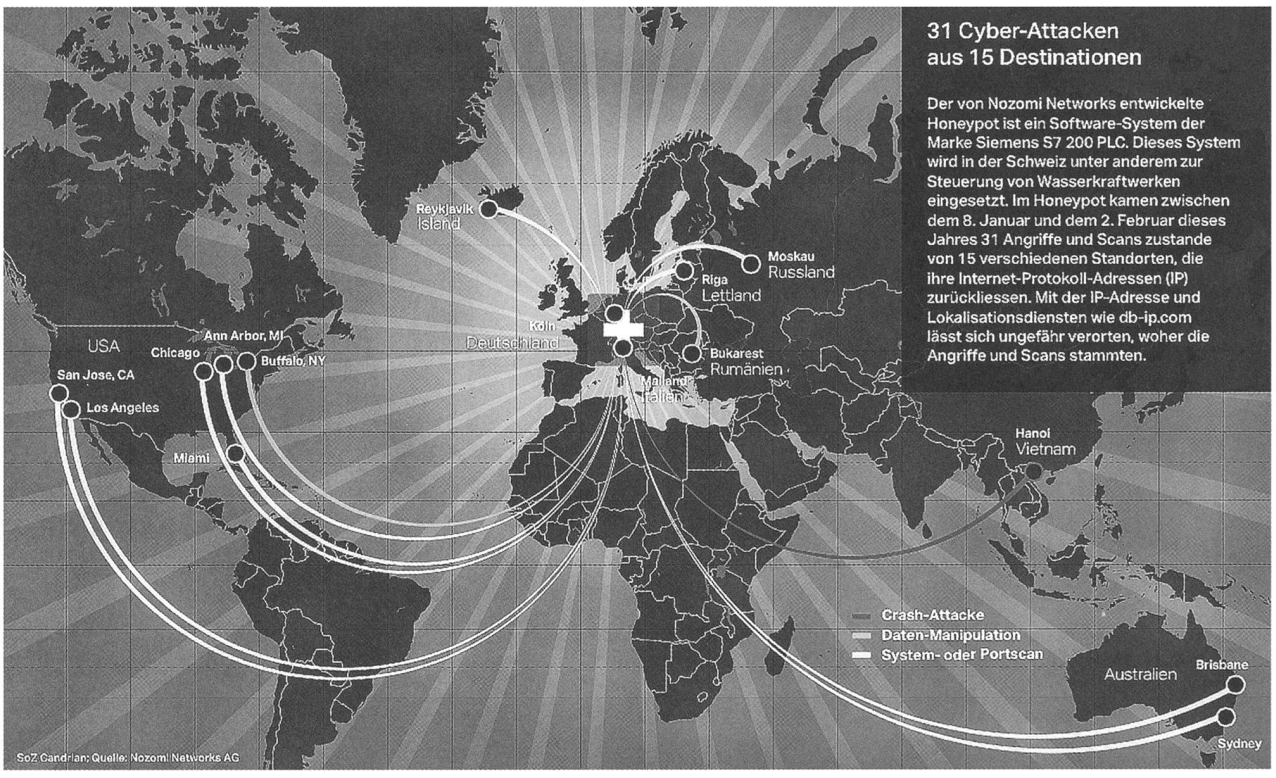
Il contesto

Grazie al grande successo e relativa espansione dell'Internet[1] e dei relativi servizi che operano e/o supportano tale piattaforma, privati, aziende ed enti statali sono ormai da anni progressivamente confrontati ad ambienti altamente tecnologici, interconnessi, pervasivi anche nella vita quotidiana e sempre più spesso aggiornati in tempo reale, da cui traggono benefici in termini di servizi e prestazioni rapide, correlate ad un'alta disponibilità operativa e senza più limiti geografici definiti.

La crescita economica, l'esistenza di un'azienda, il funzionamento di una collettività come pure del singolo ne sono ormai condizionati anche se in forme diverse. Nel contempo si assiste pure ad una lenta ma progressiva concentrazione e dipendenza da strutture con marcato rischio sistemico ovvero che possiamo definire critiche ai sensi della dipendenza che assumono i servizi da loro erogati, quest'ultimi a loro volta interconnessi e dipendenti da delicati processi regolati da livelli di servizio.[2]

Una breve panoramica mostra tuttavia come tale evoluzione attragga anche altri attori, le cui finalità puntuali si ripercuotono globalmente. Ecco alcuni recenti ma significativi esempi:

- l'attacco alla televisione francese TV5 Monde con messaggi dell'IS sul sito Facebook[3]
- l'inchiesta riguardo la panne elettrica occorsa a Washington DC[4]
- problemi tecnici che colpiscono la Borsa di New York, l'United Airlines e alcuni giornali negli USA[5]
- gli attacchi multipli contro impianti preposti all'arricchimento di uranio[6]
- l'affare dello spionaggio di capi di Stato Europei[7] e del Bundestag tedesco[8]
- le rilevazioni da Edward Snowden riguardo attività di spionaggio contro il governo f rancese[9]



- l'attacco al sito della ministero della Difesa italiano e altre infrastrutture[10]
- Kaspersky, società di software antivirus russo, vittima di un software di spionaggio[11]
- l'attacco alla società Hacking Team, azienda che vende software spia ai Governi[12]

Nuova dimensione

Visto in un'ottica più estesa, ormai assistiamo all'inserimento di una nuova importante dimensione di comunicazione rispetto a quelle conosciute tradizionalmente quali via terra, via mare, via aria o via spazio. Il cyber-spazio[13] determina dalla sua nascita negli anni 70 del secolo scorso una dimensione completamente diversa in quanto de-materializza l'aspetto geografico creandone de facto uno virtuale con proprie regole.

E se da una parte ha permesso una crescita senza precedenti, dall'altra risulta essere anche particolarmente pervasivo come lo conosciamo ormai oggi perché tocca una moltitudine d'attori nell'ambito economico, finanziario, governamentale, civile. E pure nel contesto politico-militare.

Come ogni dimensione, presenta anch'essa forme di vulnerabilità e minaccia che andando a mirare l'integrità dell'informazione presente nel cyber-spazio ne condiziona i processi operativi, il patrimonio sensibile di dati come pure l'identità andando di conseguenza ad influenzare l'erogazione di servizi, la produzione industriale, la reputazione e l'azione di soggetti fisici e giuridici. In ultima istanza anche una collettività.

Una possibile materializzazione delle minacce avviene grazie al raggiungimento di almeno tre fattori concomitanti quali in particolare:

- la debolezza intrinseca e presente nel sistema come tale, il quale potrebbe rappresentare un'opportunità per un attacco ("vulnerability");
- la conoscenza della presenza di debolezze da parte di terzi, conoscenze evinte in modalità diverse; questo stato favorisce l'insorgere di potenziali attori ("knowledge");
- la motivazione di potenziali attori unitamente ad un grado rispettivo di capacità siano esse tecniche che di conoscenze nel mettere in atto la propria azione ("ability to execute").

Come si può facilmente evincere, si tratta di uno spettro assai ampio di scenari che possono materializzarsi all'interno di un sistema multidimensionale. Sono quindi opportune delle precisazioni.

Attori

È possibile formulare una classificazione in termini qualitativi probabili attori in gruppi differenti che si contraddistinguono per capacità e motivazione.

Utilizzatori di soluzioni – Attori senza specifiche conoscenze ma che utilizzando strumenti liberamente disponibili possono arrecare danni che in genere sono a carattere limitato – circoscritto, a cui un sistema sottoposto a sicurezza[14] non causa particolari perturbazioni.

Sviluppatori di soluzioni mirate a vulnerabilità – Attori che dispongono di costanti informazioni che permettono di poter mettere in atto soluzioni specifiche e mirate allo sfruttamento di vulnerabilità conosciute anche in cerchie ristrette.[15]

Organizzazioni professionali e criminali – Attori che grazie all'adozione di modelli e strumenti sviluppati allo scopo, perseguono azioni con finalità di truffa[16] o spionaggio per conto terzi. Grazie alla possibilità di poter operare senza limiti geografici, sfruttano il differenziale legislativo vigente tra la nazione da dove parte l'attacco e quella a cui è destinato per poter portare a compimento le proprie iniziative.

Advanced Persistent Threats – Attori che operano in modalità particolarmente sofisticata verso oggetti selezionati con finalità estremamente mirate e di medio-lungo termine. Gli attacchi possono essere eseguiti sfruttando lacune dei sistemi per cui non esistono tracce elettroniche esplicite oppure tramite il posizionamento di malware a carattere operativo a basso impatto apparente. Non sempre l'effetto di queste minacce sono visibili.[17]

Organizzazioni e servizi legati a nazioni – Attori presenti in numero limitato ma che possono esercitare un'azione estremante efficace data la loro posizione dominante (sia in termini commerciali che governamentali) possono avere un influsso diretto o indiretto nella realizzazione di determinate parti di sistemi e soluzioni presenti. In altri termini la loro dettagliata conoscenza d'implementazione[19] rispettivamente l'influsso verso determinate scelte realizzative non di pubblico dominio, può garantire un vantaggio competitivo in termini di fattore tempo in caso di necessità.[19]

Finalità

Chiariti i possibili gruppi d'attori, è determinante comprendere le possibili finalità che possono essere ricercate. Le forme a seguire sono elencate in funzione della crescente pericolosità.

Vandalismo – Le finalità sono variegate: possono passare da azioni di protesta per presunte disattese situazioni politiche-economiche fino a fenomeni di vendetta puntuale contro singoli o società e rispettivi simboli, sfruttando anche l'economia delle masse del popolo presente in Rete. Grazie all'amplificazione quasi in tempo reale e diffusa in relazione al soggetto dell'attacco su scala planetaria fornita dai media, gli effetti possono comportare tra gli altri un danno d'immagine difficilmente recuperabile in tempi brevi con impatti economico-finanziari anche rilevanti.

Criminale – Singoli o appartenenti a gruppi o organizzazioni, perpetuano una o più azioni combinate basate su truffa, furto, ricatto, falsificazione e diffamazione in base a proprie iniziative o su mandato.[20] Lo spettro di contesti che ne risultano possono essere riconducibili situazioni di natura finanziaria, personale o legati alla concorrenza ma anche d'altra finalità specie se il mandante è qualificabile in forma indiretta sono dei Stati. Le azioni in questo contesto sono particolarmente sofisticate e molto focalizzate all'obiettivo da raggiungere.[21]

Spionaggio – L'oggetto delle azioni è la ricerca di informazioni e dati per poter raggiungere all'insaputa della parte lesa un vantaggio, non necessariamente a carattere economico ma anche politico e militare. Tramite l'uso di strumenti e metodi legati ai Servizi d'Informazione, attori quali Stati, aziende o persone private (spesso su mandato), operano in modo tale che le proprie azioni, se scoperte non siano a loro riconducibili. Questa forma

4 – 8 novembre 2015
Locarno Palazzetto Fevi

La Brigata fanteria di montagna 9 ti invita all'esposizione „Il tuo esercito" nell'ambito di Espoverbano a Locarno.

Benvenuti!

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Esercito svizzero

esercito.ch/iltuoesercito

d'operatività può risultare particolarmente amplificata dalle modalità di interazione nell'ambiente Cyber, impone conseguentemente grossi sforzi nell'indentificare con ragionevole certezza i veri attori e in seconda istanza i mandanti ultimi.[22]

Sabotaggio – Le motivazioni possono essere molteplici come visto nelle altre forme. L'obiettivo è di ricercare un danno primariamente verso processi gestiti da infrastrutture IT, telecomunicazione e controllo. Questo si materializza in interruzioni di servizio che possono causare a dipendenza dell'ampiezza della portata a successivi danni anche di carattere fisico. Non è difficile immaginare impatti nell'ambito della fornitura di corrente elettrica, della logistica e trasporti, dell'economia e finanza. Azioni di questo tipo possono risultare essere parte integrante di fasi specifiche nell'ambito di un processo di controllo strategico di aziende o settori economici, ma sicuramente più in generale di azioni di destabilizzazione e successivo controllo di Stati.

Terrorismo – Interessante costatare che più che azioni comportanti danni (anche tramite una combinazione di mezzi tradizionali o fisici con la distruzione puntuale di oggetti facenti capo all'ambiente Cyber), un trend ormai consolidato consiste in organizzazioni di matrice terroristica che usano la realtà Cyber all'esterno del proprio sistema quale veicolo di propaganda e reclutamento mentre all'interno per comunicazione e ricerca informazioni.[23]

Conflitto – È da prevedersi l'uso delle componenti Cyber integrate nell'ambito delle Operazioni tradizionali aventi per oggetto non solo le infrastrutture civili, ma anche quelle militari legate al C4ISTAR.[24] Sono quindi possibili forme di semplice disturbo di funzionamento fino al completo annullamento della capacità operativa. Effetto tutt'altro che da escludere visto il largo spettro d'utilizzo di componentistica elettronica presente negli Eserciti.[25]

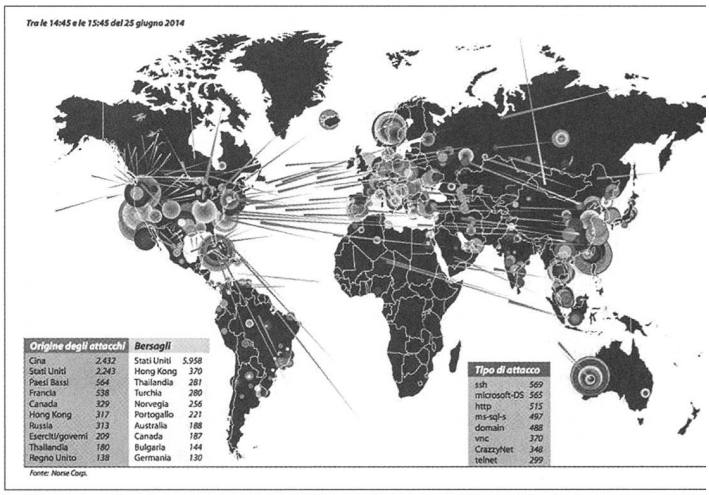
È opportuno rilevare alla luce delle forme possibili appena descritte[26], a differenza di una visione più classica, la realtà Cyber in questa fase annulla de facto la componente numerica degli attori e dei strumenti, ponendo piuttosto l'attenzione riguardo la competenza e l'efficacia di pochi ma estremamente preparati attori.

Soggetti esposti

In questo tipo di realtà tutti sono fondamentalmente un bersaglio. Ma è sulla base dell'analisi in un contesto globale (ambiente) della robustezza del proprio sistema, dei processi supportati, dalla rilevanza delle informazioni in esso presente, del grado di rilevanza sistemico in un particolare contesto, l'interesse che si riveste in uno spazio temporale definito, che è possibile effettuare ragionevolmente dei distinguo.

Forme di attacco e difesa

È impossibile effettuare in questa sede una trattazione dettagliata riguardo le possibili forme di attacco. Riteniamo solo più a titolo informativo alcune delle tecniche e procedimenti classificati come Remote Exploits, Social Engineering, cavalli di Troia, Denial of Services, botnet, ransomware, govware, backdoors a livello di applicativi e di firmare, dispositivi esplicitamente manipolati. In sostanza varianti che possono essere applicate a dipendenza della finalità ricercata.



Di maggiore interesse riveste la parte riguardo la difesa, in quanto per definizione non esiste la sicurezza con garanzia al 100% in questo tipo di realtà. Si tratta quindi di sviluppare dei modelli operativi multidisciplinari.

Il primo framework che presentiamo è basato su un concetto a blocchi tematici interdipendenti che vedono la centralità in un sistema di costante monitoraggio dei rischi con le seguenti dimensioni:

- protezione: misure tecnico-organizzative implementate in modo da rispondere alle possibili minacce secondo a dei criteri definiti;[27]
- prevenzione: azioni dirette a impedire il verificarsi o il propagarsi di eventi non desiderati o dannosi; spesso trattasi di misure organizzative-procedurali-comportamentali;
- capacità di reazione: insieme di processi, risorse e strumenti che possono affrontare con successo situazioni a fronte di accadimenti, non solo fino al ripristino della situazione in origine;
- anticipazione: capacità e misure implementate per comprendere possibili minacce; queste possono essere ricondotte a un sistema di ricerca e segnalazione informazioni accurato;[28]
- dissuasione: implementazione di una configurazione di misure credibili tali da potenzialmente impedire un soggetto terzo ad intraprendere l'azione pena le possibili reazioni e/o rappresaglie.[29]

Il secondo framework denominato Cyber Security Incident Cycle Model[30] è quello proposto dalla NATO, sicuramente più articolato e facente riferimento a molteplici attori e capacità di coordinamento e intervento, come ad esempio a gremi di Cyber

Governance e Diplomacy come pure di Counter Cybercrime. È evidente che il modello presenta un grado di maturità finale che sarà possibile incontrare solo più avanti nel tempo.

Sfide aperte

Nel 2013 il Consiglio federale ha approvato il piano di attuazione della Strategia nazionale per la protezione della Svizzera contro i rischi Cyber. Le misure approvate si prefiggono di rafforzare la prevenzione e la gestione della continuità operativa e delle crisi ma anche l'acquisizione di esperti in cibernetica nell'Amministrazione federale nonché la costituzione di un Comitato interdipartimentale ai fini del coordinamento. Ci permettiamo di porre a questo proposito una domanda: è sufficiente? Sicuramente di tratta di un primo importante passo, ma importanti sfide sono sul tavolo.

Da un punto di vista tecnologico, l'evoluzione della tecnica e delle relative esigenze di interconnessione non conosce limiti[31], dove vi è una crescente complessità intrinseca e una progressiva assenza di trasparenza riguardo agli "oggetti" che trattano informazioni. Senza contare l'enorme pressione esercitata dei mercati nel ridurre costantemente i cicli di vita delle rispettive componenti.

Chi opera nell'ambito di enti e/o infrastrutture critiche, ha sicuramente riconosciuto la necessità d'operare con componenti e/o oggetti certificati nell'ambito di tutto lo spettro quale possibile garanzia. Questo però comporta oneri importanti nei relativi processi e nella conoscenza da mettere in campo per assicurare il livello di sicurezza ricercato, in ultima istanza che incidono sui fattori costi e tempi.

L'evitare implementazioni delle famose back doors nelle soluzioni di sicurezza per questioni diverse è di difficile attuazione specie per quelle relative alla cifratura o securizzazione dei dati, non da ultimo paradossalmente proprio per aspetti di "sicurezza nazionale". Progetti sviluppati nell'ambito dell'open source domain non hanno fornito al momento risultati consolidati. Ne consegue de facto una sempre data vulnerabilità.

Il fenomeno della gestione per mandato – altrimenti detto in Outsourcing con prestazioni soggette a livello di servizio – risultano spesso sotto la pressione dei costi e con obiettivi strategici non sempre allineati. Lo stesso si costata anche nell'ambito degli sviluppi e nelle implementazioni. Non è quindi da escludere rischi residui nella qualità dell'esecuzione e certificazione.

L'esistenza di imprese con una bassa percezione del problema, specie nell'ambito delle PMI che non rientrano in settori economici fortemente regolamentati. L'assenza d'approfondite conoscenze nel campo oppure dall'accettazione dei rischi per ragioni d'ordine economico, possono condurre ad un limitarsi a soluzioni minime di protezione o non vederne neanche la necessità.

Tema delicato è pure l'interdipendenza tra realtà pubbliche e private, con i relativi perimetri di responsabilità e autorità dove sono in gioco l'operatività d'infrastrutture critiche, diverse delle quali ora privatizzate. In particolare la problematica può risiedere fino a dove uno Stato può legiferare nel contesto specifico rispettivamente può pretendere un livello effettivo minimo di sicurezza. Un passo concreto potrebbe risiedere nell'integrare nel processo generale gruppi d'interesse e associazioni mantello che potranno accompagnare le differenti realtà verso partner privati "certificati".[32]

Ruolo e posizionamento dell'Esercito

Anche considerati gli attuali fronti di tensione, in un orizzonte temporale di medio termine la possibilità di un conflitto armato in Europa è attualmente ritenuto poco probabile.[33] Per contro avvenimenti nel contesto Cyber con impatti verso la Società possono essere considerati come più possibili. E le conseguenze, date le interdipendenze e il grado tecnologico raggiunto, sono importanti per il relativo funzionamento.

L'Esercito come riserva strategica nazionale, deve poter assicurare il proprio operato anche in scenari Cyber Defence, ovvero dove la minaccia comporta azioni sia contro oggetti nell'ambito civile che contro l'Esercito medesimo. Questo può avvenire primariamente garantendo la propria prontezza e la capacità d'assolvere i compiti. Secondariamente poter operare a titolo sussidiario nel contesto Cyber.

Come traspare anche dal citato piano della Confederazione, i possibili ambiti sono:

- assicurare una comunicazione resiliente a favore dell'autorità pubblica e di selezionate strutture a rischio sistemico classificate;
- supporto verso partner e istanze legati alla sicurezza innalzandone il livello di resilienza a livello di infrastrutture critiche;
- protezione integrale (inteso come logica e fisica) di oggetti particolarmente sensibili;
- contributo fattivo nell'ambito dell'informazione, analisi e difesa di minacce nell'ambito Cyber.

Questo determina l'integrazione di una dottrina d'impiego Cyber nel framework operativo, la definizione e acquisizione di mezzi e risorse, adeguare e completare la relativa istruzione. Una rivoluzione che per analogia è avvenuta nel passato con l'avvento di una nuova dimensione sul campo di battaglia.

Considerazioni conclusive

Solo una società civile che è in grado d'integrare nel suo dispositivo di sicurezza tutte le dimensioni, quindi anche quella Cyber, può risultare resiliente a fronte delle opportunità e delle minacce nell'Era dell'Informazione. Giudicando inoltre l'aumento sempre più significativo d'attività legate ad attori di Stato[34], oltre ad attori pubblici e privati una parte preminente dovrà essere gioco forza ricoperta dall'Esercito.[35] ■

Bibliografia

- "National Cyber Security Framework Manual", NATO – CCDCOE, Alexander Klimburg, 2012
- "Strategia nazionale per la protezione della Svizzera contro i Cyber-rischi", DDPS, 2012
- "Framework for Improving Critical Infrastructure Cybersecurity", NIST, 2014
- "Rapporto annuale 2014", SCOCI - Servizio di coordinazione per la lotta contro la criminalità su Internet, 2015
- "Katastrophen und Notlagen Schweiz – Technischer Risikobereicht 2015", UFPP, 2015

Note

1 Internet o rete digitale globale come insieme delle reti, siano esse pubbliche che private (o riservate), che interconnesse permettono la trasmissione dati via cavo o etere sia in forma aperta che crittografata, indipendentemente dalla finalità.

2 Un trend riconosciuto da oltre una decina d'anni anche nel settore terziario, frutto di operazioni di trasformazione e dislocazione dei processi grazie all'effetto della globalizzazione. De facto si è pure assistito ad uno spostamento del rischio operativo sulla catena del valore, con possibili concentrazioni di rischio su un numero relativamente limitato di attori.

3 http://www.bbc.com/news/world-europe-33072034

4 http://www.armstrongeconomics.com/archives/29167

5 http://www.notiziegeopolitiche.net/?p=54460

6 http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529

7 http://www.nzz.ch/international/deutschland-und-oesterreich/nsa-spaehte-nicht-nur-merkel-aus-1.18572839

8 http://www.n24.de/n24/Nachrichten/Politik/d/6801100/cyberangriff-auf-bundestag-hat-folgen.html

9 http://www.lemonde.fr/technologies/article/2013/10/25/the-nsa-s-intern-inquiry-about-the-elysee-hacking-revealed_3502734_651865.html

10 http://italia-24news.it/2015/05/20/siti-di-expo-e-ministero-difesa-sotto-attacco-hacker-arresti-e-perquisizioni-15169-38015/

11 http://www.nzz.ch/digital/kaspersky-faellt-cyberangriff-zum-opfer-ld.586

12 http://www.cdt.ch/tempo-libero/internet/134493/la-situazione-e-fuori-controllo.html

13 Ricercando una definizione, si potrebbe formulare in tal senso: "Spazio operativo dove i dati sono ripresi, memorizzati, trasmessi, elaborati, classificati, codificati, presentati. Questo a favore di azioni che trovano una materializzazione fisica".

14 Come si vedrà più avanti, soluzioni che possono essere ritenute robuste sono quelle che dispongono di misure tecnico-organizzative operative, sono sottoposte a interventi regolari di Vulnerability Assessments (verifiche della solidità delle configurazioni e dell'architetture) e Penetration Test (verifiche effettive delle configurazioni in modalità controllata), dispongono di soluzioni IDS (monitoraggio di intrusioni) e di una capacità di reazione a fronte di un attacco.

15 Si tratta di soggetti che, disponendo di conoscenze superiori nei vari meccanismi di sicurezza delle soluzioni oggetto di attacco, sanno trarre il massimo profitto dalle debolezze riconosciute.

16 Il settore finanziario in particolare, ma anche tutti gli attori con rilevanza transazionale in termini di denaro, sono un ambiente particolarmente fertile. Lo sfruttamento delle debolezze, in particolare del comportamento dei fruitori dei relativi servizi, ne facilita il compito.

17 La tecnologia applicata dipende dalla finalità ricercata. Nei classici casi quali "Red October" l'obiettivo era la ricerca d'informazioni nel periodo più lungo possibile, mentre per "Stuxnet" era un'azione di sabotaggio di apparecchiature in un contesto d'uso basato sul medio periodo.

18 La complessità delle soluzioni tecniche adottate, sempre più stratificate, garantisce in ultima istanza solo ai grandi player di soluzioni la conoscenza di dettaglio. Il trend consolidato del framework ad oggetti, i quali si richiamano a loro volta in modalità "trasparente" in una logica di riutilizzo per velocizzarne lo sviluppo, in realtà maschera le relative logiche ed allarga la diffusione di potenziali lacune.

19 Nella pubblicazione edita nel 2014 "When Google met Wikileaks" Julian Assange mostra l'influenza fra lo Stato e una piattaforma di massa, frutto di un incontro avuto nel 2011 con Eric Schmid, Chairman di Google.

20 Fonte di preoccupazione le nuove forme di ricatto a cui singoli attori sono vittime; vedi anche il contributo http://www.nzz.ch/mehr/digital/cybererpressung-ransomware-tox-ld.449

21 Va considerato che dove l'obiettivo è ritenuto tecnicamente sicuro, il focus può essere spostato verso il fattore umano, anello sempre più debole attuando tecniche nell'ambito del "Social Engineering" accompagnando il tutto da azioni riconducibili a forme di violenza fisica.

22 Vedi il recente caso legato alla Sony con presunti attacchi perpetrati a partire dalla Corea del Nord in occasione della divulgazione di un discutibile film; la situazione non è ancora stata resa trasparente ad oggi.

23 Vedi anche l'articolo recente apparso sul CdT del 9 luglio 2015, "ISIS La Jihad su e-book e Twitter, ecco come i gruppi fondamentalisti utilizzano i nuovi mezzi di comunicazione di massa".

24 C4ISTAR - Command, Control, Communications, Computers, Information/Intelligence, Surveillance, Targeting, Acquisition and Reconnaissance.

25 L'introduzione della funzione IT e telecomunicazione ha permesso un salto quantico nell'ambito della efficienza ed efficacia non solo del Comando, Comunicazione e Controllo ma anche dell'uso di armi, apparecchi e mezzi.

26 Anche se non trattato specificatamente, non possiamo per completezza almeno non citare situazioni accidentali circoscritte oppure con effetto domino. A questi scenari non si possono escludere una sovrapposizione di azioni puntuali che sfruttano la debolezza inaspettata e momentanea del sistema.

27 L'adozione di misure standardizzate e coordinate costituisce uno dei fattori critici di successo; vedi anche "Sfide aperte".

28 L'articolazione della possibile rete d'informazioni dipende dalla natura del sistema che risulta essere oggetto di protezione; immediata la comprensione del grado di complessità per una copertura a livello di infrastrutture critiche in un contesto di sicurezza nazionale.

29 Tipicamente queste possono essere sia a carattere tecnico (p.es. interruzione dell'accesso), giuridico (p. es. perseguimento legale correlato a sanzioni) o reazione sia Cyber che fisica (p.es. tramite enti militari o civili preposti).

30 Vedi The Five Mandates and the Six Elements of the Cyber Security Incident Cycle Model.

31 Auf der Suche nach der «Killer-App», http://www.nzz.ch/finanzen/auf-der-suche-nach-der-killer-app-1.18574888

32 Il mercato offre sul tema il modello ISO/IEC 27032:2012 - Security techniques - Guidelines for cybersecurity.

33 D'interesse anche il contributo del Generale di Corpo d'Armata dell'Esercito Italiano Fabio Mini apparso in Limes 01/2015 dal titolo "Le guerre non scoppiano più - I paradigmi bellici classici sono esauriti."

34 http://www.limesonline.com/chi-non-fa-ciberspionaggio-di-stato-alzi-la-mano/79367

35 http://news.usni.org/2015/07/02/document-2015-u-s-national-military-strategy