Zeitschrift: Rivista Militare Svizzera di lingua italiana : RMSI
Herausgeber: Associazione Rivista Militare Svizzera di lingua italiana
Band: 90 (2018)
Heft: 5

Artikel: CIOR : le sfide della digitalizzazione
Autor: Giedemann, Stefano
DOI: https://doi.org/10.5169/seals-846897

CIOR – Le sfide della digitalizzazione

col
Stefano Giedemann

Dai temi determinati dalla confrontazione tradizionale alle sfide attuali determinate dalla tecnologia: operazioni e resilienza nel Cyber spazio, l'iper-informazione multicanale e la proliferazione dell'automazione negli armamenti. Ecco alcuni temi chiave trattati negli eventi dell'anno in corso e che forniscono quindi uno spaccato interessante nell'ambito della politica di sicurezza nella sfera d'interesse della NATO.

col Stefano Giedemann
vicepresidente SSU e vicepresidente CIOR per la Svizzera

Introduzione

Nell'anno del 50° di esistenza della *Confederazione Internazionale degli Ufficiali di Riserva* (CIOR), i cui festeggiamenti ufficiali si svolgeranno prossimamente nella nuova sede NATO a Bruxelles, non sono mancati durante i tradizionali incontri anche le giornate di studio e seminari durante i quali sono stati trattati temi di stretta attualità, in particolare il fenomeno della digitalizzazione del, e attorno al, campo di battaglia.

Se da una parte si assiste a un ritorno sempre più marcato all'uso dell'informazione ai sensi d'influenzare il pubblico definito, sia tramite i canali tradizionali ma soprattutto i media digitali, dall'altra vi è ormai piena consapevolezza che la digitalizzazione impone maggior impegno nella sicurezza relativa alla tecnologia interconnessa e più attenzione all'accelerazione nell'ambito dell'automazione degli armamenti.

Winter Seminar

Nell'ambito del tradizionale Winter Seminar svoltosi a inizio febbraio a Bonn, la decina di relatori provenienti da diverse realtà si sono confrontati sull'arco di tre giorni sulla semplice domanda "Cyber Threats – are we prepared?", non tanto nella declinazione stretta militare come avvenuto l'anno precedente ma piuttosto con uno sguardo attento e critico verso l'ambiente economico-sociale.

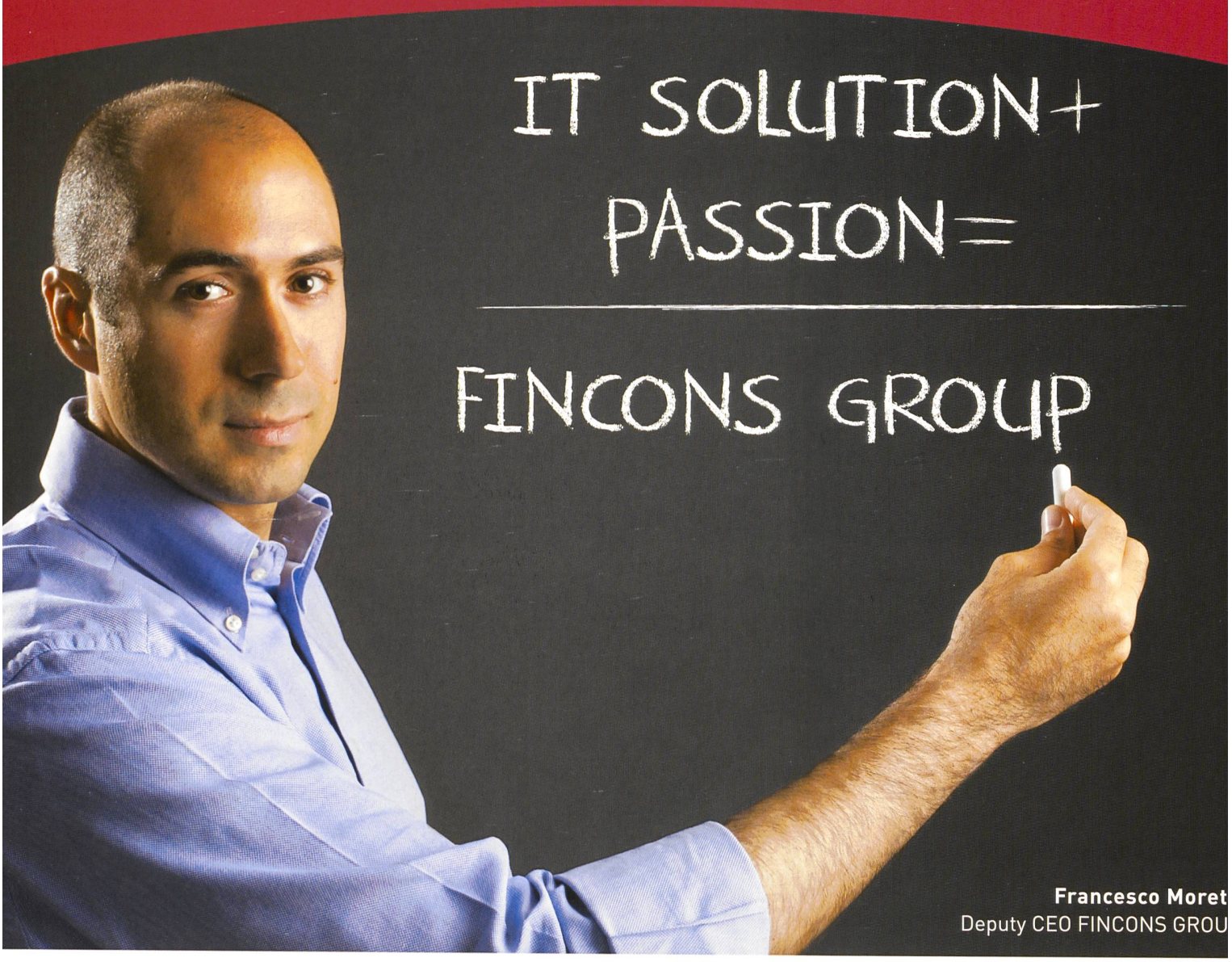
La percezione rilevata dopo alcuni significativi eventi negativi in tali ambiti, porta a riflettere sulla vulnerabilità delle nostre attuali infrastrutture tanto che non è impensabile ritenere plausibile lo scenario secondo cui, a fronte di un'eventuale aggressione sistematica portata in tale spazio, ci si ritrovi in una seria situazione d'instabilità tale da non riuscire poi più a riprenderne il controllo. In altri termini nel contesto militare di non riuscire a mobilitare e gestire le operazioni con un relativo successo; analogamente nell'ambito economico-finanziario disturbare pesantemente il normale funzionamento degli scambi e degli approvvigionamenti fino al relativo fallimento.

La motivazione va ricercata nel *fenomeno di progressiva concentrazione dei rischi* (in termini di prestatari di tecnologia e servizi, come pure di aziende che le erogano), che genera un paradosso mai visto nella società moderna nell'ambito specifico: *il rischio non ha una caratteristica endemica o epidemica, ma epidemico concentrato*, ovvero l'effetto è a propagazione quasi immediata e sistemica.

Quale rimedio a fronte di tale situazione? Primariamente riconoscere che il design delle soluzioni e la governance delle medesime deve sempre più passare da una riforma nella modalità con cui queste vengono realizzate e gestite: la regola del *bubble-driven* degli ultimi due decenni orientata al *short time-to-market* va ora allineata con il principio *security-by-design*. Ecco quindi che diversi sistemi standard disponibili e adottati dal mercato saranno da ristrutturare nel tempo, perché attualmente troppo vulnerabili e quindi soggetti a frequenti e costosi aggiornamenti di sicurezza. Questo gioco forza comporterà nel medio termine l'introduzione di una nuova generazione di soluzioni e – di conseguenza – nuovi investimenti in periodi non necessariamente, e dal punto di vista economico, interessanti.

Secondariamente riprendere il *principio della resilienza*. L'iperconnessione con altri partner del proprio ambiente operativo, sia per necessità commerciale (accesso ai mercati) sia per scelta strategica (partner distribuiti della catena del valore aggiunto) necessita attenzione: in termini olistici i vantaggi attuali dati dalla globalizzazione delle interconnessioni necessitanti per competere assommati ai rischi correlati compensano economicamente i costi in caso di evento negativo? Di conseguenza, tenuto conto che risultare vittima indiretta di azioni portate da Stati o gruppi criminali verso target fuori dal proprio

Abbiamo aggiunto all'IT il nostro valore più grande.



Conoscenza dei business in cui operiamo, competenze specialistiche, metodo: la nostra base è questa. Solida. Ma è la passione la nostra marcia in più, quella che ci ha fatto crescere e ci fa essere da 30 anni un punto di riferimento irrinunciabile per tante imprese leader.

La passione per il nostro lavoro: stare accanto ai manager, aiutarli a realizzare le strategie offrendo le soluzioni IT più innovative in tutte le fasi che compongono la catena del valore di un'impresa.

La passione per le risposte che fanno la differenza nella gestione del business.

FINCONS **FINCONS GROUP**

You shape your strategies, we partner to achieve your goals!

FINCONS GROUP 30 YEARS OF I.T. PASSION

www.finconsgroup.com

ambito economico oppure anche semplicemente di black-outs strutturali è statisticamente sempre più probabile, il fattore centrale di successo del singolo attore è la robustezza tecnico-operativa nel contesto settoriale in cui si trova.

Unendo questi due aspetti, ecco l'importanza di progredire nel processo d'implementazione di una società resiliente nell'ambito del rischio della sicurezza informatica e basata su tre livelli come indicato da diversi esperti rifacendosi anche alle indicazioni presenti nei vari White Papers nazionali:

- *Top* – Coordinamento statale per la difesa integrata su infrastrutture critiche legate al funzionamento dello Stato nel suo insieme, persecuzione legale anche internazionale;

- *Middle* – Resilienza all'interno dei sistemi macro-economici, quali la finanza, le comunicazioni e i trasporti, la logistica e l'approvvigionamento energetico e alimentare, l'economia privata; questo obbliga a regolamentazioni settoriali che i singoli attori possono adottare a seconda delle specialità;

- *Baseline* – Robustezza del singolo elemento nell'eco-sistema (cittadino incluso, in ultima istanza), ovvero obbligatorietà che ogni soggetto debba assicurare le misure adeguate per resistere ad attacchi puntuali e a lui indirizzati, senza mettere in crisi il sistema superiore.

Da queste considerazioni sono poi declinabili le implicazioni per l'Esercito, fortemente dipendente dall'economia civile negli strumenti tecnici legati ad esempio ai processi logistici e delle risorse umane così come nella comunicazione e nella condotta.

Summer Congress

Durante il congresso estivo svoltosi a Québec a inizio agosto, nell'ambito della giornata tradizionale legata al Simposio, tutti i partecipanti hanno potuto interagire con i relatori nelle

differenti presentazioni attorno al tema "Utilization of Reserve Forces for the fight against disruptive warfare formats".

In una prima fase è stato ripreso il tema del Winter Seminar, introducendo meglio la componente di *Information Warfare* (o Info Ops) strettamente ad esso correlato. Interessante il modello tecnico a 7 livelli che sta pure alla base della sicurezza nel campo cibernetico ISO-OSI con l'aggiunta di ulteriori piani non tecnici quali *People* (non solo mappando le relazioni sociali, ma andando a minare la fiducia tra essi e le organizzazioni come pure i sistemi), *Money* (con interruzioni dell'erogazione dei servizi, lo spionaggio industriale fino alla compromissione dell'operatività delle infrastrutture critiche) e *Politics* (con la disinformazione e la manipolazione nell'intento di allontanare il cittadino nel suo consenso democratico). Questi nuovi livelli applicati al Cyberspazio concorrono ora in maniera più diretta, immediata e disruttiva rispetto al passato, minando a vari livelli fino alla volontà di coesione di una porzione di popolazione, con effetti ben chiaramente comprensibili specie se correlati alla geopolitica di potere.

In una seconda fase sono state approcciate le conseguenze della digitalizzazione nell'automazione, con in particolare a titolo esemplificativo l'uso esponenziale di droni come pure – più

in generale – automi e armamenti a progressiva capacità e intelligenza artificiale (anche chiamati *sistemi d'arma autonomi letali*). Alla luce delle recenti prese di coscienza della problematica ai più alti livelli quali le Nazioni Unite, si è cercato di strutturare la comprensione della portata intorno a tre grandi aree tematiche: aspetti tecnologici, aspetti militari e considerazioni etico-giuridiche.

Da un punto di vista *tecnologico*, sebbene non vi sia ancora una definizione condivisa tra gli addetti ai lavori, è possibile operare una prima distinzione tra sistemi altamente automatizzati, ossia quelli che hanno funzioni autonome, ma che dipendono da pre-programmazioni umane, e sistemi autonomi che invece sono capaci di apprendere e adattarsi al contesto anche prescindendo dalla programmazione iniziale. Alla luce di tale distinzione, è possibile sostenere come i sistemi che rientrano nella prima di tali due categorie possano trovare disciplina all'interno delle norme di diritto esistenti e non sollevare problemi nell'imputazione della responsabilità giuridica del loro utilizzo, mentre i secondi potrebbero presentare delle problematicità sotto il profilo legale ed etico.
Tuttavia come rilevato da un relatore, la mancanza di una definizione di lavoro condivisa rimane ancora una questione aperta e fonte di un acceso dibattito: *la relazione uomo-macchina e il concetto di prevedibilità*. Quanto al primo, il grado di autonomia di un determinato sistema d'arma potrebbe essere valutato in base al suo rapporto con gli operatori umani e al punto in cui il controllo umano si interrompe nel ciclo di selezione e ingaggio degli obiettivi. A tale riguardo emergono i concetti di *meaningful human control* e *appropriate level of human judgment*, intesi come fattori determinanti sia per la definizione di autonomia di un sistema sia per stabilire il limite oltre cui certe armi potrebbero sollevare dei dubbi sotto il profilo etico. Per il secondo concetto da considerare è la prevedibilità dove, in linea di principio meno un sistema è prevedibile – perché in grado di evolvere e apprendere dalla propria esperienza adattandosi a contesti dinamici, indipendentemente dalla programmazione di partenza – più esso è da considerarsi autonomo.

Un'analisi più approfondita dello stato dell'arte della ricerca e sviluppo nel settore delle tecnologie autonome, sia in ambito civile sia militare, nonché un'esplorazione dei possibili sviluppi futuri, consente di classificare ulteriormente i sistemi d'arma esistenti *in base al loro grado di autonomia*. In particolare, si possono distinguere sistemi operati a distanza, sistemi automatici e sistemi autonomi. Questa distinzione evidenzia come le tecnologie attuali dipendano tutte e in varia misura dal monitoraggio e dalla supervisione dell'uomo.

Nell'ambito della ricerca, lo sviluppo di tecnologie completamente autonome si scontra con almeno due ostacoli. Da un punto di vista prettamente tecnico, si evidenziano ancora dei *limiti strutturali nella capacità dei sistemi autonomi di gestire situazioni impreviste e complesse e di elaborare dati abbastanza rapidamente*; a questi si aggiunge la *riluttanza umana* che tende a dubitare delle capacità e dell'adeguatezza dei sistemi tecnologicamente complessi e a non utilizzare sistemi sui quali non si può avere pieno comando e controllo.

Se ci si sposta invece sul piano legale sono due le *questioni etico-giuridiche* principalmente dibattute. Da un lato, viene generalmente affermato che il diritto internazionale umanitario esistente si applicherebbe come a qualsiasi sistema d'arma, anche allo stadio della ricerca o sviluppo. Gradi elevati di autonomia, in altri termini, non potrebbero giustificare la violazione delle norme e dei principi del diritto internazionale. Al contempo è ribadito come proprio l'applicazione di tali principi, in particolare quelli della proporzionalità e della distinzione, richiederebbe delle valutazioni di carattere soggettivo che, per loro stessa definizione, necessitano di un input umano.

Particolare attenzione è stata infine dedicata alle *legal reviews*, ex art. 36 del Primo Protocollo aggiuntivo alle Convenzioni di Ginevra del 1949 relativo alla protezione delle vittime dei conflitti armati internazionali. La disposizione richiede che nello studio, messa a punto, acquisizione o adozione di una nuova arma, di nuovi mezzi o metodi di guerra, si proceda a una valutazione/analisi atta a stabilire se il suo impiego sia conforme o meno alle disposizioni del suddetto Protocollo o al diritto internazionale generalmente applicabile. In questo contesto emerge anche il concetto di *accountability*, ovvero della necessità di assicurare che l'utilizzo di sistemi d'arma autonomi non pregiudichi una chiara e netta identificazione dei responsabili delle decisioni sull'utilizzo della forza.
Se da un lato l'uso di armi autonome rappresenta una tecnologia che affascina per i suoi potenziali impieghi nei teatri operativi, dall'altro presenta vari fattori di rischio legati al loro sviluppo e impiego, alcuni dei quali connessi a questioni di carattere prettamente tecnico. La complessità tecnologica delle funzionalità autonome potrebbe generare comportamenti non previsti e indesiderati, soprattutto in contesti complessi e dinamici. Il rischio di comportamenti imprevedibili sarebbe maggiore per le tecnologie capaci di apprendere e adattare autonomamente la propria condotta al contesto operativo.

Oltre a questi fattori tecnici, ve ne sono altri di natura più politica e strategica che vanno segnalati come potenzialmente rischiosi, soprattutto nel settore della sicurezza. Lo sviluppo, la produzione e la commercializzazione potrebbero ingenerare *una nuova corsa agli armamenti e accentuare la componente asimmetrica dei conflitti* oggi in essere e determinare, quindi, una maggiore instabilità a livello regionale e globale. La soglia psicologica oltre la quale decidere l'impiego della forza da parte di chi può fare uso di sistemi d'arma autonomi invece che di uomini si abbasserebbe ulteriormente. Infine, la *proliferazione illecita di materiali, tecnologie e know-how* da parte di attori non statali illegittimi, come gruppi armati e terroristi, riceverebbe un ulteriore impulso.

In conclusione

Ai presenti è apparso ormai sempre più chiaro che il cambiamento degli scenari e dei teatri di confronto è sempre più complesso e interconnesso con il mondo civile e la relativa digitalizzazione. Ciò favorisce *l'integrazione degli ufficiali riservisti* (nel caso svizzero di milizia) nei processi di presa di conoscenza, concezione e applicazione. Infatti le esperienze giornalmente raccolte trovano sempre più spazio e opportunità per fornire importanti indicazioni a certe cerchie del mondo militare ritenuto – in generale a livello europeo – ancora troppo orientato al confronto simmetrico-cinetico tradizionale. ◆





Riferimenti

www.ccdcoe.org/cyber-security-strategy-documents.html
www.ccdcoe.org/national-cyber-security-organisation.html

ICRC [Comitato internazionale della Croce Rossa], *Ethics and autonomous weapon systems: an ethical basis for human control?*, UN-CCW/GGE.1/2018/WP.5, pubblicato il 29 marzo 2018 e discusso il 13 aprile 2018 a Ginevra presso le Nazioni Unite nell'ambito del Group of governmental experts of the high contracting parties to the convention on prohibitions or restrictions on the use of certain conventional weapons which may be deemed to be excessively injurious or to have indiscriminate effects.