

FOCUS DIFESA

CYBER

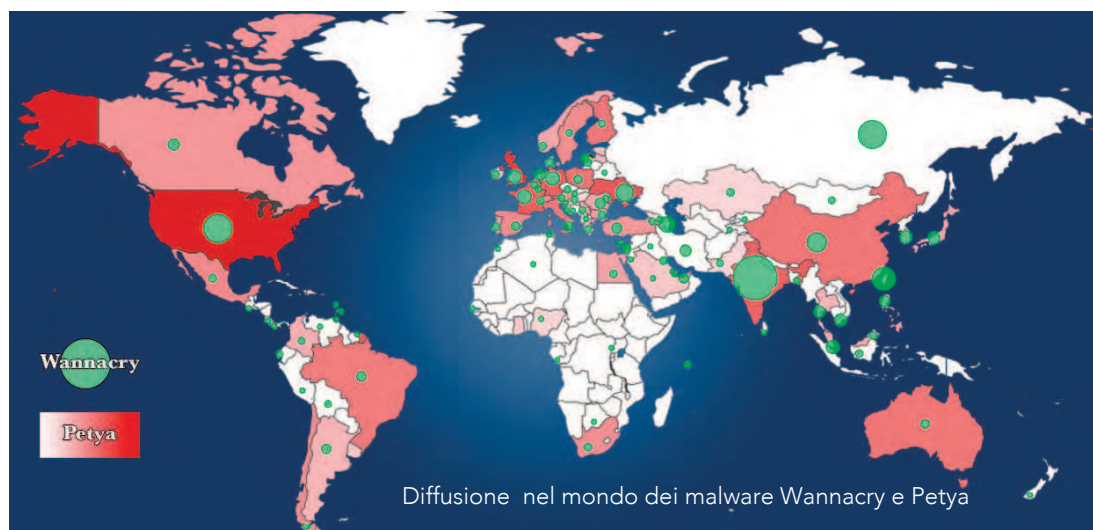
The background of the page is a dark, textured surface. Overlaid on this is a stylized world map made of small, glowing red and white squares. A network of red lines with small dots at the intersections is superimposed over the map, suggesting global connectivity or data flow. In the background, there are faint, larger-scale patterns of binary code (0s and 1s) in a reddish-pink hue.

DEFENCE

Nasce il
Comando Interforze
per le Operazioni Cibernetiche



*Intervista al
Capo di Stato Maggiore della Difesa
Generale Claudio GRAZIANO*



Nelle scorse settimane nel mondo si sono verificati attacchi cyber di larga scala (Wannacry e Petya), la cui frequenza è in crescita: siamo in un nuovo campo di battaglia? “La minaccia cibernetica sta assumendo un crescente rilievo in forma direttamente proporzionale alla dipendenza informatica assunta dai paesi tecnologicamente più avanzati. Sin dai primi anni 2000 si è registrata la condotta di operazioni cibernetiche. Un attacco cibernetico di alto profilo, condotto da un organismo statale o addirittura multinazionale, può creare dei danni assolutamente elevati. Da un punto di vista militare, oggi lo spazio cibernetico – che è un dominio trasversale a quelli tradizionali (terrestre, marittimo, aereo e spaziale) caratterizzato da mancanza di geospecificità, e limitate capacità di attribuzione - rappresenta quindi un vero e proprio teatro di operazioni, con una novità: non è appannaggio esclusivo del-

le componenti militari, visto che trovano spazio anche organizzazioni e individui non necessariamente riconducibili ad entità statuali. Siamo di fronte a uno dei più efficaci metodi di lotta asimmetrica perché anche un singolo individuo può costituire una minaccia per lo Stato o soggetti come l'Unione Europea e la NATO”.

Che incidenza ha la dimensione cyber nel campo della tecnologia militare? “Ormai il 60% della nostra attività è cyber, se consideriamo l'elevato livello tecnologico che caratterizza gli assetti delle nostre Forze Armate. Ciò implica una esposizione che può impattare su diversi aspetti della sfera militare, come la gestione dei sistemi d'arma e le comunicazioni tattiche ed operative nel corso delle operazioni. In alcuni casi il livello tecnologico si riduce addirittura a un limitato intervento dell'uomo, come ad esempio per i velivoli senza pilota che seguono rotte pre-programmate. Tale progresso, che sicuramente è un punto di



Il Ministro Pinotti e il Generale Graziano al convegno
Il pericolo corre in rete - La nuova frontiera della minaccia cibernetica, Roma – giugno 2017.

vista irrinunciabile, dall'altro rappresenta un'enorme vulnerabilità di fronte alla potenzialità di una minaccia cibernetica. Un'ipotetica intrusione nei sistemi di comando e controllo finalizzata non solo allo spionaggio, ma anche al sabotaggio e al malfunzionamento, potrebbe nei casi peggiori portare a una perdita di controllo dei propri assetti, a un decadimento delle reti di comunicazione, a un'errata geolocalizzazione delle forze in campo, fino ad arrivare alla paralisi dei sistemi di comando e controllo. Tutto ciò comprometterebbe l'esito di una campagna, di un'operazione, e sicuramente metterebbe in pericolo il nostro personale, generando effetti che si riverbererebbero sulla credibilità dell'operazione e sulla protezione delle forze".

Quali sono le contromisure adottate?

"La Difesa ha costituito un Comando Interforze per le Operazioni Cibernetiche (CIOC), in linea con gli obiettivi definiti sia in ambito europeo sia in ambito NATO

che comprendono la realizzazione di solide capacità di *cyber defence* e di protezione delle infrastrutture. Il CIOC - già operativo e proiettato verso la piena capacità nel 2019 - si basa su quattro fondamentali. Il primo è quello dell'organizzazione: personale, logistica, dottrina, operazioni e le varie componenti normali di un comando, in grado di proiettare i diversi elementi in operazione. Il secondo è costituito dalle infrastrutture, che devono disporre di sistemi protetti e prevedere anche - oserei dire - delle modalità d'azione protette, che dovranno man mano crescere anche nella cultura di tutela cibernetica. Il terzo elemento consiste nella realizzazione di una struttura per la formazione presso la Scuola telecomunicazioni delle Forze armate di Chiavari, dove ci saranno anche poligoni virtuali per l'addestramento alle operazioni *cyber*. Tale struttura opererà a favore degli ambienti interforze, interagenzia e interalleati e soprattutto in siner-



gia con il mondo accademico e quello industriale. Nella sede del CIOC vi è inoltre il *Cyber Lab*, che permetterà di acquisire gli strumenti necessari per effettuare lo studio dei *malware* e dei rimedi contro la minaccia, oltre a fornire supporto ai responsabili della progettazione, sviluppo e gestione delle reti, man mano che la minaccia viene identificata e neutralizzata. Il quarto elemento riguarda il personale: si ritiene infatti che più del 70 per cento della capacità generale di qualsiasi ambiente cibernetico dipenderà dall'abilità degli operatori. Questi andranno dunque attentamente selezionati e formati, traendo beneficio anche dal mondo accademico e della ricerca, e da altre realtà del comparto industriale nazionale. Sottolineo che la Difesa, nell'ambito delle capacità *cyber* che sta sviluppando sia per proteggere i suoi sistemi che per pianificare e condurre operazioni militari nel dominio *cyber*, in linea con il quadro normativo vigente è come sempre a disposizione del Paese, pronta a rendere disponibili in ogni momento le proprie capacità attuali e future per concorrere alla crescita della *cyber security* nazionale".

Cyber-Defence e partnership: quali le prospettive? Come l'Italia, tutti i principali Paesi e organizzazioni internazionali, compresa la NATO - che da questo punto di vista ha sempre rappresentato il motore -, si stanno dotando di strutture militari di comando e controllo per operare nel dominio cibernetico. Il Segretario generale Stoltenberg ha evidenziato un incremento del 60 per cento degli attacchi *cyber* alle strutture dell'Alleanza nel 2016, con una frequenza media di circa 500 attacchi al mese, la maggior parte dei quali non proverebbe da privati, ma da istituzioni statali di altri Paesi. Alla luce di questa preoccupante evoluzione e per affrontare la minaccia *cyber* la NATO continua a promuovere un approccio sinergico tra gli alleati e anche tra gli altri partner, puntando sul miglioramento delle capacità nazionali di difesa cibernetica, per contribuire al rafforzamento della difesa collettiva e alla sicurezza dello spazio euroatlantico. Da questo punto di vista le nostre strutture di *cyber-defence* si interfaceranno con le realtà analoghe dei Paesi amici e alleati, e in particolare con il Centro di Eccellenza della NATO di Tallinn in Estonia.

IL COMANDO INTERFORZE PER LE OPERAZIONI CIBERNETICHE - CIOC



Il recente riconoscimento del dominio *cyber* porterà molte nazioni ad avere dei comandi militari deputati alla sola condotta di operazioni cibernetiche, come ha fatto l'Italia secondo il Libro Bianco per la Difesa.

Il compito essenziale del Comando Interforze per le Operazioni Cibernetiche è quello di proteggere il sistema militare nei confronti della minaccia *cyber*, che capitalizza sulle dimensioni logica, tecnologica, fisica, sociale e ha una caratteristica fondamentale: quella della pervasività, ovvero di non avere confini e di non svelare quasi mai la vera identità e la vocazione dell'attaccante. Circa la minaccia va comunque fatto un discernimento tra ciò che è un attacco in termini di reato - ovvero un crimine per sottrarre dati, spionaggio, colpire, disturbare - da quello che può essere, e domani andrà misurato, un vero attacco militare al sistema nazionale.



Attualmente il Comando sta rinforzando la capacità in termini di *cyber security*, la difesa delle proprie reti e la tutela delle operazioni soprattutto nei teatri operativi all'estero, senza trascurare con ciò il territorio nazionale. Il focus è sulla tutela dei sistemi di comando e controllo, per assicurare un'efficiente condotta delle azioni sul campo, anche e soprattutto per tutelare la sicurezza delle forze impiegate.

La *cyber-security* rappresenta una grande opportunità per l'industria nazionale e anche per le università, chiamate a garantire la formazione superiore degli operatori *cyber*, la quale deve partire auspicabilmente già dalle scuole superiori specializzate in informatica. La Difesa dovrà affidarsi a bandi specifici per arruolare dal mondo civile gli operatori per i propri organici, oltre a contare sulle proprie risorse. Sarà sempre il fattore umano a fare la differenza, a parità di tecnologie disponibili.

Generale di B.A. Francesco Vestito, Comandante del CIOC
Colonnello Ferdinando Munno, Vice Comandante del CIOC



The Joint Cyber Command is born



**INTERVIEW WITH THE
CHIEF OF DEFENCE STAFF
General Claudio GRAZIANO**



Over the past weeks large-scale cyberattacks (Wannacry and Petya) have been carried out all over the world with increasing frequency: are we on a new battlefield?

Cyber threats are becoming more and more serious, commensurately with the digital dependency of more technologically advanced countries. Cyber-operations have been recorded since the early 2000s. A high-profile cyberattack carried out by

a state-based, or even multinational, organization can cause considerably severe damage. Cyberspace is a cross-cutting domain encompassing the traditional land, sea, air and space domains; it is characterized by a lack of geo-specificity and limited scope for attribution. From a military point of view, it is now an actual theatre of operations with a new feature: it does not exclusively pertain to military components as it also comprises organizations

and individuals that cannot be necessarily linked to nations. We are facing one of the most effective asymmetric warfare methods because an individual alone can pose a threat to a State or organizations such as the European Union or NATO”.

What is the impact of cyberspace on military technology? Considering the high technological standard of our Armed Forces’ assets, 60% of our activities is already cyber -based. This implies a potential impact on various aspects of the military domain, such as weapon system management and tactical and operational communications during operations. In some instances, the technological level entails limited human agency, as it is the case with unmanned aerial vehicles that fly programmed routes. While this represents a progression- and an essential one - it also determines vulnerability in the face of potential cyber threats. In the worst-case scenario, a violation of command and control systems - aimed not only at espionage but also at sabotage and malfunction - could supposedly cause losing control over assets and deterioration of communication networks, incorrect geolocalization of deployed forces, and even a breakdown of command and control systems. This could jeopardize a campaign - or an operation - and would certainly endanger our personnel, thus affecting the credibility of an operation and the protection of forces”.

What countermeasures have been adopted? Defence has created a Joint Cyber

Command (Comando Interforze per le Operazioni Cibernetiche - CIOC) consistently with the objectives that have been defined within both the EU and NATO, which include the creation of robust cyber defence and infrastructure defence capabilities.

The Joint Cyber Command is already running and will be achieving full operational capability in 2019. It rests on four cornerstones. The first one is organization, which comprises personnel, logistics, doctrine, operations and the various ordinary components of a headquarters with projection capabilities during an operation. The second cornerstone is info-structures, which must comprise protected systems and should rely - allow me to say - on protected operational modes to be developed in terms of cyber protection. The third cornerstone consists in creating a training organization within the Italian Armed Forces School of Telecommunications in Chiavari, where virtual firing ranges will be established with cyber operations training purposes. This organization shall work for joint, inter-agency and inter-allied bodies and, above all, synergically with both the academia and the industry. A Cyber Lab has been established at the Joint Cyber Command. The Lab is conceived to generate the tools required to study malware and face threats, and will support managers in charge of designing, developing and managing networks as a threat is being identified and neutralized. The fourth



element regards personnel. In fact, more than 70% of the overall capability of any cyber environment is supposed to depend on human skills. Therefore, operators should be carefully selected and trained, also through the support of academia and research, as well as other organizations within the national industry. Allow me to underline that Defence is invariably - and in compliance with the regulations in force - at the service of the nation when it comes to the cyber capabilities that are being developed to protect its own systems as well as plan and conduct military operations in the cyber domain. Defence is ready to make its own current and future capabilities available at any time in order to facilitate the development of national cyber security.

Cyber-Defence and international partnerships: what prospects are there? Like Italy, all main countries and international organizations, including NATO - which has always been the driving force in this

process - are developing military command and control structures to operate in the cyber domain.

Secretary General Stoltenberg has pointed out that the number of cyberattacks against Alliance structures has increased by 60% in 2016, with an average monthly frequency of approximately 500. Most of these attacks are not carried by private bodies, but by state bodies of other countries. Considering such worrying evolution and in order to cope with cyber threats, NATO continues to promote a synergic approach among both allies and other partners. This is done by relying on the improvement of national cyber defence capabilities in order to strengthen collective defence and security of the Euro-Atlantic region.

Our cyber defence structures will be interfacing with similar institutions of friendly countries and allies, and in particular with the NATO Centre of Excellence in Tallinn.

THE JOINT CYBER COMMAND

The recent acknowledgement of the relevance of the cyber domain will lead many nations to set up military commands exclusively in charge of conducting cyber operations, as Italy has done in compliance with the Defence White Paper. The fundamental task pertaining to the Joint Cyber Command is protecting the military system from cyber threats, which thrive on the logic, technological, physical and social dimensions. These threats have an intrinsic feature: they are pervasive. In fact, they have no boundaries and almost never reveal the real identity and intent of the attacker. However, a distinction should be drawn between what constitutes an attack in criminal terms – namely an offence for stealing data, spying, attacking, disrupting - and what is a real military attack on the national system, and will need to be assessed as such in the future.



At present, the Command is strengthening its cyber security capabilities, the defence of its own networks, and the protection of operations especially in theatres of operations abroad. This is all done without neglecting national territory and focussing on the protection of command and control systems in order to ensure that operations are effectively conducted on the field, especially to guarantee the safety of deployed forces. Cyber security provides a great opportunity for national industry and for universities, which are called upon to take charge of cyber operators' advanced training. This should desirably begin with IT-specialized high school education. Defence will have to recruit civilian operators through specific competitions, while still relying on its own resources. Available technologies being equal, the human factor will always make the difference.

B.Gen. Francesco Vestito - Commander
Col. Ferdinando Munno - Deputy Commander