TRADUZIONE
OTTOBRE 2017

UNIVERSITÀ DEGLI STUDI FIRENZE

OSCE: PROBLEMI DI IMPLEMENTAZIONE DELLE MISURE DI RAFFORZAMENTO DELLA FIDUCIA

DANIELA GIORDANO

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,

Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

OSCE: PROBLEMI DI IMPLEMENTAZIONE DELLE MISURE DI RAFFORZAMENTO DELLA FIDUCIA

Daniela Giordano

UNIVERSITÀ DEGLI STUDI FIRENZE

Traduzione

Ottobre 2017

RIGUARDO ALL'AUTRICE

Daniela Giordano si è laureata in Scienze Politiche presso l'università LUISS di Roma con una tesi sui fondamentalisti islamici in Arabia Saudita. Al momento sta concludendo il suo ciclo di studi con una Laurea Magistrale in Studi di Sicurezza Internazionale, programma congiunto tra la Scuola di Studi Superiori Sant'Anna e l'Università di Trento. Sta anche svolgendo un tirocinio presso l'Osservatorio Balcani Caucaso Transeuropa. Si interessa di cyber security e governance del cyber space. È responsabile della comunicazione e dei social network del Center.

OSCE: PROBLEMI DI IMPLEMENTAZIONE DELLE MISURE DI RAFFORZAMENTO DELLA FIDUCIA[1]

Guardando i dati dell'OSCE, circa 47 stati del mondo possiedono dei programmi militari cibernetici attivi, tra questi, 10 stati dispongono di cospicui budget militari o stanno sviluppando tecnologie cibernetiche offensive. È evidente che in queste circostanze, con l'incertezza dei meccanismi e degli accordi in campo ICT, si crea una seria minaccia per la sicurezza nazionale ed internazionale. L'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE) è una tra le maggiori piattaforme internazionali, all'interno della quale si conduce il lavoro per l'implementazione di misure miranti a rafforzare la fiducia (Confidence Building Measures_CBMs) nel cyberspazio. Si suppone che le misure di fiducia incrementeranno la trasparenza, miglioreranno la cooperazione, assicureranno la stabilità, ridurranno il rischio di attacchi cyber intenzionali e permetteranno di adottare decisioni soppesate.

Gli esperti dell'Istituto per i problemi della sicurezza dell'informazione dell'Università Statale di Mosca ed i rappresentanti dell'OSCE hanno discusso a lungo il problema dell'attuazione delle CBMs nel cyberspazio, a margine di un seminario scientifico, organizzato nell'ambito dell'Istituto della Statale di Mosca.

Nel 2013, come risultato di difficili negoziati, gli stati membri dell'OSCE hanno accettato il primo documento internazionale sulle CBMs nel cyberspazio per evitare situazioni di conflitto. Le undici misure, sulle quali i partecipanti dell'organizzazione sono riusciti a concordare, promuovono: lo scambio di best practices; azioni di consultazione con lo scopo di ridurre gli errori di comunicazione e la conseguente nascita di tensioni politiche o belliche; l'aumento della conoscenza e dell'informazione sull'accrescimento del potenziale in relazione all'uso sicuro dell'ICT; l'introduzione di norme legislative nazionali efficienti, che consentano di semplificare la collaborazione bilaterale e lo scambio efficiente e tempestivo di informazioni tra i dicasteri competenti,

[1] Testo originale in russo: https://interaffairs.ru/news/show/18594

compresi gli organi delle forze dell'ordine degli stati membri, con l'obiettivo di contrastare l'uso dell'ICT con fini terroristici o criminali, etc.

Nel febbraio del 2016, un secondo elenco di CBMs è stato deciso dagli stati membri dell'OSCE. Questo ha integrato il precedente documento di altri cinque punti. Tra le misure, si può evidenziare lo sviluppo di un partenariato pubblico-privato e di meccanismi di scambio di best practices in reazione alle sfide comuni di sicurezza, legate all'uso dell'ICT, come anche l'attuazione degli scambi intergovernativi in diversi formati, tra cui riunioni di lavoro, seminari e tavole rotonde, inclusi a livello regionale e/o sub-regionale. Bisogna dire che tutte le CBMs hanno carattere volontario.

In aggiunta a tutto ciò, nonostante tutti gli stati membri dell'organizzazione abbiano firmato i suddetti documenti, l'implementazione delle CBMs incontra numerosi ostacoli. Sembra che in questa questione i metodi tradizionali di collaborazione nel settore della sicurezza, per ora, non abbiano dato frutti. Per la soluzione a questi problemi, è necessaria la partecipazione di studiosi ed esperti - la cosiddetta diplomazia della 'seconda via'.

Dunque, nel 2016 un piccolo gruppo di lavoro dell'Università di Firenze (al quale in seguito si sono uniti esperti da altri centri accademici quali il Royal College, l'Università di Oxford, l'Università Tecnica del Brandeburgo, l'Università Politecnica di Cracovia Tadeusz Kościuszko, la MGIMO, etc) ha realizzato un'analisi dei problemi di realizzazione di queste misure di fiducia, che erano state adottate nel 2013. La metodologia dello studio includeva la raccolta di dati da fonti aperte e chiuse, sondaggi e la realizzazione di interviste ai rappresentanti dei governi dei paesi membri dell'OSCE. Il compito includeva anche capire esattamente quali problemi tecnici e pratici bloccassero la strada per la realizzazione delle misure e quali azioni pratiche fosse necessario intraprendere per far superare il punto morto a questo progetto.

Gli esperti hanno presentato i risultati del lavoro di ricerca dei gruppi in vari seminari scientifici, arrivando alle seguenti conclusioni: Innanzitutto, ci sono grandi differenze tra gli stati membri dell'OSCE nel loro livello di preparazione e di comprensione del problema della sicurezza informatica. Come ci si aspettava, i paesi del Nord America, ed anche dell'Europa Centrale e Settentrionale, hanno un livello più alto di coscienza del pericolo informatico, rispetto ai paesi del Caucaso Meridionale, dell'Asia Centrale e persino dell'Europa SudOccidentale. Di

conseguenza, in quei paesi dove non c'è una chiara consapevolezza sull'argomento, la sicurezza cibernetica non è all'ordine del giorno.

In secondo luogo, molti stati membri dell'associazione non sono informati in maniera dovuta su ciò che l'OSCE fa e su ciò che può offrire agli stati che sono interessati ad incrementare le proprie possibilità in ambito ICT.

In terzo luogo, tra gli stati membri vi è un'enorme differenza nella disponibilità di risorse tecnologiche, umane, finanziarie e scientifiche per un'implementazione efficace delle CBMs. Gli esperti hanno sottolineato che il maggior problema si nasconde nella scarsità di organico a diversi livelli (tanto nella sfera tecnologica, quanto nella sfera statale).

Sulla base di queste conclusioni, è stata accettata la decisione di passare alla prossima fase, vale a dire, proporre alcune raccomandazioni per risolvere i problemi esistenti. Adesso il gruppo di lavoro si occupa della creazione di meccanismi, che possano aiutare gli stati membri dell'OSCE nell'applicazione delle CBMs.

Bisogna dire che il gruppo di lavoro dell'Università di Firenze non è una struttura formale dell'OSCE, perciò tutte le raccomandazioni proposte saranno mandate al gruppo di lavoro intergovernativo per le questioni cibernetiche, che funziona invece nel quadro dell'OSCE. A seguito dei risultati della discussione è stato raggiunto un accordo sul proseguimento della cooperazione col fine di determinare le possibili forme e indicazioni della partecipazione dei rappresentanti dell'Istituto alla preparazione e alla realizzazione del Piano di lavoro per la formazione di un sistema di CBMs nell'ambito della sicurezza cibernetica e dell'uso sicuro di tecnologia della telecomunicazione. Il lavoro sull'implementazione delle CBMs nell'ambito dell'OSCE è un compito piuttosto complicato, tuttavia la sua soluzione sarà un passo importante sulla strada per la realizzazione della stabilità universale e della sicurezza nel mondo.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies