Cyber minacce (russe) e come affrontarle. La strategia Nato

Edoardo Sarti

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Research Analysis

Aprile 2020

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

Cyber minacce (russe) e come affrontarle. La strategia Nato

Edoardo Sarti

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

Aprile 2020

Riguardo all'autore

Edoardo Sarti collabora col Center for Cyber Security and International Studies dal giugno 2019. Ha conseguito la Laurea Magistrale in "Relazioni Internazionali e Studi Europei" presso la Scuola di Scienze Politiche "Cesare Alfieri" dell'Università degli Studi di Firenze con la tesi dal titolo "Il ruolo delle organizzazioni internazionali per la cooperazione nel cyberspazio un approccio costruttivista". Nel 2019 ha conseguito il corso di perfezionamento in "Intelligence e sicurezza nazionale" presso l'Università di Firenze. La sua attività di ricerca per il CCSIRS include le Relazioni Internazionali nel cyberspazio, la cyber-diplomacy e l'analisi delle politiche nazionali ed internazionali relative al cyberspazio e alle tecnologie emergenti.

Cyber minacce (russe) e come affrontarle. La strategia Nato[1]

Lo scorso 20 febbraio Stati Uniti, Regno Unito e altri paesi della Nato hanno pubblicamente condannato la Russia per il cyber-attacco che ha colpito la Georgia il 28 ottobre 2019. L'attacco, secondo quanto affermato dal Paese interessato[2], causando l'interruzione delle operazioni di siti governativi e privati e la trasmissione di alcune emittenti televisive, sarebbe stato rivolto a minare la sicurezza nazionale della Georgia, a danneggiare la popolazione e a interrompere il funzionamento delle agenzie governative.

L'attacco subito dalla Georgia, avvenuto pochi giorni dopo la pubblicazione[3] del "Nato-Georgia commission statement", in cui viene celebrato l'impegno di Tbilisi nell'offrire supporto alle operazioni e alle missioni Nato (in particolare alla *Nato Response Force* e alla *Resolute Support Mission*) e condannata l'attività destabilizzante della Russia nella regione, avrebbe ancora una volta, mostrato la volontà di Mosca di usare i cyber-attacchi come parte della propria strategia di *hybrid warfare* e la necessità per la Nato di rafforzarsi contro queste minacce.

L'*hybrid warfare* è definita[4] dalla Nato come l'impiego di strumenti militari e non-militari e di mezzi segreti e non, quali la disinformazione,

[1] La seguente analisi è apparsa su Formiche.net il giorno 11 aprile 2020 ed è reperibile al seguente link: https://formiche.net/2020/04/cyber-russia-nato-strategia/.

[2] Ministry of Foreign Affairs of Georgia, https://mfa.gov.ge/.

[3] Nato, "Nato-Georgia Commission Statement", 3 ottobre 2019, https://www.nato.int/cps/en/natohq/official_texts_169323.htm?selectedLocale=en.

[4] Nato, "Nato response to hybrid threats", 8 agosto 2019, https://www.nato.int/cps/en/natohq/topics_156338.htm.

i cyber-attacchi, la pressione economica e l'uso di gruppi armati irregolari, per confondere le linee tra guerra e pace e seminare il dubbio nella mente delle popolazioni bersaglio per destabilizzarle e ottenere un vantaggio politico. Nel corso degli ultimi anni la Russia si sarebbe dimostrata molto abile nell'utilizzo di questi metodi, soprattutto attraverso l'azione di gruppi non statali, che le hanno permesso di condurre operazioni militari, come in Ucraina nel 2014, o di interferire nelle elezioni politiche di altri paesi, come in quelle americane del 2016, garantendo però a Mosca una certa "*deniability*".

Nel contesto della *hybrid warfare*, il cyberspazio sarebbe stato sfruttato dalla Russia soprattutto come strumento di *information warfare* per la propaganda, la manipolazione, la distorsione di informazioni e la diffusione di fake news e come *warfare domain* per condurre operazioni di spionaggio, di furto o manipolazione di dati e di cyber-attacchi per danneggiare o distruggere infrastrutture critiche o assetti operativi degli Stati avversari.

Dunque, anche il cyber-attacco contro la Georgia sembrerebbe essere parte di questa campagna ibrida di Mosca che mira ad influenzare le scelte politiche degli altri paesi senza intervenire con mezzi convenzionali, poiché anche in questo caso, come affermato dal Segretario di Stato americano Mike Pompeo, l'obiettivo russo era quello di "creare insicurezza e indebolire le istituzioni democratiche" di un paese, la Georgia, divenuto sempre più rilevante dal punto di vista strategico sia per la Russia che per la Nato nel loro confronto nella regione.

Lo sfruttamento del cyberspazio da parte di attori, statali o non statali, per condurre operazioni offensive ha spinto i paesi alleati ad elaborare nuove strategie che favorissero un adattamento della Nato alle nuove minacce, in particolare a quelle cibernetiche, poste alla

sicurezza collettiva. Questo processo di adattamento è partito col Summit di Praga del 2002[5], quando è stata per la prima volta riconosciuta la necessità di dare avvio a tale processo anche attraverso l'elaborazione di misure che rafforzassero le difese degli Stati contro i cyber attacchi.

Dal 2002 ad oggi, la strategia della Nato nel cyberspazio si è progressivamente evoluta dalla "semplice" difesa delle infrastrutture critiche dell'Organizzazione e dei singoli paesi. Oggi l'obiettivo della Nato nel cyberspazio è riassumibile con la triade "*prepare, deter and defence*". Il primo obiettivo consiste nell'accrescere la consapevolezza dei paesi membri sulle minacce poste dal cyberspazio, sull'individuazione delle minacce e sul rafforzamento della resilienza degli Stati in caso di attacco. Ciò è stato perseguito, secondo quando stabilito con l'*Enhanced Nato Policy on Cyber Defence*, attraverso: la creazione di *Rapid Reaction Teams* sulla base di MoU firmati tra la Nato e ciascun Paese membro per assisterli in caso di necessità o attacco; lo sviluppo a livello nazionale del *Nato Defence Planning Process*, con cui la Nato identifica le capacità necessarie per armonizzare le difese nazionali e ne favorisce l'adozione; la creazione di partnership strategiche con gli alleati, come nel caso del *Technical Arrangement on Cyber Defence* con l'UE, e con il settore privato attraverso il *Nato Industry Cyber Partnership* per rafforzare la sicurezza della supply chain della difesa dell'Organizzazione.

Invece, per rafforzare le capacità di deterrenza e di difesa dell'Organizzazione nel cyber spazio, i paesi della Nato hanno sancito, nel 2014, l'applicabilità, anche in questo dominio, dell'articolo 5 del Trattato di Washington, che prevede l'assistenza collettiva degli

[5] Nato, "The Prague Summit and Nato's transformations", Brussels, 2003, https://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf.

Stati a un Paese alleato qualora esso sia vittima di un attacco armato, e nel 2016 il riconoscimento del cyberspazio come un dominio operazionale (al pari di terra, mare, aria e spazio) impegnando così i paesi a dotare l'Alleanza di capacità organizzative e tecniche necessarie non solo per proteggersi ma anche per sfruttare il cyber spazio per condurre operazioni militari in tutti gli altri domini, secondo quanto stabilito dagli Stati nel *Cyber Defence Pledge*[6].

Sebbene dunque la responsabilità primaria di rispondere ai cyber-attacchi e alle minacce ibride spetti sempre allo Stato vittima, la Nato nel corso degli anni ha dimostrato di aver sviluppato strumenti importanti per rafforzare le proprie difese. Tuttavia, come dimostrato dalla costante attività offensiva di numerosi attori internazionali nel dominio cibernetico, le infrastrutture dei paesi membri o di quelli alleati non sono del tutto al sicuro dagli attacchi degli attori malevoli. Per questo la migliore risposta agli attacchi che mirano a creare insicurezza, a destabilizzare le popolazioni dei paesi euro-atlantici e a indebolire le istituzioni democratiche è mostrare l'unità dell'organizzazione nel difendersi da queste minacce sia attraverso il rafforzamento delle capacità nazionali che di quelle collettive e nel rispondere in modo congiunto ai paesi aggressori, soprattutto ora che le investigazioni sembrano poter garantire "un elevato livello di probabilità" (espressione utilizzata dallo UK National Cyber Security Centre nell'attribuire al GRU, il servizio di intelligence militare russo, il cyber-attacco subito dalla Georgia il 28 ottobre 2019) nell'attribuzione dei cyber-attacchi, così da disincentivare gli altri Stati dal condurre operazioni offensive nel cyberspazio e garantire la sicurezza e la stabilità dei paesi membri.

[6] Nato, Cyber Defence Pledge", 8 luglio 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en.

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