https://www.geopolitika.ru
19.11.2021

La vera zona grigia di Leonid Savin

Nelle relazioni internazionali contemporanee, è stato utilizzato attivamente di recente un concetto come una "Zona Grigia". Inizialmente, questo termine è nato come costrutto teorico nelle Forze per le operazioni speciali del Pentagono, per poi svilupparsi nelle comunità politico-militari degli Stati Uniti (USA).

Di solito, il concetto di Zona Grigia viene utilizzato come indicatore per gli oppositori degli Stati Uniti e dell'Organizzazione del Trattato del Nord Atlantico (NATO). Ma anche altri Stati hanno utilizzato attivamente questo concetto negli ultimi anni, spesso sottintendendo qualcosa di diverso e vicino alla propria situazione politico-militare, all'agenda attuale e al contesto geostrategico.
Tenendo conto dell'enorme potenziale delle risorse informative e degli scienziati che servono gli interessi dell'Occidente, si dovrebbe riconoscere che la loro propaganda della Zona Grigia è molto efficace. Pertanto, gli autori occidentali fanno spesso dichiarazioni irresponsabili legate ad interessi politici e dirette contro altri Paesi. Una di queste aree è la sfera cibernetica.
Ci sono molti rapporti sui cosiddetti attacchi informatici russi (cinesi ma anche iraniani) nei media occidentali e nei rapporti dei gruppi di riflessione. Le pubblicazioni sono ben progettate e talvolta includono citazioni [1] di autori russi e documenti dottrinali e strategici russi.
Ma c'è un problema serio con esso: la mancanza di prove reali degli attacchi informatici russi. In altre parole, qualsiasi attività informatica illecita può essere presentata da autori occidentali (e purtroppo anche da Paesi neutrali e persino amici di altre regioni) come "operazioni russe".
Naturalmente, esiste un vero problema di diversi tipi di crimini informatici. Le tecnologie emergenti, tra cui l'intelligenza artificiale, l'informatica quantistica e le criptovalute, comportano maggiori rischi per tutti gli Stati e i loro cittadini. Le cause includono l'assenza di regolamenti internazionali per tali attività e le diverse posizioni degli Stati e un enorme divario nelle opportunità tecnologiche.

"Cyber" è la vera Zona Grigia, nonostante gli sforzi per usare questo termine per l'attività degli attori statali. E ci sono rischi elevati anche per i Paesi sviluppati. Siamo tutti all'interno di questa Zona Grigia globale. Le tendenze attuali mostrano una crescita dei crimini informatici [2] nei settori pubblico e privato nel mondo.

Con questa consapevolezza, la Russia è stata la prima a sollevare presso la principale piattaforma negoziale del pianeta - l'ONU - la questione dello sviluppo, sotto i suoi auspici, di un meccanismo pratico incentrato sui crimini nel campo dell'uso delle tecnologie informatiche, volto a combattere tali crimini e con un contenuto completo. Il messaggio principale è “ammassare” i cybercriminali con tutto il mondo, complicare seriamente le attività degli intrusi e non lasciare loro scappatoie per sfuggire alla giustizia, anche se la catena degli eventi coinvolge la giurisdizione di più Stati con ordinamenti giuridici diversi da regioni diverse del pianeta. Tenendo conto del fatto che la Convenzione delle Nazioni Unite contro la Corruzione e la Convenzione delle Nazioni Unite contro la Criminalità Organizzata Transnazionale hanno percorso un percorso simile, la creazione di una convenzione universale sulla lotta all'informazione e ai crimini informatici è percepita positivamente.
Tuttavia, in un primo momento, questa idea ha incontrato una seria opposizione da parte degli Stati occidentali, che da quasi vent'anni promuovono strenuamente la Convenzione del Consiglio d'Europa sui Crimini Informatici del 2001, meglio nota come Convenzione di Budapest, come una sorta di “gold standard” in questo settore. Sessantacinque Stati sono diventati suoi partecipanti. La Russia e la maggior parte degli Stati membri delle Nazioni Unite non hanno firmato questa convenzione a causa delle sue gravi carenze, le principali delle quali sono il numero ridotto di crimini (9 in totale), la mancanza di statistiche ufficiali di applicazione e l'alto rischio di violare il principio della sovranità statale, dei diritti umani e delle libertà fondamentali dello Stato parte di questa convenzione con il pretesto di combattere la criminalità informatica (articolo 32b sull'accesso transfrontaliero alle informazioni).
Allo stesso tempo, gli apologeti della Convenzione di Budapest hanno a lungo bloccato ogni discussione in sede ONU sullo sviluppo di standard uniformi in questo settore, affermando che non c'è alternativa alla visione. Il risultato di ciò è stato l'emergere di iniziative e meccanismi legislativi locali in vari Paesi del mondo, la frammentazione della cooperazione internazionale e, di conseguenza, un forte aumento delle azioni illegali nella sfera dell'informazione.
La Russia è stata in grado di invertire questa tendenza negativa offrendo alla comunità internazionale l'idea di creare una piattaforma negoziale a tutti gli effetti per lo sviluppo della prima convenzione informatica delle Nazioni Unite. Il risultato di ciò è stata l'istituzione con risoluzione dell'Assemblea generale delle Nazioni Unite 74/247 del 27 dicembre 2019 di un comitato intergovernativo speciale di esperti sullo sviluppo sotto gli auspici delle Nazioni Unite di una convenzione internazionale globale sul contrasto all'uso di tecnologie dell'informazione e cibernetiche a fini criminali (di seguito – il Comitato Speciale). Quarantasette Stati sono diventati coautori del documento.

Nel 2021, la Russia è riuscita a fare un passo avanti in questa direzione.

> Questo è stato un serio risultato diplomatico nella direzione della lotta alla criminalità informatica e la prova che la Russia sta dando un contributo significativo alla lotta contro di essa.

Gli esperti delle forze dell'ordine e i diplomatici degli Stati membri delle Nazioni Unite dovranno effettivamente sviluppare una convenzione globale con la partecipazione di tutte le parti interessate entro 2 anni e sottoporla all'esame e all'approvazione dell'Assemblea generale delle Nazioni Unite nel 2023-2024 durante la sua 78a sessione. A tal fine, il Comitato Speciale terrà 7 sessioni sostanziali: 4 a New York, 3 a Vienna. Il primo incontro è previsto per il 17-28 gennaio 2022.
La Russia ritiene che per alcuni partecipanti alla Convenzione di Budapest, la prospettiva di avere due documenti contemporaneamente – universale e regionale – non sia un problema, al contrario, apparirà una gamma più ampia di strumenti per le forze dell'ordine per trovare, detenere e condannare criminali informatici. Pertanto, c'è la possibilità di raggiungere un compromesso sul documento finale durante i negoziati.

Nato

[1] https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf
[2] https://www.embroker.com/blog/cyber-attack-statistics/
****

Articolo originale di Leonid Savin:
https://www.geopolitica.ru/en/article/real-grey-zone
Costantino Ceoldo