SENATO DELLA REPUBBLICA

XIX LEGISLATURA

Doc. XII-*quater*
n. 3

ASSEMBLEA PARLAMENTARE DELLA NATO

Dichiarazione n. 475

Rafforzare la resilienza informatica delle società alleate

Trasmessa il 20 dicembre 2022

NATO PARLIAMENTARY ASSEMBLY

RESOLUTION n. 475

Strengthening the cyber resilience of allied societies [1]

THE ASSEMBLY,

1. *Acknowledging* the essential contribution of digital technologies to the functioning, well-being, cohesion and security of Allied societies;

2. *Concerned* about the growth, sophistication and increasingly destabilising impact of malicious cyber activities targeting all sectors, including public services, private companies and democratic institutions;

3. *Commending* efforts made in recent years by Allies and NATO to enhance their capacity to prevent, deter and counter malicious cyber activities; and *welcoming* the emphasis on combatting the latter and commitments made in NATO's new Strategic Concept;

4. *Alarmed* by the aggressive and irresponsible behaviour of authoritarian states in cyberspace; and *concerned* by the multiplication and diversification of malicious non-state cyber actors, their objectives and their techniques;

5. *Strongly denouncing* the unacceptable proliferation of malicious cyber activities against critical civilian infrastructure in Ukraine before and during Russia's new illegal and unprovoked invasion of the country, and *recognising* the importance of Allied support to Ukrainian authorities in thwarting them;

6. *Reaffirming* that Allies have a duty to maintain and strengthen their national cyber resilience and that NATO can provide support in this regard, notably through the Cyber Defence Pledge;

7. *Stressing* that NATO has recognised cyberspace as an operational domain; and *reiterating* the possibility for the North Atlantic Council to decide, on a case-by-case basis, when a cyber-attack would lead to the invocation of Article 5;

8. *Reaffirming* the crucial role of partnerships in combatting cyber threats that defy borders, and *welcoming* the extensive and effective cooperation between NATO and the European Union (EU) in this area;

9. *Recalling* that enhancing the cyber security of Allied societies cannot be achieved at the cost of undermining the democratic freedoms, rights and principles that underpin them;

10. *Noting* that the international community has recognised the applicability of international law in cyberspace, and *reiterating* the Alliance's commitment to its observance in order to promote a free, open, peaceful and secure cyberspace;

11. *URGES* the member governments and parliaments of the North Atlantic Al-

(1) Presented by the Committee on Democracy and Security and adopted by the Plenary Assembly on Monday 21 November 2022.

liance and, where appropriate, NATO bodies:

a. to swiftly implement agreed-on common policies, notably the Cyber Defence Pledge, the Comprehensive Cyber Defence Policy and the new Strategic Concept;

b. to enhance cyber deterrence and defence capabilities:

i. by being transparent about their action doctrines;

ii. by consolidating their ability to quickly and effectively coordinate their responses, in particular concerning attribution, to cyber activities while respecting Allies' national competence;

iii. by reserving the right to voluntarily adopt joint measures against perpetrators of cyber operations below the threshold at which they would be considered armed attacks warranting a military response;

iv. by taking action and developing cyber capabilities – including, at the national level, offensive capabilities – and greater interoperability to enable Allies to impose significant costs on perpetrators for their malicious cyber activities;

c. to deepen understanding of cyber threats, intelligence sharing and research, for example through the creation of dedicated applications for the general public, and to invest in network security in order to better prepare for and thwart malicious cyber activities;

d. to strengthen national policies and legal frameworks for combatting cyber threats and to continue working towards the development and implementation of international standards for responsible behaviour in cyberspace;

e. to intensify cooperation with relevant international organisations, notably the EU, partner countries, industry and academia, in particular by consolidating the exchange of information and best practices;

f. to raise awareness among all societal actors of their individual role in collective cyber resilience; to deepen collaboration with all private sector actors; and to strengthen civil-military cooperation in the cyber domain;

g. to maintain and increase support for partner countries facing cyber risks, in particular Ukraine, in order to counteract the irresponsible malicious cyber activities against the latter in the context of Russia's escalating war of aggression;

h. to pursue and strengthen the regular organisation of exercises and training involving all the actors concerned, aimed at identifying their cyber vulnerabilities and testing and developing their individual and collective capacity to react to and recover from malicious cyber activities;

i. to ensure that parliaments, civil society and the public have all the information and means necessary to monitor measures aimed at enhancing cyber security to make sure that these do not infringe on democratic values or individual rights.

ASSEMBLEA PARLAMENTARE DELLA NATO

RISOLUZIONE n. 475

Rafforzare la resilienza informatica delle società alleate

L'Assemblea,

1. *riconoscendo* il contributo essenziale delle tecnologie digitali al buon funzionamento, al benessere, alla coesione e alla sicurezza delle società alleate;

2. *preoccupata* dall'aumento, dalla sofisticazione e dall'impatto sempre più destabilizzante delle attività informatiche malevole che colpiscono tutti i settori, compresi i servizi pubblici, le aziende private e le istituzioni democratiche;

3. *elogiando* gli sforzi profusi negli ultimi anni dagli Alleati e dalla NATO per rafforzare la loro capacità di prevenire, scoraggiare o contrastare le attività informatiche malevole e *accogliendo con favore* il risalto dato alla lotta contro di esse e gli impegni assunti nell'ambito del nuovo Concetto strategico della NATO;

4. *allarmata* dal comportamento aggressivo e irresponsabile di Stati autoritari nel cyberspazio e *preoccupata* per il moltiplicarsi e diversificarsi dei soggetti informatici malevoli non statali, dei loro obiettivi e delle tecniche da essi impiegate;

5. *denunciando con forza* l'inaccettabile proliferazione delle attività informatiche malevole contro infrastrutture civili critiche in Ucraina prima e durante la nuova invasione illegale e non provocata del Paese da parte della Russia, e *riconoscendo* l'importanza del sostegno fornito dagli Alleati alle autorità ucraine nel contrasto a tali azioni;

6. *ribadendo* che gli Alleati hanno il dovere di mantenere e potenziare la loro resilienza informatica nazionale e che la NATO può fornire sostegno a tale riguardo, specie attraverso il Cyber Defence Pledge [Impegno per la difesa informatica];

7. *sottolineando* che la NATO ha riconosciuto il cyberspazio quale area operativa e *riaffermando* che il Consiglio Nord Atlantico può decidere, valutando caso per caso, quando un attacco informatico possa determinare l'invocazione dell'art. 5;

8. *ribadendo* il ruolo cruciale dei partenariati nella lotta a minacce informatiche che non conoscono frontiere, e *plaudendo* all'ampia ed efficace cooperazione tra la NATO e l'Unione europea (UE) in tale campo;

9. *ricordando* che il rafforzamento della sicurezza informatica delle società alleate non può essere ottenuto mettendo a repentaglio le libertà, i diritti e i principi democratici su cui esse si fondano;

10. *rilevando* che la comunità internazionale ha riconosciuto l'applicabilità del diritto internazionale al cyberspazio, e *riaffermando* l'attaccamento dell'Alleanza al suo rispetto al fine di favorire un cyberspazio libero, aperto, pacifico e sicuro;

11. *ESORTA VIVAMENTE* i governi e i Parlamenti dei Paesi membri dell'Alleanza atlantica e, se del caso, gli organi della NATO a:

a. attuare celermente le politiche comuni concordate, tra cui il Cyber Defence Pledge [Impegno per la difesa informatica], la Comprehensive Cyber Defence Policy [Politica globale di difesa informatica] e il nuovo Concetto strategico;

b. rafforzare le loro capacità di deterrenza e difesa informatiche:

i. dando prova di trasparenza in merito alle loro dottrine operative;

ii. consolidando la loro capacità di coordinare con rapidità ed efficacia le loro risposte alle attività informatiche malevole, specie per quanto attiene all'attribuzione nel rispetto della competenza nazionale degli Alleati;

iii. riservandosi il diritto di adottare, su base volontaria, misure collettive contro gli autori di operazioni informatiche al di sotto della soglia sopra la quale sarebbero considerate attacchi armati tali da giustificare una risposta militare;

iv. prendendo misure e sviluppando capacità informatiche – anche, a livello nazionale, di natura offensiva – nonché una maggiore interoperabilità per consentire agli Alleati di infliggere costi significativi agli autori di tali attività informatiche malevole;

c. approfondire la comprensione delle minacce informatiche, la condivisione delle informazioni e la ricerca, ad esempio tramite lo sviluppo di applicazioni destinate al vasto pubblico, e investire nella sicurezza delle reti per prepararsi meglio alle attività informatiche malevole ed essere in grado di sventarle;

d. rafforzare le politiche e i quadri giuridici nazionali che regolano la lotta alle minacce informatiche e continuare a lavorare allo sviluppo e all'attuazione di norme internazionali che favoriscano comportamenti responsabili nel cyberspazio;

e. intensificare la cooperazione con le organizzazioni internazionali interessate, segnatamente l'UE, i Paesi partner, l'industria e il mondo accademico, in particolare rafforzando lo scambio di informazioni e di buone pratiche;

f. far prendere coscienza a tutti i soggetti sociali del ruolo di ciascuno nella resilienza informatica collettiva, approfondire la collaborazione con tutti gli attori del settore privato e rafforzare la cooperazione civile-militare in campo informatico;

g. mantenere e aumentare il sostegno ai Paesi partner che affrontano rischi informatici, e in particolare all'Ucraina, per contrastare le irresponsabili attività informatiche malevole di cui essa è fatta oggetto nel contesto della sempre più violenta guerra d'aggressione russa;

h. portare avanti e potenziare l'organizzazione periodica di esercitazioni e programmi di formazione che coinvolgano tutti i soggetti interessati e puntino a individuare le loro vulnerabilità informatiche e a collaudare e approfondire la loro capacità individuale e collettiva di reagire ad attività informatiche malevole e venirne a capo;

i. fare in modo che i Parlamenti, la società civile e l'opinione pubblica dispongano di tutte le informazioni e i mezzi necessari per monitorare le misure di rafforzamento della sicurezza informatica, al fine di garantire che esse non ledano i valori democratici e i diritti individuali.

PAGINA BIANCA

PAGINA BIANCA

190124019010