ATTI PARLAMENTARI

XVI LEGISLATURA

CAMERA DEI DEPUTATI

Doc. XII-*quater*
n. 21

ASSEMBLEA PARLAMENTARE DELLA NATO

Risoluzione n. 387
La sicurezza cibernetica

Trasmessa il 17 ottobre 2011

TIPOGRAFIA DEL SENATO

RESOLUTION 387

on

CYBER SECURITY*

The Assembly,

1. ***Recognising*** the benefits offered by the cyber domain to our societies as well as to the defence and security sector, including opportunities for greater situational awareness and co-ordination among the armed forces of the Allies as well as for the Alliance's public diplomacy;

2. But also ***concerned*** with the emergence of a new category of threats that target national information infrastructures, and that could seriously undermine the security interests of the Alliance and its member states;

3. ***Anxious*** that cyber defence capabilities and awareness of cyber threats vary significantly across NATO member states thereby weakening the Alliance's overall cyber security;

4. ***Welcoming*** the decisions made by the leaders of the Alliance at the NATO Lisbon Summit and the meeting of NATO Defence Ministers in June 2011, identifying cyber security as one of the key priorities of the Alliance;

5. ***Welcoming*** the recent start of the procurement process to pursue full operational capability for the new NATO Policy on Cyber Defence, which will result in significantly higher levels of protection of the Alliance's networks;

6. ***Saluting*** NATO's approach aimed at expanding its cyber defence policy to include centralised cyber protection of all NATO bodies and the use of NATO's defence planning processes in the development of the Allies' cyber defence capabilities;

7. ***Believing*** that, in view of the growing scope and severity of cyber attacks, in addition to exploiting fully the opportunities offered by Article 4, the potential application of Article 5 of the Washington Treaty in case of a serious cyber attack against the Alliance or its individual members, should not be ruled out;

8. ***Noting*** that legislative "black holes" still exist both at a national level and in terms of international law when it comes to setting security standards for the cyber domain;

---

* Presented by the Committee on the Civil Dimension of Security and adopted by the Plenary Assembly on Monday 10 October 2011, Bucharest, Romania.

9. ***Emphasising*** that stricter security regulations for the cyber domain should not come at the cost of reduced civil liberties and rights, such as freedom of speech and the right to communicate over the Internet, and ***noting*** the key role of the Internet in mobilising democratic movements in authoritarian countries;

10. **URGES** member governments and parliaments of the North Atlantic Alliance:

a. to ensure swift implementation of the revised NATO Policy on Cyber Defence and the related cyber defence Action Plan, adopted in June 2011, introducing the cyber dimension in all three of NATO's core tasks: collective defence, crisis management and co-operative security;

b. to promote domestic awareness of cyber threats, taking into account lessons learned from milestone events including the cyber attacks against Estonia in 2007 and against Georgia in 2008 as well as the emergence of Stuxnet malicious software;

c. to scrutinize domestic legal frameworks, ensuring that coherent and effective laws are in place to address the evolving cyber threats;

d. to provide necessary support for the efficient functioning of national Computer Incident Response Teams, and to invest sufficiently in the training of national cyber security experts;

e. to promote closer partnerships between governments, the private sector and civil society organisations in order to ensure the security of government networks and improve the exchange of expertise in case of a breach of security;

f. to ensure that the introduction of additional security measures in the cyber domain are accompanied by adequate mechanisms of parliamentary and public oversight over their respective government institutions;

g. to support international efforts to develop universal norms of acceptable behaviour in the cyber domain against the use of cyber attacks on civilian targets, and that would promote exchange of best practices and establish mechanisms of international assistance to stricken nations, while ensuring full universal access to the Internet as a venue for the exchange of ideas and information;

h. to ensure that adequate attention is paid to the physical protection of networks, including undersea fibre-optic infrastructures;

11. **URGES** relevant NATO bodies:

a. to ensure that NATO Computer Incident Response Capability is fully operational by the end of 2012, and that NATO's cyber defence services are centralised;

b. to facilitate, if requested, national efforts of NATO member states to acquire adequate cyber defence expertise and state-of-the-art technologies;

c. to test the efficacy of NATO and member states' cyber defence efforts through NATO's periodic international exercises, and to ensure that these exercises are fully funded, staffed and well-attended;

d. to use capabilities such as NATO Cyber Defence Management Board and NATO Co-operative Cyber Defence Centre of Excellence, to analyse rapid developments further in the cyber domain and to develop strategies for strengthening cyber defences across the Alliance, while exploiting the advantages of the information age through initiatives such as NATO Network Enabled Capability;

e. to develop further the existing co-operation mechanisms with the relevant EU institutions, with the particular aim of supporting the EU's legislative efforts to establish robust cyber security standards across the private sector;

f. to increase assistance, if requested, to NATO partner countries in the field of cyber security, particularly by sharing best practices and raising awareness of cyber threats.

RESOLUTION 387

sur

LA CYBERSECURITE*

L'Assemblée,

1. ***Reconnaissant*** les avantages qu'offre le domaine cybernétique pour nos sociétés ainsi que pour le secteur de la défense et de la sécurité, y compris les possibilités d'améliorer la prise de conscience de la situation et la coordination entre les forces armées des Alliés, ainsi que pour la diplomatie publique de l'Alliance ;

2. Mais également ***préoccupée*** par l'émergence d'une nouvelle catégorie de menaces dirigées contre des infrastructures informatiques nationales, qui pourraient gravement compromettre les intérêts de l'Alliance et de ses pays membres en matière de sécurité ;

3. ***Inquiète*** à l'idée que les capacités de cyberdéfense et la sensibilisation aux menaces cybernétiques varient considérablement d'un pays membre de l'OTAN à l'autre, affaiblissant ainsi la cybersécurité globale de l'Alliance ;

4. ***Se félicitant*** des décisions prises par les dirigeants de l'Alliance au Sommet de l'OTAN de Lisbonne et à la réunion des ministres de la Défense de l'OTAN en juin 2011, érigeant la cybersécurité au rang de priorité pour l'Alliance ;

5. ***Se félicitant*** du lancement récent du processus d'approvisionnement visant à se doter d'une capacité parfaitement opérationnelle pour la nouvelle Politique de l'OTAN sur la cyberdéfense, qui permettra à terme d'atteindre un niveau de protection des réseaux de l'Alliance nettement supérieur ;

6. ***Saluant*** l'approche de l'OTAN visant à élargir sa politique de cyberdéfense pour y intégrer la protection cybernétique centralisée de tous les organismes de l'OTAN et l'utilisation des processus de planification de défense de l'OTAN dans la mise au point des capacités de cyberdéfense des Alliés ;

7. ***Convaincue*** que, face à la gravité et à l'ampleur croissantes des cyberattaques, tout en tirant pleinement parti des possibilités qu'offre l'article 4, il ne faut pas écarter la possibilité de faire jouer l'article 5 du Traité de Washington en cas d'attaque cybernétique grave contre l'Alliance ou l'un de ses membres ;

---

* Présentée par la Commission sur la dimension civile de la sécurité et adoptée par l'Assemblée plénière le lundi 10 octobre 2011 à Bucarest, Roumanie.

8. ***Notant*** que des "trous noirs" juridiques existent toujours tant au niveau national qu'en droit international lorsqu'il s'agit de fixer des normes de sécurité pour le domaine cybernétique ;

9. ***Faisant valoir*** que la mise en place de règles plus strictes en matière de sécurité pour le domaine cybernétique ne doit pas se faire au prix d'une réduction des droits et des libertés civiles, comme la liberté d'expression et le droit de communiquer sur Internet et, ***notant*** le rôle central que joue Internet pour mobiliser les mouvements démocratiques dans les pays autoritaires ;

10. **INVITE INSTAMMENT** les gouvernements et les parlements des pays membres de l'Alliance atlantique :

a. à assurer la mise en œuvre rapide de la Politique révisée de l'OTAN sur la cyberdéfense et du Plan d'action cyberdéfense y afférent, adoptés en juin 2011, inscrivant la dimension cybernétique au cœur des trois tâches fondamentales de l'OTAN : la défense collective, la gestion de crise et la sécurité coopérative ;

b. à promouvoir la sensibilisation aux menaces cybernétiques au niveau national, en prenant en compte les enseignements tirés des événements marquants dont les cyberattaques contre l'Estonie en 2007 et contre la Géorgie en 2008 ainsi que l'apparition du logiciel malveillant Stuxnet ;

c. à passer en revue les cadres juridiques nationaux, s'assurant de l'existence de lois cohérentes et efficaces pour parer aux menaces cybernétiques en constante évolution ;

d. à fournir le soutien nécessaire au fonctionnement efficace des Equipes nationales d'intervention en cas d'incident informatique et à doter de fonds suffisants la formation d'experts nationaux en cybersécurité ;

e. à promouvoir des partenariats plus étroits entre les pouvoirs publics, le secteur privé et les organisations de la société civile en vue d'assurer la sécurité des réseaux gouvernementaux et d'améliorer l'échange de savoir-faire en cas de violation du système de sécurité ;

f. à veiller à ce que l'introduction de nouvelles mesures de sécurité dans le domaine cybernétique s'accompagne des mécanismes appropriés de contrôle parlementaire et public des organismes gouvernementaux correspondants ;

g. à appuyer les efforts internationaux visant à mettre en place des normes universelles de comportement acceptable dans le domaine cybernétique contre le lancement de cyberattaques à l'encontre des cibles civiles et qui encourageraient l'échange des meilleures pratiques et établiraient des mécanismes d'assistance internationale aux pays en difficulté, tout en assurant un accès universel sans réserve à Internet comme lieu d'échange d'idées et d'informations ;

h. à veiller à ce qu'une attention adéquate soit donnée à la protection physique des réseaux, y compris des infrastructures sous-marines à fibres optiques ;

11. **INVITE INSTAMMENT** les organismes de l'OTAN concernés :

a. à veiller à ce que la Capacité OTAN de Réaction aux Incidents Informatiques soit entièrement opérationnelle d'ici fin 2012 et à ce que les services OTAN de cyberdéfense soient centralisés ;

b. à faciliter, le cas échéant, les efforts déployés, au niveau national, par les Etats membres de l'OTAN pour acquérir des technologies de pointe et des compétences adéquates en matière de cyberdéfense ;

c. à mettre à l'épreuve les efforts déployés par l'OTAN et les Etats membres en matière de cyberdéfense via des exercices périodiques de l'OTAN au niveau international et à veiller à ce que ces exercices soient dotés des fonds et du personnel suffisants et jouissent d'un niveau de participation satisfaisant ;

d. à faire appel aux capacités de l'OTAN telles que l'Autorité de gestion de la cyberdéfense et le Centre d'excellence pour la cyberdéfense en coopération, pour analyser davantage les développements rapides qui interviennent dans le domaine cybernétique et pour mettre au point des stratégies de nature à renforcer la cyberdéfense dans tous les pays de l'Alliance, tout en tirant parti des avantages de l'ère de l'information grâce à des initiatives telles que la capacité réseaucentrique de l'OTAN ;

e. à renforcer les mécanismes de coopération existants avec les institutions compétentes de l'UE, notamment pour appuyer les efforts juridiques que déploie l'UE pour établir des normes rigoureuses de cybersécurité dans l'ensemble du secteur privé ;

f. à accroître, si nécessaire, l'assistance aux pays partenaires de l'OTAN dans le domaine de la cybersécurité, notamment en échangeant les meilleures pratiques et en les sensibilisant davantage aux cybermenaces.

N.B. Traduzione non ufficiale

RISOLUZIONE n. 387

su

LA SICUREZZA CIBERNETICA

Presentata dalla Commissione sulla dimensione civile della sicurezza e adottata dall'Assemblea plenaria
lunedì 10 ottobre 2011, Bucarest, Romania

L'Assemblea,

1. Riconoscendo i benefici offerti dal settore cibernetico alle nostre società nonché al settore della difesa e della sicurezza, incluse le possibilità di migliorare la conoscenza della situazione operativa e il coordinamento tra le forze armate degli Alleati nonché la diplomazia pubblica dell'Alleanza;

2. Ma altresì preoccupata dall'emergere di una nuova categoria di minacce dirette contro le infrastrutture informatiche nazionali, che potrebbero compromettere gravemente gli interessi dell'Alleanza e dei suoi Stati membri in materia di sicurezza;

3. Preoccupata dall'idea che le capacità di cyberdifesa e la consapevolezza delle minacce cibernetiche variano considerevolmente tra i paesi membri della NATO, indebolendo così la sicurezza cibernetica globale dell'Alleanza;

4. Accogliendo favorevolmente le decisioni assunte dai leader dell'Alleanza in occasione del Vertice NATO di Lisbona e della riunione dei ministri della difesa della NATO nel giugno 2011, che hanno collocato la sicurezza cibernetica tra le priorità fondamentali dell'Alleanza;

5. Accogliendo con favore il recente lancio del processo di approvvigionamento volto ad acquisire la piena capacità operativa della nuova Politica NATO di difesa cibernetica, che comporterà un significativo aumento dei livelli di protezione delle reti dell'Alleanza;

6. Encomiando l'approccio della NATO mirante ad ampliare la propria politica di sicurezza cibernetica per includervi la protezione cibernetica centralizzata di tutti gli organismi della NATO e l'utilizzo dei processi di pianificazione di difesa della NATO nella messa a punto delle capacità di cyberdifesa degli Alleati;

7. Persuasa che, in considerazione dell'ampiezza e della gravità crescente degli attacchi cibernetici, oltre a sfruttare pienamente le opportunità offerte dall'articolo 4, non bisogna

scartare la possibilità di applicare l'articolo 5 del Trattato di Washington in caso di grave attacco contro l'Alleanza o uno dei suoi membri;

8. Osservando che esistono tuttora "buchi neri" legislativi sia a livello nazionale sia in termini di diritto internazionale riguardo alla fissazione di norme di sicurezza per il settore cibernetico;

9. Sottolineando che l'adozione di norme più severe in materia di sicurezza per il settore cibernetico non deve comportare un prezzo in termini di riduzione dei diritti e delle libertà civili, come la libertà di espressione e il diritto di comunicare via Internet, e osservando il ruolo centrale di Internet nel mobilitare i movimenti democratici nei paesi autoritari;

10. SOLLECITA i governi e i parlamenti dei paesi membri dell'Alleanza atlantica:

a. ad assicurare la rapida attuazione della Politica rivista della NATO sulla cyberdifesa e il relativo Piano d'azione sulla cyberdifesa, adottati nel giugno 2011, che hanno inserito la dimensione cibernetica in tutti e tre i compiti fondamentali della NATO: difesa collettiva, gestione delle crisi e sicurezza cooperativa;

b. a promuovere la consapevolezza delle minacce cibernetiche a livello nazionale, tenendo conto degli insegnamenti tratti da avvenimenti decisivi come i cyberattacchi contro l'Estonia nel 2007 e contro la Georgia nel 2008 nonché la comparsa del malware Stuxnet;

c. a esaminare i quadri giuridici nazionali, accertandosi dell'esistenza di leggi coerenti ed efficaci per far fronte alle minacce cibernetiche in costante evoluzione;

d. a fornire il sostegno necessario per l'efficace funzionamento delle squadre nazionali di reazione agli incidenti informatici, e a investire sufficientemente nella formazione di esperti nazionali di cybersicurezza;

e. a promuovere partenariati più stretti tra i governi, il settore privato e le organizzazioni della società civile al fine di garantire la sicurezza delle reti governative e migliorare lo scambio di conoscenze specifiche in caso di violazione dei sistemi di sicurezza;

f. a garantire che l'introduzione di misure di sicurezza aggiuntive nel settore cibernetico sia accompagnata da adeguati meccanismi di controllo parlamentare e pubblico sui rispettivi organismi governativi;

g. a sostenere gli sforzi internazionali volti a mettere a punto norme universali di comportamento accettabile nel settore cibernetico contro l'uso di ciberattacchi su obiettivi civili, promuovano lo scambio di prassi ottimali e istituiscano meccanismi di assistenza internazionale a paesi in difficoltà, assicurando al tempo stesso accesso pieno e universale a Internet come luogo di scambio di idee e di informazioni;

h. ad assicurare che sia dedicata adeguata attenzione alla protezione fisica delle reti, comprese le infrastrutture sottomarine a fibre ottiche;

11. SOLLECITA gli organismi interessati della NATO:

a. a far sì che la Capacità di reazione agli incidenti informatici della NATO sia interamente operativa entro la fine del 2012 e che i servizi di cyberdifesa della NATO siano centralizzati;

b. a facilitare, se necessario, gli sforzi compiuti a livello nazionale dai paesi membri della NATO per acquisire tecnologie avanzate e competenze adeguate in materia di cyberdifesa;

c. a mettere alla prova l'efficacia degli sforzi della NATO e dei suoi Stati membri in materia di cyberdifesa tramite esercitazioni periodiche della NATO a livello internazionale e assicurare che tali esercitazioni possano contare su fondi e personale adeguati e su un livello di partecipazione soddisfacente;

d. a utilizzare capacità quali il Consiglio di gestione della cyberdifesa della NATO e il Centro di eccellenza per la cyberdifesa cooperativa della NATO per analizzare i rapidi sviluppi del settore cibernetico e per mettere a punto strategie atte a rafforzare la cyberdifesa in tutti i paesi dell'Alleanza, sfruttando al tempo stesso i vantaggi dell'era dell'informazione grazie a iniziative quali la Capacità di operare in rete della NATO (NEC);

e. a sviluppare ulteriormente meccanismi di cooperazione esistenti con le istituzioni competenti dell'UE, allo scopo specifico di sostenere gli sforzi legislativi compiuti dall'UE per stabilire norme rigorose in materia di cybersicurezza nel complesso del settore privato;

f. a incrementare, se necessario, l'assistenza ai paesi partner della NATO nel campo della sicurezza cibernetica, in particolare attraverso la condivisione delle prassi ottimali e la sensibilizzazione in materia di minacce cibernetiche.