CAMERA DEI DEPUTATI Doc. **XII-*ter*** N. **18**

ASSEMBLEA DELL'UNIONE DELL'EUROPA OCCIDENTALE ASSEMBLEA INTERPARLAMENTARE EUROPEA DELLA SICUREZZA E DELLA DIFESA

55ª Sessione ordinaria
(Parigi, 2-4 dicembre 2008)

Raccomandazione n. 831 [1]

Sulla guerra informatica (o ciber-guerra) [2]

Trasmessa il 31 dicembre 2008

L'Assemblée,

(i) Constatant l'importance croissante des réseaux informatiques et du réseau Internet dans l'organisation et le fonctionnement des sociétés européennes;

(ii) Constatant l'importance du secteur informatique et des réseaux informatiques pour l'économie en général (opérations bancaires, commerce, échanges d'informations économiques, par exemple);

(iii) Constatant les progrès technologiques accomplis dans ce domaine et les avantages de toutes sortes qui en découlent, des points de vue social, économique, culturel et politique;

(iv) Constatant l'informatisation croissante des dispositifs de défense nationaux, au niveau des structures de commandement et de contrôle (C2) et des équipements, jusqu'au soldat infocentré sur le théâtre des opérations;

(v) Considérant en conséquence que les réseaux informatiques et le réseau

(1) Adoptée par l'Assemblée le 3 décembre 2008, au cours de sa 3ème séance plénière.

(2) Exposé des motifs: voir rapport présenté au nom de la Commission de défense par M. Chope (Royaume-Uni, Groupe fédéré) et M. Tarmo Kõuts (Estonie, Groupe fédéré), rapporteurs, Document 2022.

Internet revêtent une dimension stratégique dont il est nécessaire d'assurer la sécurité aux niveaux public et privé;

(vi) Constatant que ces réseaux, de par leur conception initiale et leur caractère global, sont vulnérables à des actes de perturbation et de déstabilisation et qu'ils peuvent aussi être utilisés pour des actions de déstabilisation ou de désinformation ou pour des actes criminels, par exemple;

(vii) Considérant que toute réponse aux menaces sur les réseaux informatiques, publics et privés, doit aussi être globale et inclusive, faisant appel aux capacités gouvernementales, aux entreprises du secteur et à la société en général (les utilisateurs particuliers);

(viii) Considérant, du fait du caractère global du réseau Internet, qu'il est nécessaire de mettre en place des mécanismes de coopération internationale pour combattre la cybercriminalité et le cyberterrorisme, selon l'exemple de la Convention du Conseil de l'Europe sur la cybercriminalité;

(ix) Constatant les conséquences négatives des attaques informatiques généralisées dont l'Estonie a été victime en avril et mai 2007;

(x) Notant qu'en dépit de l'ampleur de ces attaques, les autorités estoniennes ont pu en atténuer les effets, les neutraliser et contre-attaquer de manière à fermer les sites informatiques à l'origine de certaines actions malveillantes;

(xi) Constatant que cette défense a été possible grâce à l'état de préparation des autorités estoniennes chargées de la défense informatique, lesquelles ont également bénéficié de l'assistance internationale fournie notamment par les Etats de l'OTAN;

(xii) Constatant cependant la difficulté à identifier et à appréhender les auteurs de ces attaques;

(xiii) Notant aussi la difficulté de classer ce type d'attaques en les considérant ou non comme des cas d'agression armée ou des actes de guerre;

(xiv) Constatant que lors de la guerre des cinq jours entre la Géorgie et la Russie, des moyens de guerre informatique ont été utilisés, parallèlement à des actions militaires conventionnelles, par les deux belligérants;

(xv) Considérant que ces événements confirment une fois de plus l'utilisation offensive des moyens informatiques dans les opérations militaires;

(xvi) Considérant que les événements survenus en Estonie, en 2007 et en Géorgie, en 2008, démontrent le besoin d'une approche proactive et coordonnée, au niveau national et entre alliés, de la défense informatique;

(xvii) Notant avec satisfaction, à ce titre, la décision prise par l'OTAN, sur proposition des autorités estoniennes en 2004, de mettre sur pied un Centre d'excellence pour la cyberdéfense en coopération (CCD-COE), à Tallinn, en Estonie, même s'il n'est doté que d'un budget limité;

(xviii) Constatant que ce Centre d'excellence doit être pleinement opérationnel à la fin de 2008 et qu'un nombre croissant d'Etats européens, ainsi que les Etats-Unis, en font déjà partie ou participeront à ses activités dès que le Centre sera homologué par les autorités compétentes de l'OTAN;

(xix) Exprimant son soutien à cette initiative et considérant qu'il est nécessaire de veiller à ce que le Centre dispose des moyens humains, matériels et budgétaires adéquats pour atteindre les objectifs fixés par l'OTAN dans ce domaine;

(xx) Considérant que le Centre d'excellence doit pouvoir être intégré dans un réseau reliant avec l'OTAN et entre eux les centres nationaux de sécurité informatique relevant de la compétence des ministères de la défense, et qu'il importe dans cette logique d'oeuvrer à la mise en place d'un tel maillage;

(xxi) Considérant aussi que la protection de l'infrastructure informatique civile et de sécurité doit rester sous la responsabilité des autorités civiles et de sécurité, dans le cadre d'un partenariat publicprivé;

(xxii) Notant que le Plan de développement des capacités de l'Union européenne, adopté le 8 juillet 2008 au sein de l'Agence européenne de défense, inclut les opérations et les capacités infocentrées dans la liste des 12 actions prioritaires en matière de capacités de défense européennes;

(xxiii) Constatant que l'Union européenne, notamment dans l'espace de liberté, de sécurité et de justice, dispose déjà d'une Agence en charge des questions de sécurité informatique civile;

(xxiv) Considérant qu'il est nécessaire de coordonner, dans une approche cohérente et efficace, les efforts entrepris par les différents piliers de l'Union européenne dans ce domaine et d'assister les Etats nationaux, selon le principe de subsidiarité;

(xxv) Considérant que la sécurité informatique en Europe passe par une coopération et une coordination accrues entre l'UE, l'OTAN et les autorités nationales, dans le respect des compétences de chacun de ces acteurs majeurs;

(xxvi) Considérant que les parlements nationaux ont un rôle central à jouer dans ce domaine, d'une part en discutant et en votant des lois nationales et en ratifiant des accords internationaux de sécurité et de défense informatique et, de l'autre, en veillant au respect des droits et des libertés fondamentaux, publics et privés, caractéristiques des démocraties développées,

RECOMMANDE AU CONSEIL DE L'UNION DE L'EUROPE OCCIDENTALE ET AU CONSEIL DE L'UNION EUROPÉENNE

1. D'oeuvrer, dans le cadre d'une approche commune, pour la définition et la classification des risques et des menaces dans le domaine de la sécurité et de la défense informatiques;

2. De soutenir les initiatives européennes et transatlantiques visant l'amélioration et le développement des capacités collectives et nationales dans ce domaine, à l'image de la création du Centre d'excellence pour la cyberdéfense en coopération, à Tallin, en Estonie;

3. De mettre en oeuvre le concept de l'OTAN de cyberdéfense et d'encourager la coopération et l'échange d'informations entre l'OTAN et l'UE dans ce domaine;

4. D'envisager de confier à l'Agence européenne de défense la responsabilité de l'élaboration, du développement et de la mise en oeuvre d'un concept de sécurité et de défense informatique au titre de la PESD;

5. De coopérer entre Etats et de mettre en place des mécanismes d'assistance rapide et de mise à disposition d'infrastructures informatiques de sauvegarde et de repli, en cas de cyberattaques systémiques multisectorielles sur un ou plusieurs Etats alliés;

6. De dialoguer et de mettre en place des mécanismes de coopération avec d'autres Etats dans le monde qui sont confrontés aux mêmes risques et menaces informatiques;

7. De rechercher l'harmonisation entre les lois et les pratiques nationales concernant le réseau Internet et son utilisation de manière à limiter au maximum ou à éviter l'apparition et le développement de vulnérabilités géographiques informatiques dont pourraient profiter des acteurs malveillants, étatiques et non-étatiques;

8. De tenir l'Assemblée informée de l'état des discussions et des réalisations en matière de sécurité et de défense informatiques, qui ont des implications réelles en termes de sécurité et de défense collectives, au sein de l'OTAN et de l'UE.

N. B. Traduzione non ufficiale

Raccomandazione 831 ([1])

Sulla guerra informatica (o ciber-guerra) ([2])

L'Assemblea,

I. Constatando la crescente diffusione di reti informatiche e di internet nell'organizzazione e nella gestione delle aziende europee;

II. Constatando l'importanza del settore informatico e delle reti informatiche per l'economia nel complesso (transazioni bancarie, commercio, scambio di informazione finanziaria, per esempio);

III. Constatando i progressi tecnologici raggiunti in questo ambito e i conseguenti molteplici benefici nelle sfere sociali, economiche, culturali e politiche;

IV. Constatando la crescente informatizzazione dei sistemi di difesa nazionale nell'area delle strutture e attrezzature comando e controllo (C2), fino al soldato supportato dalla rete nel teatro delle operazioni;

V. Considerando come risultato che esiste una dimensione strategica delle reti informatiche e di internet per le quali è necessario assicurare sicurezza nell'ambito pubblico e privato;

VI. Constatando che suddette reti, a causa del loro scopo originario e della loro natura globale, sono soggette a interruzioni e a destabilizzazione e possono essere inoltre utilizzate per destabilizzare, disinformare o ad esempio per attività criminali;

VII. Considerando che ogni risposta a potenziali minacce a reti informatiche pubbliche o private deve essere globale e onnicomprensiva e attingere alle capacità dello Stato e delle aziende del settore e della società civile (utenti privati);

VIII. Considerando che, data la natura globale di internet, è necessario creare meccanismi di cooperazione internazionale per combattere la ciber-criminalità e il ciber-terrorismo, seguendo l'esempio della Convenzione del Consiglio d'Europa sulla ciber-criminalità;

IX. Constatando le conseguenze negative dei ciber-attacchi contro l'Estonia nei mesi di aprile e maggio 2007;

X. Constatando che nonostante la portata di questi attacchi, le autorità estoni sono state in grado di ridurre gli effetti, neutralizzarli e contrastarli riuscendo a chiudere i siti da cui provenivano alcune delle azioni criminose perpetrate;

XI. Consapevole che tale azione di difesa è stata resa possibile dalla capacità di reazione immediata delle autorità estoni

---

([1]) Adottata dell'Assemblea durante la seconda seduta del 3 Dicembre 2008.

([2]) Motivazione: cfr. la relazione presentata a nome della Commissione di Difesa dall'on. Chope, (Regno Unito, Gruppo Federato) e dell'on. Kõuts, (Estonia, Gruppo Fedrato), Relatori, Documento 2022.

incaricate della ciber-difesa e che tali autorità hanno usufruito degli aiuti internazionali, in particolare dagli stati membri della NATO;

XII. Constatando, tuttavia, la difficoltà di individuare e arrestare i responsabili di tali attacchi;

XIII. Constatando, anche la difficoltà di classificare questo tipo di attacco come un attacco armato o un atto di guerra;

XIV. Constatando che durante i cinque giorni di guerra tra Georgia e Russia, la ciber-guerra è stata condotta parallelamente ad un'azione militare convenzionale da entrambe le parti belligeranti;

XV. Costatando che questi eventi danno un ulteriore conferma della possibilità di impiegare la tecnologia informatica nelle operazioni militari per usi offensivi;

XVI. Considerando che quanto avvenuto in Estonia nel 2007 e in Georgia nel 2008 dimostra la necessità di un'impostazione di ciber-difesa interattiva e coordinata sia a livello nazionale che tra alleati;

XVII. Costatando con soddisfazione a questo proposito la decisione presa dalla NATO, sulla base di una proposta delle autorità estoni nel 2004, di stabilire un centro cooperativo di eccellenza per la ciber-difesa (CCD-CoE) a Tallinn, in Estonia se pur con risorse limitate;

XVIII. Costatando che questo centro di eccellenza dovrebbe essere pienamente operativo entro la fine del 2008 e che un numero crescente di stati europei e gli Stati Uniti hanno già preso parte o parteciperanno alle sue attività in attesa dell'approvazione del centro da parte delle autorità pertinenti della NATO;

XIX. Esprimendo il suo sostegno a questa iniziativa e considerando che è necessaria assicurare che il Centro abbia sufficienti risorse umane, materiali e finanziarie per raggiungere gli obiettivi stabiliti dalla NATO in questo ambito;

XX. Considerando che il centro d'eccellenza deve essere in grado di entrare in una rete connessa con la NATO e con i centri nazionali di ciber-sicurezza sotto il controllo dei ministri della difesa e che per raggiungere tale obiettivo è importante adoperarsi per istituire tale rete;

XXI. Considerando, inoltre, che tanto la protezione delle infrastrutture di sicurezza che di quelle civili dovrebbe essere di responsabilità delle autorità civili e di sicurezza, come componente della partnership pubblica-privata;

XXII. Costatando che il Piano di Sviluppo delle Capacità dell'Unione europea, adottato l'8 luglio 2008 dall'Agenzia europea per la Difesa, comprende le capacità e operazioni supportate dalla rete nella lista delle 12 azioni prioritarie nel settore delle capacità della difesa europea;

XXIII. Costatando che l'Unione europea, in particolar modo nei settori della libertà, sicurezza e giustizia, dispone già di un'Agenzia responsabile le questioni inerenti di ciber-sicurezza civile;

XXIV. Considerando che è necessario adottare un'impostazione coerente ed efficace al fine di coordinare gli sforzi intrapresi dai differenti pilastri dell'Unione europea in tale ambito e assistere gli stati nazionali a rispettare il principio di sussidiarietà;

XXV. Considerando che la ciber-sicurezza in Europa richiede una maggiore cooperazione e coordinamento tra l'UE, la NATO e le autorità nazionali fatte salve le rispettive responsabilità di ciascuno di essi;

XXVI. Considerando che i Parlamenti nazionali svolgono un ruolo fondamentale in tale area, sia tramite la discussione e la votazione di leggi nazionali sia la ratifica di accordi internazionali sulla ciber-sicurezza e ciber-difesa e sia garantendo le libertà e i diritti fondamentali, caratteristica delle democrazie mature, sia nella sfera pubblica che privata,

RACCOMANDA AL CONSIGLIO DELL'UNIONE DELL'EUROPA OCCIDENTALE E AL CONSIGLIO DELL'UNIONE EUROPEA DI:

1. Adottare misure rientranti in un approccio comune per definire e classificare i rischi e le minacce nell'ambito della ciber-sicurezza e ciber-difesa;

2. Sostenere le iniziative europee e transatlantiche che mirano a migliorare e costruire capacità collettive e nazionali in tale settore, come l'istituzione di un centro cooperativo di eccellenza per la ciber-difesa a Tallin, Estonia;

3. Attuare il concetto di ciber-difesa della NATO e incoraggiare la cooperazione e lo scambio di informazioni tra la NATO e l'UE in tale ambito;

4. Prendere in considerazione l'idea di affidare all'Agenzia europea per la Difesa la responsabilità di redigere, sviluppare e attuare un concetto di ciber-sicurezza e ciberdifesa in conformità con la PESD;

5. Garantire la cooperazione tra gli stati e stabilire meccanismi per una celere assistenza e la fornitura di infrastrutture informatiche per la memorizzazione e il back up in caso di ciber-attacchi sistematici multi settoriali ad uno o più stati alleati;

6. Intavolare un dialogo e istituire meccanismi di cooperazione con altri stati nel mondo che affrontino gli stessi rischi e minacce di natura informatica;

7. Cercare di armonizzare le leggi e le procedure nazionali relative a internet e al suo uso, allo scopo di ridurre o evitare il crearsi e il diffondersi di punti deboli nella rete informatica che potrebbero essere sfruttati da soggetti statali o non statali malintenzionati;

8. Informare l'Assemblea sullo stato di avanzamento delle discussioni e dei lavori portati avanti all'interno della NATO e dell'UE nell'ambito della ciber-sicurezza e ciber-difesa che abbiano effettive implicazioni per la sicurezza e la difesa collettive.