Cyber (e Digital) Diplomacy

Cybersecurity nel contesto internazionale
Forum Cyber 4.0
Aula Magna Università La Sapienza

Roma,
06/06/2023

A cura della Min. Plen. Laura Carpini
Capo Unità per le politiche e la sicurezza dello spazio cibernetico

Ministero degli Affari Esteri
e della Cooperazione Internazionale

Agenda

- **Contesto Internazionale**
- **Il lavoro dell'Unità per le politiche e la sicurezza dello spazio cibernetico**
- **Priorità e livelli di Cooperazione**
- **Messaggi Chiave**

Contesto internazionale: come influenza ed è influenzato dalle questioni cyber/digitali

- La creazione dello spazio cibernetico e di Internet come **game-changer per le relazioni internazionali.**
- **Incremento esponenziale delle azioni malevole**
- Peculiarità e complessità dello spazio cibernetico per la relativa **assenza di confini tradizionali e di regolamentazione pattizia** che può avere un **impatto sulla sovranità** degli Stati**.**
- Crescente **competizione tra le potenze** che trova nella **lotta per supremazia tecnologica** un terreno naturale di confronto
- Ruolo dell'**UE** potenzialmente più proteso verso la **resilienza e l'autonomia tecnologia e strategica**, continuando a perseguire il ruolo di **regolatore globale** ed al contempo di stimolo all'innovazione a livello interno.
- Effetti globali della **pandemia** che hanno accelerato e reso molto più attuali processi, confronti e bisogni relativi alla digitalizzazione.
- I codici malevoli e le vulnerabilità possono essere **un'arma** ad alto potenziale di spillover, e questo pone grandi problemi di sicurezza e stabilità internazionale. Questione della deterrenza.
- **Caso ucraino**, azioni malevole poi attribuite alla Russia si sono succedute in preparazione con l'attacco cinetico, attori non statuali
- In generale lo spazio cibernetico è uno dei **terreni di competizione internazionale** globale tra potenze ma anche un **potenziale strumento di sovversione** di alcuni principi cardine.
- **Istituzione di uffici cyber** nei vari Ministeri degli Esteri.

Costituzione dell'Unità per le politiche dello spazio cibernetico

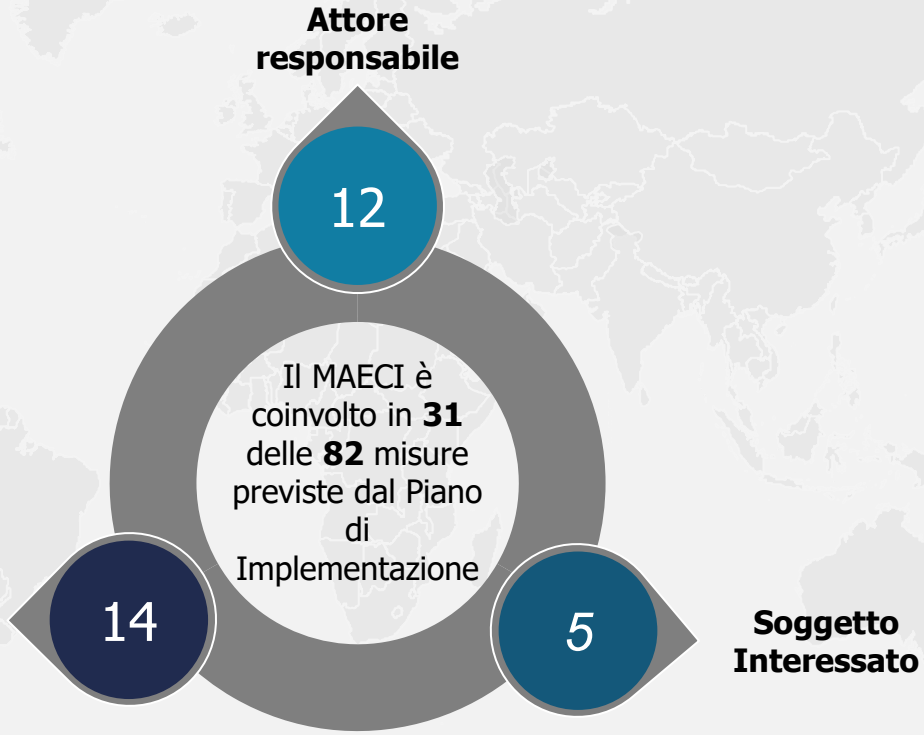
Con il DM 20 dicembre 2019 n. 1202/2722 presso la DGAP viene istituita l'**Unità per le politiche e la sicurezza dello spazio cibernetico per accompagnare lo sviluppo dell'architettura nazionale di sicurezza cibernetica**.

Le principali funzioni / competenze dell'Unità sono:

- Coordinamento in materia di diplomazia della sicurezza cibernetica e processi di governance internazionale dello spazio cibernetico e di internet;
- questioni relative allo spazio cibernetico e alle tecnologie emergenti nell'ambito digitale;
- rapporti con enti, organizzazioni e organismi internazionali preposti alla sicurezza cibernetica e alle questioni digitali, con il settore privato, il mondo accademico e la società civile per le materie di competenza.

Ruolo della Cyber Diplomacy nella Strategia di Cybersicurezza Nazionale

Cyber Diplomacy, intesa come il ricorso a strumenti e iniziative diplomatiche per conseguire gli interessi nazionali del Paese nello spazio cibernetico e come parte delle più ampie attività di politica estera, tenuto conto dell'impatto della tecnologia sulle relazioni internazionali.



Priorità: Cooperazione in ambito UE

- **EU's Cybersecurity Strategy for the Digital Decade:** La nuova Strategia Europea si propone di rafforzare la resilienza collettiva dell'Europa contro le minacce informatiche e garantire che tutti i cittadini e le imprese possano beneficiare pienamente dei servizi e strumenti digitali. Da seguire e applicare in collaborazione con la Commissione e il SEAE.
  1) resilienza interna, sovranità tecnologica e leadership
  2) sviluppo delle capacità operative per attività di prevenzione, deterrenza e di risposta
  3) promozione di uno spazio cibernetico globale e aperto

- **EU Cyber Diplomacy Toolbox:** una raccolta di strumenti per sistematizzare le possibili azioni diplomatiche a disposizione dell'UE per prevenire o rispondere ad azioni malevole, al fine di mantenere la pace e la stabilità dello spazio cibernetico. Tra queste spicca la possibilità di adottare misure restrittive contro individui o enti ritenuti responsabili di azioni malevole ai danni di uno o più Stati dell'UE. (approfondimento nella slide seguente).

- **Postura cyber dell'Unione europea**: questa posizione nasce dalla necessità dell'UE di essere in grado di rispondere in modo rapido agli attacchi informatici e fare pieno uso di tutti i suoi strumenti. Nelle conclusioni il Consiglio ha evidenziato le cinque funzioni dell'UE nel settore cibernetico: rafforzare la resilienza e le capacità di protezione; rafforzare la solidarietà e la gestione globale delle crisi; promuovere la visione dell'UE del ciberspazio; rafforzare la cooperazione con i paesi partner e le organizzazioni internazionali; prevenire, difendersi e rispondere agli attacchi informatici.

Priorità: Cooperazione Multilaterale

ONU

- **Gruppi di Esperti Governativi (GGE)**: previsione di norme di comportamento responsabile da parte degli Stati, applicabilità del diritto internazionale nell'uso delle ICT e **Confidence Building Measures, CBMs**.
- **Open-ended Working Group (OEWG)**: posizione italiana circa la totale **applicabilità del diritto internazionale allo spazio cibernetico**. -> adozione rapporto consensuale che inoltre menziona tra le raccomandazioni un **Programme of Action.** Ultima riunione sostanziale lo scorso luglio. Progetto di risoluzione sul PoA.

NATO

- Adozione del cosiddetto "**Cyber Defence Pledge**", come strumento di convergenza degli sforzi dei singoli Alleati in materia di resilienza ad attacchi cyber. **NATO CYBER DEFENCE PLEDGE Conference 2022 a Roma. VCISC e rivitalizzazione del pledge**
- Affinamento della **roadmap per l'attuazione della dichiarazione dello spazio cyber come dominio operativo** e nell'integrazione nelle missioni e operazioni NATO, a livello tecnico-militare, di effetti cibernetici sovrani messi a disposizione dell'Alleanza da singole Nazioni alleate.
- Nuovo «**Concetto strategico**» adottato a Madrid e ruolo della parte cyber.

OSCE

- Sono state sviluppate una serie di **CBM**, volte a far convergere le percezioni dei diversi Stati sull'uso delle ICT. Sviluppo più recente: previo coordinamento e accordo con l'ACN, l'Unità ha curato, in raccordo con DIS prima e ACN poi, l'adozione dell'Italia alla **CBM-14**.
- Durante la presidenza italiana dell'OSCE nel 2018 l'Italia ha ospitato una **Conferenza sulla sicurezza cibernetica**, volta a rappresentare una piattaforma di condivisione e scambio di visioni in merito alla sicurezza digitale nella regione, per promuovere la resilienza cibernetica anche attraverso il **partenariato pubblico-privato** ed analizzare le prospettive fino al 2025.

Food for Thought – il caso ucraino

Il **conflitto in Ucraina** stimola alcune riflessioni anche nella **sfera cyber/digitale**. Quali conseguenze si possono trarre per l'immediato futuro? Ecco alcuni **spunti di riflessione** provocatori:

- **L'arma cibernetica** e suo uso in un conflitto, armi autonome e intelligenza artificiale
- **Ruolo del settore privato** e attori non statuali
- Stiamo assistendo a una **frammentazione delle reti e** della governance **di Internet ("Splinternet")?**

Messaggi Chiave

- Digitalizzazione e Cyber come temi di politica estera e relazioni internazionali.
- Chiavi di lettura: globalizzazione/sovranità; libertà/regole; automazione/elemento umano; Stato/settore privato ecc…
- Pervasività della digitalizzazione e delle conseguenti questioni di sicurezza creano sfide, ma anche enormi opportunità di lavoro, non solo tecniche ma in tutte i settori affini o che hanno una declinazione digitale/cyber.
- Materia in continua evoluzione, che subirà ulteriori modifiche con l'avvento di nuove tecnologie. Sfida dell'Intelligenza Artificiale

GRAZIE

Roma,
21/11/2022

Laura Carpini
Laura.carpini@esteri.it

Ministero degli Affari Esteri
e della Cooperazione Internazionale