

Sorvegliare e sanzionare

La difesa della democrazia nell'Unione europea di fronte alle minacce cibernetiche

Dott.ssa Susanna Villani - Dipartimento di Scienze Giuridiche (Università di Bologna)

Nell'ambito del Modulo Jean Monnet DIGEOMETRY - DIGital EurOpe for Multi-Speed intEgraTion and democRacY



Sorvegliare e sanzionare: la difesa della democrazia nell'Unione europea di fronte alle minacce cibernetiche

Sorvegliare e sanzionare: la difesa della democrazia nell'Unione europea di fronte alle minacce cibernetiche

La cybersicurezza è diventata una priorità fondamentale per l'Unione europea, alla luce dell'aumento degli attacchi informatici che minacciano la democrazia e la stabilità degli Stati membri e delle sue istituzioni. Le misure restrittive adottate dall'UE rappresentano uno strumento cruciale per garantire la sicurezza collettiva e proteggere i valori fondamentali dell'Unione.





Evoluzione della strategia UE in materia di cybersecurity

Analizzeremo l'evoluzione della strategia dell'Unione europea per affrontare le minacce cibernetiche evidenziando i passaggi chiave.



Regime delle misure restrittive contro attacchi informatici

Esamineremo il regime di misure restrittive (sanzioni) adottato dall'UE per rispondere agli attacchi informatici.



Interazione con il quadro costituzionale UE

Valuteremo come le misure restrittive si integrano con la cornice giuridica e i principi costituzionali dell'Unione europea.



Criticità applicative e nuove sfide

Analizzeremo le applicazioni pratiche delle misure restrittive, evidenziando le sfide e le criticità riscontrate negli interventi dell'UE.

Obiettivi del seminario



Evoluzione della strategia UE in materia di cybersicurezza

Analizzeremo l'evoluzione della strategia dell'Unione europea per affrontare le minacce cibernetiche, evidenziando i passaggi chiave.



Regime delle misure restrittive contro attacchi informatici

Esamineremo il regime di misure restrittive (sanzioni) adottato dall'UE per rispondere agli attacchi informatici.



Interazione con il quadro costituzionale UE

Valuteremo come le misure restrittive si integrano con la cornice giuridica e i principi costituzionali dell'Unione europea.



Criticità applicative e nuove sfide

Analizzeremo le applicazioni pratiche delle misure restrittive, evidenziando le sfide e le criticità riscontrate negli interventi dell'UE.



WannaCry: il ransomware devastante (2017)

Il ransomware WannaCry, distribuito in un gruppo chat Telegram, ha colpito oltre 150.000 sistemi in 150 paesi, causando danni per oltre 4 miliardi di dollari.



NotPetya: l'attacco su scala globale (2017)

NotPetya, un ransomware distribuito in un gruppo chat Telegram, ha colpito oltre 100.000 sistemi in 100 paesi, causando danni per oltre 10 miliardi di dollari.



Cloud Hopper: furto di dati aziendali (2014-2017)

Cloud Hopper, un ransomware distribuito in un gruppo chat Telegram, ha colpito oltre 10.000 sistemi in 10 paesi, causando danni per oltre 100 milioni di dollari.



Tipologie di attacchi informatici:

- malware (come virus e ransomware),
- phishing,
- attacchi DDoS
- attacchi alle password

Attacchi cyber: le origini

WannaCry: il ransomware devastante (2017)

Il ransomware WannaCry, attribuito al gruppo nordcoreano APT38, ha causato danni globali enormi, infettando centinaia di migliaia di computer in oltre 150 paesi e colpendo in particolare i sistemi sanitari nel Regno Unito.



NotPetya: l'attacco su scala globale (2017)

NotPetya, attribuito alla Russia, ha mirato principalmente aziende in Ucraina ma si è diffuso rapidamente, causando perdite stimate in miliardi di dollari a livello globale, rendendolo uno degli attacchi più costosi della storia.



Cloud Hopper: furto di dati aziendali (2014-2017)

Cloud Hopper, attribuito al gruppo cinese APT10, ha avuto come obiettivo le società di servizi IT per rubare dati sensibili di clienti in tutto il mondo, evidenziando l'importanza della protezione delle informazioni aziendali.





Crescita degli attacchi informatici (strumenti disponibili anche nei dark web)

Il numero di attacchi informatici è in costante crescita, con un aumento del 30% nel 2020. Gli strumenti utilizzati per gli attacchi sono sempre più sofisticati e disponibili anche nei dark web.

Stato per il sostegno da 1.200 al 1.700 milioni l'anno degli hacker



Impatto su ordine pubblico e istituzioni

La cybersecurity è un tema che tocca tutti gli aspetti della vita pubblica e delle istituzioni. L'impatto degli attacchi informatici può essere devastante per la democrazia e la sicurezza nazionale.



Cybersecurity e Unione della Sicurezza

La cybersecurity è un tema che tocca tutti gli aspetti della vita pubblica e delle istituzioni. L'impatto degli attacchi informatici può essere devastante per la democrazia e la sicurezza nazionale.



Connessione con i valori dell'UE

La cybersecurity è un tema che tocca tutti gli aspetti della vita pubblica e delle istituzioni. L'impatto degli attacchi informatici può essere devastante per la democrazia e la sicurezza nazionale.



Cyberattacchi ed elezioni europee 2021

La cybersecurity è un tema che tocca tutti gli aspetti della vita pubblica e delle istituzioni. L'impatto degli attacchi informatici può essere devastante per la democrazia e la sicurezza nazionale.



Perché la
cybersicurezza è un
tema
“costituzionale”?

Crescita degli attacchi informatici (strumenti disponibili anche nel dark web)

Negli ultimi anni, l'Unione europea ha registrato un aumento significativo degli attacchi informatici, con incidenti di spionaggio e ransomware che hanno compromesso la sicurezza nazionale e messo a rischio la stabilità economica, democratica e sociale degli Stati membri.

Malware a noleggio da 5.000\$ al mese:
l'ultima frontiera degli hacker

27 Maggio 2022



Impatto su ordine pubblico e istituzioni

Le minacce cibernetiche hanno ripercussioni dirette sull'ordine pubblico, minano l'integrità delle istituzioni e possono compromettere le infrastrutture critiche, esponendo vulnerabilità che possono essere sfruttate da attori ostili.



Cybersecurity e Unione della Sicurezza

La cybersicurezza è un elemento cruciale della Strategia dell'UE per un'Unione della Sicurezza (COM/2020/605 final), poiché integra sia le misure interne che quelle esterne per garantire la protezione collettiva contro attacchi informatici e minacce alla sicurezza.



Connessione con i valori dell'UE

La cybersicurezza è intrinsecamente collegata ai valori fondamentali dell'UE, come stabilito nell'articolo 2 del Trattato sull'Unione Europea (TUE), e agli obiettivi di politica estera delineati nell'articolo 21 del TUE, sottolineando l'importanza della protezione dei diritti fondamentali.



Cyberattacchi ed elezioni europee 2024

- Attacco alla CDU (Germania) alla vigilia delle elezioni europee (6-9 giugno 2024).
- Grave attacco informatico con parti dell'infrastruttura IT della CDU messe offline.
- Collettivo filorusso NoName057(16) rivendica offensive DDoS legate alle elezioni.
- Motivazione dichiarata: Parlamento europeo = "organo pseudo-democratico e russofobico".
- Target: portali UE, siti di partiti nei Paesi Bassi e risorse web in Spagna e nei Paesi Bassi.



Le competenze dell'UE nel dominio cyber



Nessuna base giuridica espressa



Sicurezza nazionale (art. 4, par.2, TUE):
competenza esclusiva degli Stati membri



PESC: salvaguardare i suoi valori, i suoi interessi
fondamentali, la sua sicurezza, la sua indipendenza e la
sua integrità (art. 21, par. 2(a), TUE)



Approccio multilivello e ibrido

L'evoluzione delle strategie UE sulla cybersicurezza

Tracciamento delle principali fasi e sviluppi delle politiche UE in risposta alle minacce cibernetiche.

2013

Lanciare la strategia "Open, Safe and Secure Cyberpace" (JOIN 2013) (final), ponendo le basi per una cybersicurezza condivisa a livello UE.

2017

Introduzione della strategia "Resilience, Deterrence and Defence" (MCIN/2017/0450 final), focalizzandosi sulla resilienza e sulla difesa contro attacchi cibernetic.

2020

Pubblicazione della "EU Cybersecurity Strategy for the Digital Decade" (COM/2020/11 final), per affrontare le sfide future nella cybersicurezza.

2022

Adozione della "Strategic Compass for Security and Defence" da parte del Consiglio, per rafforzare la cooperazione nella cybersicurezza.

2025

Pubblicazione della "European Preparedness Cyber Strategy" (COM/2025/130 final), per una preparazione proattiva contro gli attacchi cibernetic.

2013

Lanciata la strategia 'Open, Safe and Secure Cyberspace' (JOIN(2013) 1 final), ponendo le basi per una cybersicurezza condivisa a livello UE

2017

Introduzione della strategia 'Resilience, Deterrence and Defence' (JOIN/2017/0450 final), focalizzandosi sulla resilienza e sulla difesa contro attacchi cibernetici

2020

Pubblicazione della 'EU Cybersecurity Strategy for the Digital Decade' (JOIN/2020/18 final), per affrontare le sfide future nella cybersicurezza

2022

Adozione della 'Strategic Compass for Security and Defence' da parte del Consiglio, per rafforzare la cooperazione nella cybersicurezza

2025

Pianificazione della 'European Preparedness Union Strategy' (JOIN(2025) 130 final), per una preparazione collettiva contro attacchi informatici imminenti

Prevent

- Direttiva NIS 2
- Cybersecurity Act (certificazione)
- Cyber Resilience Act (CRA)
- Cyber Solidarity Act

Respond

- Cyber Crisis Management
- Cyber Emergency Mechanism

Detect

- European Cybersecurity Alert System
- Cyber Hubs

Deter

- Cyber Defence Policy
- Cyber Diplomacy Toolbox



Prevenire e rispondere ai cyber attacchi

La Cyber Diplomatic Toolbox dell'UE è progettata per rafforzare e migliorare i cyber attacchi attraverso un approccio coordinato tra gli Stati membri. Essa si propone di rafforzare le capacità di risposta e prevenzione contro minacce cyberetiche.



Coordinamento tra Stati membri

Il coordinamento politico-diplomatico è essenziale per un efficace risposta alle minacce cyberetiche. Attraverso strategie coordinate, gli Stati membri possono condividere informazioni, risorse e buone pratiche. Facilitare il lavoro PESCO e collaborazione con NATO.



Promozione dei valori europei

Il modello UE promuove il rispetto dei diritti fondamentali e dello Stato di diritto, assicurando che le politiche di cybersecurity siano in linea con i valori europei. Ciò implica un impegno costante per il multilateralismo e la cooperazione internazionale.

La Cyber Diplomatic Toolbox (2017)



Prevenire e rispondere ai cyber attacchi

La Cyber Diplomatic Toolbox dell'UE è progettata per affrontare e mitigare i cyber attacchi attraverso un approccio coordinato tra gli Stati membri. Essa si propone di rafforzare le capacità di risposta e prevenzione contro minacce cibernetiche.



Coordinamento tra Stati membri

Il coordinamento politico-diplomatico è essenziale per un'efficace risposta alle minacce cibernetiche. Attraverso dialoghi e collaborazioni, gli Stati membri possono condividere informazioni, risorse e buone pratiche. Esercitazioni tramite PESCO e collaborazione con NATO.



Promozione dei valori europei

Il modello UE promuove il rispetto dei diritti fondamentali e dello Stato di diritto, assicurando che le politiche di cybersicurezza siano in linea con i valori europei. Ciò implica un impegno costante per il multilateralismo e la cooperazione internazionale.

Le misure restrittive dell'UE contro attacchi informatici

Definizione di "attacco informatico": azioni non autorizzate che comportano l'accesso a o interferenze con i sistemi di informazione, interferenza nei dati o intercettazione dei dati

Decisione
(PESC)
2019/797
del Consiglio

Regolamento
(UE)
2019/796
del Consiglio

Soggetti colpiti:
- Stati membri
- Istituzioni UE
- Stati terzi
- Organizzazioni internazionali

Divieti di viaggio
e circolazione
(art. 4
decisione)

Congelamento di
beni per i
soggetti colpiti
dalle sanzioni
(art. 5 decisione)

Cyber-attacco con effetti significativi (art. 3 decisione PESC 2019/797)

Un attacco informatico che ha causato o può causare danni significativi a persone, sistemi, dati, infrastrutture, servizi o attività, o a uno o più di questi elementi, in modo da compromettere la sicurezza, la stabilità o la resilienza di uno o più di questi elementi.



Minaccia esterna all'UE

Un'azione o un'attività che rappresenta una minaccia per la sicurezza, la stabilità o la resilienza di uno o più di questi elementi, in modo da compromettere la sicurezza, la stabilità o la resilienza di uno o più di questi elementi.



Quando l'UE può sanzionare? I criteri

Cyber-attacco con effetti significativi (art. 3 decisione PESD 2019/797)

Per attivare il regime di misure restrittive, è fondamentale che ci sia un cyber-attacco che generi effetti significativi, come danni economici o sociali rilevanti, furto o manipolazione di dati, o compromissione di infrastrutture critiche. Questi criteri aiutano a definire la gravità e l'impatto dell'attacco sul sistema e sulla sicurezza degli Stati membri.



Minaccia esterna all'UE

In aggiunta agli effetti significativi, è necessaria l'esistenza di una minaccia esterna all'Unione europea. Questo implica che le sanzioni sono giustificate quando l'attacco proviene da attori esterni, in grado di minacciare la sicurezza e la stabilità dell'Unione nel suo complesso.



Chi può essere colpito dalle sanzioni?

(oggi 17 soggetti e 4 entità)



Autori materiali dell'attacco



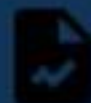
Soggetti di supporto tecnico



Soggetti di supporto finanziario



Soggetti di supporto logistico



Entità e individui legati a Stati terzi

Il nodo dell'attribuzione



Attribuzione Tecnica

L'attribuzione tecnica si basa su analisi dettagliate condotte da esperti informatici che esaminano i dati, il codice dannoso e le modalità operative degli attacchi. Questo processo richiede competenze specialistiche e strumenti avanzati per identificare il responsabile di un attacco informatico in modo preciso e oggettivo.



Attribuzione Politica

L'attribuzione politica implica una decisione (all'unanimità) degli Stati membri dell'UE, che devono valutare le prove disponibili e decidere se e come attribuire responsabilità a un attore statale o non statale. Questa fase è spesso influenzata da considerazioni diplomatiche e strategiche, rendendo il processo complesso e soggetto a interpretazioni diverse.

Criticità costituzionali del regime

- Diritti fondamentali a rischio (caso Kadi, 2008, cause riunite C-402/05 P e C-415/05)
- Opacità nelle procedure di verifica (trasparenza)
- Difficoltà di contestazione
- Discrezionalità del Consiglio (politica e diplomatica)
- Necessità di unanimità (anzichè MQ ai sensi dell'art. 215 TFUE)

Reazioni? Osservazioni? Curiosità?

GRAZIE!

Jean Monnet Module “DIGEOMETRY” (DIGital EurOpe for Multi-Speed intEgraTion and democRacY)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.



PROJECT DIGEOMETRY — Digital Europe for Multi-Speed Integration and Democracy — GA101238791

