CONVEGNO
«STORIA DEL TERRORISMO. IL CONTRASTO AL TERRORISMO INTERNAZIONALE, QUALI SCENARI FUTURI?»

EVERSIONE INTERNAZIONALE ED ECOSISTEMA DIGITALE: IL CYBER TERRORISMO, DA MEZZO DI PROPAGANDA E RECLUTAMENTO AD ARMA DI ATTACCO

Corte di Cassazione, 11 Dicembre 2018

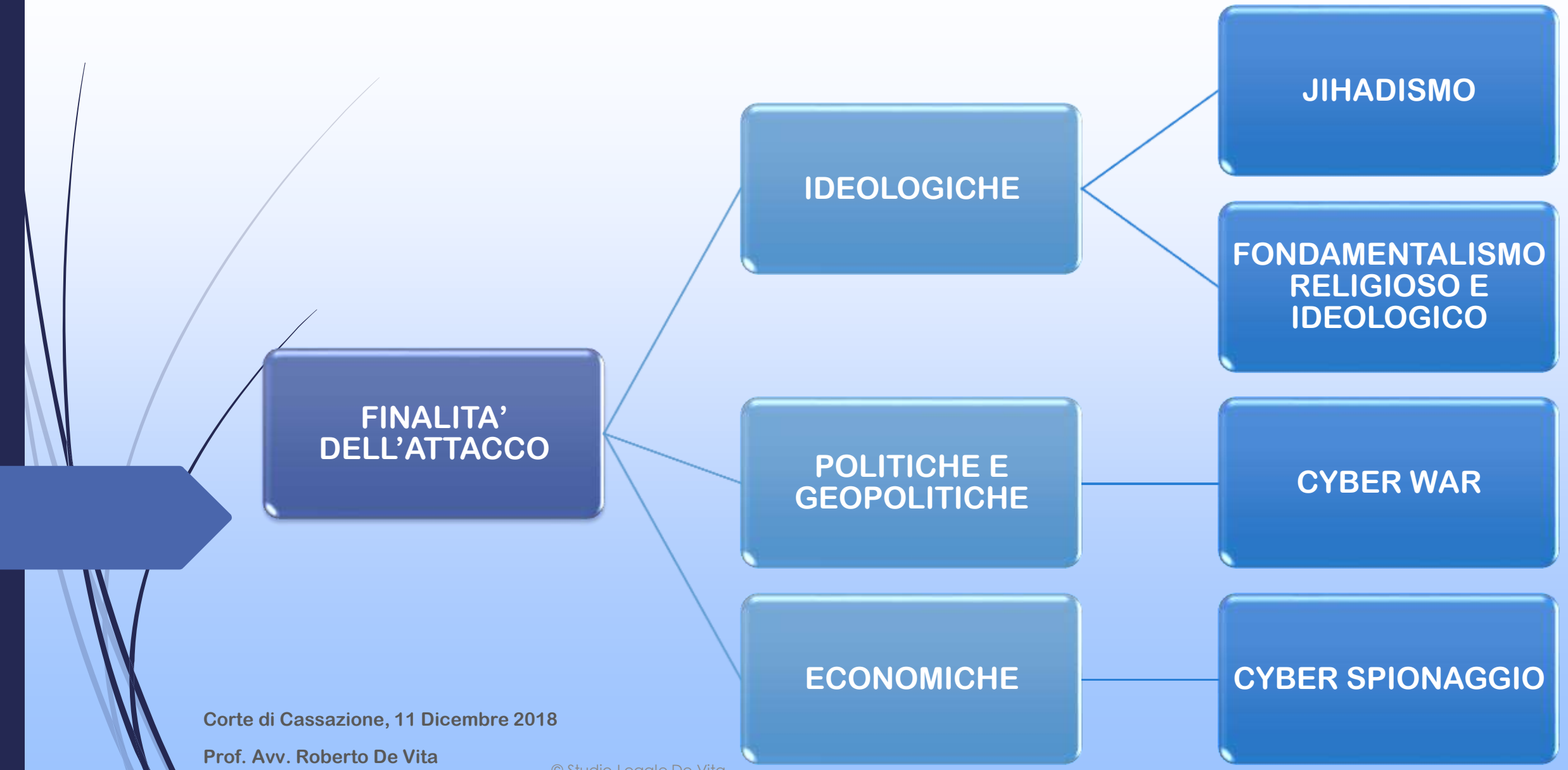
Prof. Avv. Roberto De Vita

ECOSISTEMA DIGITALE: I NUMERI

- Accesso ad Internet nel 2018: 4,208 mld persone (55.1% popolazione mondiale)
- Più del 70% degli utenti è in paesi in via di sviluppo (49% Asia, 11% Africa, 10.4 % Sud America, 3.9% Middle East)*
- Internet of things (IoT): entro il 2020 il rapporto tra devices connessi e individuo sarà di 1:6

*Internet World Stats, June 30, 2018

IL CYBER TERRORISMO



Corte di Cassazione, 11 Dicembre 2018

Prof. Avv. Roberto De Vita

IL CYBER TERRORISMO: DEFINIZIONI

FBI

«Any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violance against non-combatant targets by sub-national groups or clandestine agents»

NATO

«A cyber attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal»

IL CYBER TERRORISMO: DEFINIZIONI

Corte di Cassazione, 11 Dicembre 2018

Prof. Avv. Roberto De Vita

TERRORISMO E SOCIAL MEDIA

La perdita di territori nel 2016/2017 da parte dell'IS non è coincisa con la perdita di autorità tra i seguaci né ha condotto ad un decremento degli attacchi.

Al contrario, i vari gruppi hanno continuato ad utilizzare la rete per diffondere la loro dottrina ed ispirare atti di terrorismo*.

*Europol IOCTA 2018, Internet Organised Crime Threat Assessment

TERRORISMO E SOCIAL MEDIA

Nel 2016 i simpatizzanti IS hanno trasferito le loro comunicazioni da piattaforme aperte (Twitter e Facebook) a canali criptati di comunicazione (Telegram, Signal, Threema).

La loro evoluzione tecnologica si è adeguata alle nuove opportunità offerte dalla rete, dallo sfruttamento del dark web alla diffusione delle criptomonete*.

*Europol IOCTA 2018, Internet Organised Crime Threat Assessment

TERRORISMO E SOCIAL MEDIA

I soggetti impegnati nella lotta al terrorismo di matrice islamica stanno impiegando risorse sempre maggiori in «operazioni cyber» volte a contrastare le nuove competenze e capacità digitali dei gruppi:

- **il 25 Aprile 2018 gli Stati UE, USA e Canada hanno sferrato un attacco congiunto contro la macchina propagandistica dell'IS (principalmente Amaq News Agency, Al-Bayan Radio, Halumu e Nashir News) al fine di interromperne la funzionalità;***

- **un altro attacco ha riguardato la chiusura massiva su varie piattaforme di account di simpatizzanti IS riconducibili ad un unico pool (al-Ansar Bank o «Bank of Supporters») che abilitava gli utenti a bypassare le procedure di registrazione per mantenere anonimi i profili.***

*Europol IOCTA 2018, Internet Organised Crime Threat Assessment

IL FINANZIAMENTO: CRIPTOVALUTE

- Le criptovalute rappresentano una grande risorsa per il finanziamento dei gruppi terroristici poiché consentono transazioni ingenti di denaro al di fuori dei normali circuiti finanziari.

- Già nel 2014 l'IS aveva scoperto le criptomonete ma è solo dal 2017 che ha utilizzato donazioni massive (soprattutto in Bitcoin e Zcash) attraverso chat anonime e canali chiusi di comunicazione, ovvero ne ha sollecitato l'uso da parte dei simpatizzanti.

- La maggior parte dei fondi sono stati utilizzati per finanziare le infrastrutture tecnologiche ed acquistare hosting servers.*

*Europol IOCTA 2018, Internet Organised Crime Threat Assessment

IL FINANZIAMENTO
CYBER MONEY LAUNDERING

Il riciclaggio è uno degli strumenti necessari per il finanziamento dei gruppi terroristici.
Secondo il FATF (Financial Action Task Force) il riciclaggio avviene ormai attraverso il c.d. PML (Professional Money Laundering), ovvero professionisti dotati di specifiche competenze ed abilità, messe al servizio di criminalità organizzata e gruppi terroristici.

PML: singoli individui, organizzazioni di professionisti o interi network composti da molteplici professionalità, tutte coinvolte nelle singole fasi delle operazioni (commercialisti, contabili, notai, avvocati, bancari, brokers, providers di trust e servizi societari nonché di servizi finanziari, esperti di transazioni elettroniche e criptovalute).*

Corte di Cassazione, 11 Dicembre 2018

Prof. Avv. Roberto De Vita

*FATF Report – Professional Money Laundering, July 2018

IL FINANZIAMENTO
CYBER MONEY LAUNDERING

Commissione Europea

Direttiva UE 2018/843 del 30.05.2018 - modifica della c.d. quarta direttiva sul riciclaggio relativa "alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo":

- ✓ preoccupazione per la crescente convergenza tra criminalità organizzata e terrorismo e l'utilizzo della tecnologia in campo finanziario: il grado di anonimato delle operazioni in valute virtuali rispetto ai classici trasferimenti di fondi potrebbe avvantaggiare le organizzazioni terroristiche per nascondere e trasferire denaro;

- ✓ altri rischi potenziali riguardano l'irreversibilità delle operazioni, la gestione di operazioni fraudolente, la natura opaca e tecnologicamente complessa del settore e la mancanza di garanzie regolamentari. *

*Direttiva UE 2018/843 del 30.05.2018 (entrata in vigore il 9.07.2018 e dovrà essere recepita entro il 10.01.2020)

IL FINANZIAMENTO
CYBER MONEY LAUNDERING

Direttiva UE 2018/843 del 30.05.2018* – Principali novità in materia di contrasto al finanziamento del terrorismo:

- ✓ Ampliamento del novero di soggetti sottoposti ad obblighi antiriciclaggio (es. prestatori di servizi di cambio valuta digitale e di gestione di portafoglio digitale)
- ✓ Estensione degli obblighi anche per le criptovalute
- ✓ Riduzione di soglie e limiti di utilizzo per carte prepagate anonime

*Direttiva UE 2018/843 del 30.05.2018 (entrata in vigore il 9.07.2018 e dovrà essere recepita entro il 10.01.2020)

CONVEGNO
«STORIA DEL TERRORISMO. IL CONTRASTO AL TERRORISMO INTERNAZIONALE, QUALI SCENARI FUTURI?»

EVERSIONE INTERNAZIONALE ED ECOSISTEMA DIGITALE: IL CYBER TERRORISMO, DA MEZZO DI PROPAGANDA E RECLUTAMENTO AD ARMA DI ATTACCO

Corte di Cassazione, 11 Dicembre 2018

Prof. Avv. Roberto De Vita