COMMISSIONE IV
DIFESA

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

3.

SEDUTA DI MARTEDÌ 8 MARZO 2016

PRESIDENZA DEL PRESIDENTE **FRANCESCO SAVERIO GAROFANI**

INDICE

N. B. Sigle dei gruppi parlamentari: Partito Democratico: PD; MoVimento 5 Stelle: M5S; Forza Italia - Il Popolo della Libertà - Berlusconi Presidente: (FI-PdL); Area Popolare (NCD-UDC): (AP); Sinistra Italiana-Sinistra Ecologia Libertà: SI-SEL; Scelta Civica per l'Italia: (SCpI); Lega Nord e Autonomie - Lega dei Popoli - Noi con Salvini: (LNA); Democrazia Solidale-Centro Democratico (DeS-CD); Fratelli d'Italia-Alleanza Nazionale: (FdI-AN); Misto: Misto; Misto-Alleanza Liberalpopolare Autonomie ALA-MAIE-Movimento Associativo Italiani all'Estero: Misto-ALA-MAIE; Misto-Minoranze Linguistiche: Misto-Min.Ling; Misto-Partito Socialista Italiano (PSI) - Liberali per l'Italia (PLI): Misto-PSI-PLI; Misto-Alternativa Libera-Possibile: Misto-AL-P; Misto-Conservatori e Riformisti: Misto-CR; Misto-USEI (Unione Sudamericana Emigrati Italiani): Misto-USEI.

PRESIDENZA DEL PRESIDENTE FRANCESCO SAVERIO GAROFANI

La seduta comincia alle 11.35.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori sarà assicurata anche attraverso l'attivazione di impianti audiovisivi a circuito chiuso, la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla web-tv della Camera dei deputati.

Audizione del professor Alessandro Politi, direttore della NATO *Defense College Foundation*.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, l'audizione del professor Alessandro Politi, direttore della NATO *Defense College Foundation*.

Saluto e do il benvenuto al professor Politi, che ringrazio per la sua disponibilità. Il professore è analista politico-strategico e direttore della NATO *Defense College Foundation*, oltre che, tra le altre cose, docente di geopolitica, geoeconomia e *intelligence* presso la Società italiana per l'organizzazione internazionale (SIOI).

Come di consueto, dopo l'intervento del nostro ospite darò la parola ai colleghi che vorranno rivolgere domande e osservazioni. Poi il professore risponderà a queste domande. Senza indugi, do la parola al professor Politi.

ALESSANDRO POLITI, *Direttore della NATO Defense College Foundation*. Grazie, presidente, innanzitutto per l'onore e la considerazione accordatimi. Cercherò di farvi una rapida presentazione di un inquadramento che non è il solito inquadramento tecnico per minacce cybercriminali, cyberterroristiche oppure di guerra informatica, non perché queste dimensioni non vengano considerate, ma perché vorrei cercare di fornirvi un insieme che, in mancanza di meglio, chiameremo geopolitico.

Perché dico « in mancanza di meglio » ? Perché, in realtà, lo spazio informatico, ossia lo spazio cibernetico, rappresenta la liquefazione della geopolitica. La geopolitica è fatta di cose tangibili, è la proiezione consapevole di un disegno politico sulla carta geografica. La dimensione immateriale di tutte le varie frontiere ha scarso riguardo.

La dimensione informatica è una dimensione non solo di potenza, ma anche di dipendenza. Se guardate la *slide* che apre questa presentazione, vedete che uno degli schermi ha una flebo o un'iniezione di eroina nella vena di chi usa costantemente i mezzi informatici. Non si tratta soltanto delle persone affette da dipendenza e più o meno giovani, ma proprio del fatto che tutti noi siamo connessi necessariamente a questo tipo di rete.

Il mondo non è più lo stesso, decisamente no, ma qualche volta siamo ingombrati da una serie di categorie anche tradizionali e familiari inconsce che non ce lo fanno vedere nella sua nuova dimensione. Tra un po' di tempo vedrete che le linee sulla carta geografica che ancora studiamo, naturalmente, a scuola e nelle varie carte politiche sono delle linee immaginarie. Qualche volta movimenti terroristici come *Dawla*, ossia lo Stato islamico, si incaricano di farci vedere che

queste frontiere sono molto immaginarie. Infatti, non esistono più una Siria e un Iraq, ma esiste un « Siraq », se volete.

In un mondo liquido, perché la frontiera dovrebbe essere una barriera ? Capisco che adesso in Europa centrale la gente si affanni a erigere muri, ma in realtà i muri hanno sempre funzionato molto poco, a cominciare dal *limes* romano e dalla Grande muraglia cinese. Oggi uno Stato intelligente è quello che sa usare la delimitazione legale, che noi chiamiamo anche frontiera, come una spugna, ossia come un filtro attivo e non solo passivo, non solo come un intercettore di cose negative, ma anche come un trampolino per scambiare delle cose positive.

La quarta *slide* raffigura la realtà dei traffici legali aerei. La quinta mostra, invece, la realtà dei traffici marittimi. Come vedete, c'è una serie di *plot*, di linee che collegano i vari porti, ma, per il resto, siamo fuori dalle dimensioni di frontiera a noi molto care. Ogni storia di contrabbando dimostra che le frontiere sono permeabili e gli stupefacenti lo dimostrano ancora di più. In questo senso i migranti sono molto più facili da intercettare.

La *slide* intitolata « Mondo e poteri » ci introduce in un mondo in cui lo Stato è in « sfarinamento » o svuotamento finanziario e, purtroppo, proprio sul Mediterraneo tocchiamo questo fenomeno con mano in modo molto plastico. Tutta la catena di Stati che vanno da Nouakchott a Kiev sono o visibilmente sfarinati, o disfunzionali, o a rischio di dissolversi o comunque di diventare molto evanescenti.

Un tempo potevamo dire che il Nord del mondo è quello capace di fornire risposte, ma, se avete un Nord del mondo svuotato finanziariamente, capite bene che esiste un problema di operatività. Non ci sono dei pieni, ma ci sono dei vuoti. Fare surf in mezzo alle onde vuote è un esercizio estremamente rischioso.

I poteri emergenti e forti non sono statali. La stessa *slide* riporta tre o quattro parole che vi danno un quadro abbastanza chiaro. Naturalmente, le mutazioni del cyberspazio sono parte di questi poteri forti emergenti, oppure già assai emersi. Spesso ci sono visioni geoeconomiche e, quindi, proiezioni di progetti economici, proiezioni consapevoli sulla carta geografica, che apparentemente sono statali, ma che, in realtà, sono guidate da *lobby* non statali. Abbiamo un problema di identificazione, almeno mentale, di quali sono gli attori, prima ancora di decidere quali sono i nostri avversari.

I tre blocchi di punti della *slide* « Equilibri e poteri » vi fanno vedere come siamo passati da un mondo bipolare, che conoscevamo molto bene, a una brevissima stagione unipolare, che non è durata più di dieci anni. Alla fine, tra l'unipolarismo consociativo di Herbert Bush e di Clinton e quello coercitivo « o con noi o contro di noi » di Bush, tutto questo è durato fino al 2004. Subito dopo abbiamo avuto un multipolarismo che non è anarchico, ma « disarchico », ossia che non ha una chiara gerarchia riconoscibile nonostante ci siano dei numeri uno. Non c'è più un ordine strutturante.

Questo lo vediamo in modo molto chiaro anche con eventi che abbiamo tutti vissuto. Quando siamo andati in Afghanistan, come NATO, c'eravamo tutti e 28. Quando siamo andati in Libia, eravamo nove e due col tassametro. Quando dovevamo andare in Siria, c'erano due dichiarati, ma non ci è andato nessuno. Quello che molti commentatori si ostinano ancora a chiamare l'Occidente è ormai una quadriglia a geometria variabile, ma questo vale per tutto il mondo. Non ci sono assi.

La conseguenza, come vedete, è un multipolarismo disfunzionale. Le grandi Istituzioni funzionano male, e funzionano male perché spesso si scelgono dei presidenti di Commissione e dei Segretari generali mediocri, ma questo è solo il sintomo di una scelta.

Ovviamente, da analista, sto parlando di grandi Istituzioni internazionali e tutti sappiamo trarre le conseguenze con grande rapidità. Tuttavia, da analista, sono costretto, anche parlando come NATO *Defense College Foundation*, a guardare in faccia la realtà per quella che è. Quello però è un sintomo, che poi diventa anche causa a valle. Il sintomo è che 10, 20, 30,

200 Stati scelgono delle persone che non sono capaci di manovrare più di tanto la macchina.

Questo ci porta alla fine dei blocchi, già da un bel pezzo, all'emergere di reti che dei vari gruppi di Stati se ne infischiano e alla competizione, anzi alla « copetizione » ingarbugliata, che è una collaborazione-competizione. Non ci sono rapporti univoci. Nemmeno oggi tra Stati Uniti e Russia ci sono rapporti univoci di ostilità. Questo è piuttosto visibile.

Per affrontare questo mondo è bene guardarlo con altre lenti. Una di queste è il concetto di *geonetwork*, ossia di reti di interessi, che possono essere pubblici o privati, che vengono geograficamente organizzate attorno a dei grandi oceani. Nella *slide* « I Geonetworks » in azzurro vedete il *geonetwork* Pacifico, in verde quello Indiano, in rosso quello Africano, che è ancora un continente tutto sommato piuttosto isolato, e in giallo quello Atlantico, che non è più il *geonetwork* del Nord Atlantico. La realtà dell'Atlantico del Sud, che ci piaccia o no, è molto importante.

Un altro modo per capire questo mondo molto diverso è vederlo per faglie di interessi economici primari. La *slide* « Le faglie » si riferisce proprio a un'economia di base: primaria, secondaria e terziaria. La rossa è la fascia di Paesi che campano di industria estrattiva o agricola, ossia di materie prime soprattutto. La gialla rappresenta i Paesi che, invece, sono soprattutto economie di trasformazione. In arancio c'è il misto – Corea del Sud, Giappone e Hong Kong – tra manifattura e finanza. Infine, in discretissimo grigio fumo di Londra, c'è un'ellisse che unisce i due Stati più finanziarizzati – se così si può dire – al mondo, cioè Regno Unito e Stati Uniti.

Questo tipo di divergenze sono le cose che fanno le guerre mondiali, non il conflitto in Ucraina o un terrorista che spara a un arciduca d'Austria, peraltro privo di reali poteri. La faglia allora era tra Gran Bretagna e Germania, potenze esportatrici, tecnologiche e finanziarie in chiara competizione. Quella che poi, correttamente, viene chiamata la Seconda guerra dei trent'anni gira intorno a quali attori? Inizialmente Gran Bretagna e Germania e poi, immediatamente dopo, i due veri vincitori della Seconda guerra mondiale, Stati Uniti e Unione Sovietica. È lì che si toccano le divergenze di interessi, che sono componibili politicamente, ma che, se lasciate andare per il verso loro, per inerzia, portano quanto meno a frizioni estremamente serie.

Un altro modo per guardare questo mondo – la *slide* « The 7 shaping flows » tocca proprio l'essenza delle reti – è quello dei cosiddetti flussi strutturanti. A sinistra avete la gerarchia per le economie ricche, a destra la gerarchia per le economie di sopravvivenza. In realtà, come stiamo capendo, l'ecosistema è fondamentale per tutti. L'ecosistema è un flusso. Seguono poi l'acqua potabile, il cibo, le migrazioni reali e virtuali – anche con un *call center* o un'università virtuale c'è una migrazione – l'energia convenzionale e non convenzionale (il non convenzionale è chiaramente il rinnovabile; l'energia digitale è quella che combina a fondo i vantaggi della digitalizzazione delle fonti energetiche), gli investimenti di capitale fisso, investito e finanziario e, infine, la conoscenza. È chiaro che tutto il mondo *cyber* è legatissimo al flusso della conoscenza, ma è anche molto legato ad altri flussi, come vedremo presto.

La *slide* « Root nameserver: residenza iniziale » indica i *root name server*, ossia i *server* che fanno funzionare internet, quelli che deconfliggono una serie di attribuzioni, nomi e situazioni. Questa è la residenza iniziale, che prima era molto fisica. Ce n'erano grossomodo dieci negli Stati Uniti e il resto – molto pochi – fuori.

Tutto questo è diventato rapidamente demoltiplicato e distribuito. La residenza fissa di queste masse di *server* è rimasta ancora in quattro posti. Negli Stati Uniti sono diventati ormai due o tre. Gli altri sono stati distribuiti attraverso Anycast, ossia una demoltiplicazione che permette la ridondanza della rete.

Esiste un fatto estremamente fisico: Internet non può funzionare senza queste macchine e, ovviamente, non può funzio-

nare senza un'altra cosa importante, i cavi di comunicazione transoceanici, che sono le vere dorsali di comunicazione, insieme a quelle continentali, e la distribuzione della fibra nelle città. Prima di quella c'erano la *strata* romana e la ferrovia. Questo era l'Internet del passato. Questo è quello che abbiamo oggi. Mancano in questo quadro le comunicazioni satellitari, che in realtà sono una frazione minima, come capacità di trasporto dati. Tuttavia è utile tenerle presenti anche se è il cavo quello che trasporta di più.

La *slide* « Dimensione cyber-statale » rappresenta una rapida storia, di cui ovviamente vi risparmio i dettagli, di un po' di azioni statali nel cyberspazio, con una serie di bandierine che vi fanno capire chi si sta attrezzando e perché. Volevo solamente attirare l'attenzione su alcuni attori più di altri, perché sono spesso quelli più dimenticati.

Come vedete nella successiva *slide* « Dimensione cyber-statale II », la NATO, dopo l'attacco all'Estonia, ha avuto un ruolo importante e questo suo Centro di eccellenza nella difesa cibernetica sta svolgendo un ruolo attivo anche, come vedremo, nelle questioni ucraine. Come quantità di denaro immesso, però, siamo a livelli molto bassi. Questo è un problema dell'alleanza, che andrebbe affrontato, ma non è l'unico, devo dire. Vedremo che risultati ci darà Varsavia.

I problemi informatici dell'Ucraina non sono nuovi. Risalgono già al 2012, ben prima della crisi di Maidan Nezalezhnosti. Come vedete nella *slide* « Ucraina », a destra c'è una serie di attori che sono stati più o meno presenti in questo tipo di vicende. L'ultimo è CyberBerkut, un gruppo assolutamente privato, che però sostiene degli interessi – chiamiamoli così in senso lato – separatisti. C'è anche lo stesso Sandworm. Sono tutte organizzazioni private. L'attacco più recente è arrivato alle elezioni.

La Romania è la nazione guida proprio per conto di questo centro di Tallinn, il CCDCOE, come lo vedete raffigurato nella successiva *slide* « Ucraina II » in quella sorta di disegno un po' propagandistico che rappresenta lo scontro tra il serpente e l'aquila, ma la capacità di attacco di una serie di attori è piuttosto interessante.

Non si tratta mai di un attacco decisivo, per ora. Parlare di cyberguerra tra Ucraina e Russia è, francamente, esagerato. Certamente c'è una serie di azioni molto significative, ma l'elemento statale cerca sempre di avere un profilo estremamente basso, evidentemente per motivi di interesse. Non mi sembra che Putin appartenga alla categoria dei santi.

È interessante notare, però, che Kiev, almeno per quello che ancora si riesce a sapere oggi, non è riuscita a mettere in piedi un centro di comando difensivo identificabile nelle faccende di cybersicurezza. Probabilmente avrà un CERT, ma non una struttura di livello superiore.

È interessante notare, invece, che altri Governi l'hanno fatto, come il Brasile, per esempio, già dal 2010, e l'Iran, che è stato vittima e, quindi, ha messo in piedi un'organizzazione, in mano – guarda caso – ai Pasdaran. Si tratta di un comando di cyberdifesa, che però fa parte di un comando di difesa passiva civile che fa parte dello Stato maggiore della difesa, un *composé* piuttosto interessante. Poi c'è l'India.

Attiro l'attenzione su questi attori perché sono, in genere, dimenticati, mentre invece la dimensione c'è. Se anche non esistesse Internet, siamo già in un mondo globale. Quello che accade a Canicattì potrebbe avere la stessa rilevanza di quello che accade a Nauru nel Pacifico profondo. Se non adottiamo questo tipo di mentalità, veniamo regolarmente sorpresi.

È interessante notare che la Segreteria di Stato vaticana ha al suo interno gli affreschi del mondo del Quattrocento, sempre. Non è la palla di Giò Pomodoro fuori. Non c'è bisogno di affrescare adesso la Camera, ma mentalmente è importante capire che l'Italia non è semplicemente un posto dell'Europa, del Mediterraneo e dell'Atlantico. È un posto nel mondo, e nella realtà cibernetica questo è proprio evidente.

Le quattro *slide* riferite all'Area cyberterroristica ci danno un po' l'idea di quello che fanno i terroristi. Soprattutto adesso

va molto di moda la dimensione jihadista, che peraltro è ormai vecchia dal 1979. Che cosa fanno soprattutto ? Lavorano innanzitutto alla cifratura, perché si devono difendere. È abbastanza ovvio.

Si è fatto tutto un gran parlare del danno che avrebbe fatto Snowden in materia di facilitazione agli avversari degli Stati Uniti. In realtà, i problemi delle organizzazioni jihadiste hanno, al limite, avuto un'accelerata, ma erano già preesistenti.

Viene fornita anche un po' un'idea di prodotti che circolano in spazi più o meno protetti o più o meno profondi della rete e questo permette, naturalmente, di avere delle cifrature che per loro si spera siano abbastanza resistenti.

Infine c'è anche una breve infografica degli attacchi che sono stati fatti su ispirazione ISIS che evidenzia come siamo ancora a livelli che non hanno niente a che vedere con quello che possono fare attori statali in *partnership* pubblica-privata.

Ovviamente, c'è la dimensione del *cybercrime*, che ha degli attori molto interessanti. Guardate che l'Unione europea fa il 24 per cento mondiale del crimine cibernetico. Praticamente è alla pari degli Stati Uniti. Questi sono dati, purtroppo, del 2013, ma per i dati dipendiamo da pochissimi fornitori, come le grandi case di *software* antivirus, per esempio. Questo è un problema di conoscenza che a livello statale va senz'altro affrontato.

È interessante vedere chi sono le fonti – questi sono dati del 2015 – di attacchi cibernetici criminali. È seccante notare che tra i primi cinque ci sono Stati amici. Questo perché certamente c'è uno sviluppo di infrastruttura, di cultura e anche di opportunità, però il cybercrimine non è semplicemente dentro i confini di uno Stato.

In serie B arrivano i soliti sospetti usuali, ma anche dei sospetti un po' meno usuali. Per esempio, la Cina è il sospetto usuale, però Brasile, Francia e Australia lo sono un po' meno. Ovviamente, per gli americani la Francia è molto più sospetta, ma queste sono finezze politiche interne. I russi sono in serie C, eppure hanno delle cybermafie estremamente sviluppate che hanno creato dei modelli di *business* molto innovativi che continueranno.

La *slide* « Peso globale delle attività ostili » mostra, quando ancora si parla di cyberguerra, il peso reale delle diverse attività ostili, quindi nell'*hacktivism* che è un 30 per cento scarso, cioè un 29,2 per cento; rientrano ovviamente tutte le dimensioni anche cyberterroristiche contro dei siti e non quelle contro delle infrastrutture più dure o più protette, mentre il resto è soprattutto crimine, molto poco è spionaggio e un pochino di più è quello che si potrebbe chiamare « cyberguerre ».

Questo dà un'idea di quanto sia pesante il settore privato, se volete, e dà anche un'idea forse della prudenza con cui poi gli Stati, nonostante gli annunci e nonostante gli investimenti, vogliano veramente buttarsi in questo tipo di attività. Riguardo lo spionaggio, bisogna vedere quanto è calcolato correttamente perché molte persone spiate che scoprono di avere avuto i *computer* violati non lo dicono in giro per ovvi motivi. Tuttavia, anche se la quantità di spionaggio fosse superiore (certamente noi abbiamo visto casi abbastanza eclatanti), il resto per ora è quanto appena descritto.

Quale sarà la situazione di scenario a breve, ovvero entro il lasso di due anni ?

C'è una corsa contro il tempo tra diffusione legale e illegale di tecnologia, cioè lo spazio cibernetico è un luogo di diffusione di potenza dallo Stato o dai grandi Paesi verso quelli più piccoli e soprattutto dall'entità legali a quelle illegali, quindi c'è un problema di mantenere un vantaggio. Per ora, i Paesi che noi conosciamo come amici sono ancora forti, ma la crisi taglia anche questo tipo di spesa perché non sono soltanto le spese militari quelle che contano, ma anche le spese civili. È chiaro che, se io ho dei mercati in contrazione, pochi possono mandare avanti ricerca e sviluppo.

Tra gli emergenti, abbiamo Paesi citati più volte: Brasile, Cina, India, Israele, Messico, Turchia e Sudafrica. Oggi, guardando con occhi politici la dimensione

cibernetica della Turchia, se siete greci questo problema ve lo ponete già da vent'anni e se siamo italiani dobbiamo avere un occhio di attenzione, non a caso tutti i Paesi BRIC e l'Iran sono dotati di comandi cibernetici.

Sui possibili fronti a breve vorrei darvi i risultati di un'attività di ricerca che si è svolta quest'anno. Ormai, sono dieci anni che conduco questo tipo di attività, prima sotto l'egida di Nomisma e all'interno del Centro militare di studi strategici (CeMiSS) fino all'anno scorso, per cui quella ricerca è praticamente la continuazione del mio lavoro. Si tratta del *Global Insight 2016* dove un'*équipe* di giovani ricercatori ha fatto una selezione a tappeto degli eventi rilevanti mondiali, quindi non degli eventi notiziabili o degli eventi più clamorosi che vengono anzi regolarmente scartati, per vedere quali siano le tendenze che a breve sono di un certo interesse.

Vi evidenzio soprattutto le cose che hanno più attinenza con il nostro discorso di sicurezza informatica.

La prima cosa che salta all'occhio è il parassitaggio tra terrorismo e crimine organizzato. C'è già un'economia globale delle droghe, tramite soprattutto i traffici marittimi che sono quelli ancora una volta con più volume, quindi, se diciamo marittimo, per noi si intende nel Mediterraneo per primo il porto di Gioia Tauro e, per secondo, il porto del Pireo. C'è una circolazione di droghe ormai a livello globale, cioè un nastro trasportatore. Per carità, gli attori sono frammentati e a volte litigano e a volte si uccidono, ma questa saldatura globale è già in atto, sia pure attraverso diversi pezzi.

Riguardo alle tendenze del Pacifico che però sono di valenza globale, c'è la corsa ai grandi trattati (TPP, TTIP, TISA); poi vi spiegherò perché attiro la vostra attenzione su questo punto. Inoltre, c'è la fine della svalutazione competitiva che è la corsa al ribasso.

Poi ci sono dei cambi demografici negli Stati Uniti che stanno ponendo non solo un problema di maggioranza-minoranza. Gli Stati Uniti non sono più *wasp*, quindi c'è la vendetta di Santa Anna contro Davy Crockett, se volete in parte, ma è ancora più importante l'invecchiamento dalla popolazione. I lavori di estensione della vita attraverso le biotecnologie o la robotizzazione e quindi un paradigma tecnologico di una tecnologia adattata ai vecchi, cioè una gerontotecnologia, stanno trasformando il modo di intendere la tecnologia per degli impieghi anche di supremazia.

L'altra cosa su cui bisogna stare estremamente attenti è la possibilità di avere un secondo *tsunami* economico perché c'è la bolla del debito cinese, nonché il finto *deleveraging* statunitense. A livello globale, noi siamo indebitati oggi al 100 per cento. Nel 2006, quando questa crisi è iniziata, eravamo al 70 per cento del PIL mondiale.

A livello di Oceano Indiano, c'è la crisi idrica che tocca alcuni Stati in modo evidente e c'è quello che io chiamo il « trio islamico » tra Islamabad, Riad e Paesi del Consiglio di cooperazione del Golfo. Che cosa è ? Da una parte ci sono le banche islamiche e, dall'altro, il finanziamento al terrorismo.

Non voglio assolutamente stabilire dei collegamenti meccanici tra finanza islamica e terrorismo jihadista perché non ce n'è bisogno. Ai bei tempi dei *freedom fighter* contro l'Unione sovietica in Afghanistan, l'*Islamic banking* non c'era, eppure sono stati finanziati in maniera massiccia. Voglio soltanto dire che la finanza islamica si sta sviluppando come un possibile contraltare alla nota finanza internazionale, pur essendo spesso guidata da persone che vengono da esperienze finanziarie che potremmo chiamare « occidentali ». Inoltre, il finanziamento dei terroristi non è soltanto una questione di armi, ma è una questione di capacità di porsi con dei flussi in alcune intersezioni che potrebbero contare.

Veniamo all'Africa, dimenticatissima nel nostro dibattito e a torto. Il continente africano cresce di valore strategico. Non è un caso che a Gibuti ormai si diano l'appuntamento e che lì ci siano le basi di quattro Paesi di cui due assolutamente improbabili, cioè Giappone e Cina. Gibuti significa Bab el-Mandeb, che significa Yemen, che significa Somalia, che significa

Suez, che significa ancora volta Gioia Tauro. Un tempo, quando eravamo giovani, si diceva « la Cina è vicina », mentre oggi è dentro casa, non è più da un'altra parte.

C'è un altro aspetto interessante: il ritorno sugli investimenti in Africa è alto per ora. Per carità, una serie di Paesi stanno conoscendo anche loro crisi perché sono stati presi in contropiede dal crollo dei prezzi energetici. Inoltre, c'è un'altra corsa agli investimenti e agli accordi di libero commercio.

Concludiamo con i *trend* atlantici: due sono visibilissimi e, il primo, è dato dai problemi del Brexit, malamente scongiurato perché si poteva scongiurare in un altro modo, e da quello della conclusione TTIP. L'altro *trend,* meno visibile, è quello di una competizione industriale tra modelli industriali, con tanti saluti alla nostra deindustrializzazione.

Questo tipo di competizione è anche nelle difese cibernetiche perché, come voi vi ricordate, la cancelliera Angela Merkel era ben poco divertita da tutta la faccenda di NSA-Prism, detta « Datagate ».

Passerei ad alcune conclusioni. Le vecchie categorie geopolitiche vengono liquidate perché esistono delle dimensioni fisiche e statali, ma sono permeabili da reti bianche, nere e grigie. Noi italiani non abbiamo bisogno di grandi spiegazioni. Quello che possiamo usare, come parola inglese, è « *netchwork* », cioè un *network* che però funziona come un *patchwork*, quindi una cosa molto diseguale e, se volete, di stile medievale.

I fronti sono individuabili principalmente per asimmetrie informative da mantenere o da creare. I mercati finanziari – ormai è noto a tutti – si reggono sulle asimmetrie informative: dove c'è un'asimmetria informativa, c'è un interesse di attività offensiva e difensiva cibernetica, per cui è inutile tagliarle con il bisturi, visto che sono come gemelli siamesi; non funziona così in quest'ambito e non ha mai funzionato nemmeno in ambito fisico.

Un aspetto interessante è costituito dai flussi energetici e dai flussi finanziari. Si tratta di un'accoppiata di flussi che sono in cima, dopodiché ci sono le tecnologie, l'industria, i servizi, il trasporto eccetera, quindi, se volete avere una prima sensazione di dove possano nascere dei problemi, avete un parametro abbastanza ampio e flessibile.

Non ci sono cassetti né amici stabili. C'è purtroppo un *continuum* da una dimensione all'altra. Credo che il concetto cristiano di pericoresi, quindi di scoloramento da una persona della Trinità all'altra (anche se qui non siamo nel caso della Trinità) sia estremamente efficace, cioè c'è una circolarità, c'è un continuo scambio e c'è un continuo trascolorare dal legale al grigio, all'illegale, esattamente sotto, e dalla finanza visibile a quella a ombra che non è mai stata regolata, nemmeno da Obama.

Inoltre, ci sono il riciclaggio, il cyibercrimine e le mafie. Segnalo l'ascesa della mafia messicana nel settore cibernetico perché è già in corso una guerra mondiale mafiosa al ritmo di 10.000 morti all'anno, di cui il Papa si è ricordato solo ora, anche se ci voleva poco francamente. Certo, è bene che ce ne ricordiamo perché chi dice mafia messicana dice 'ndrangheta.

Infine, c'è un collegamento di fatto tra mercati e fornitori legali con quelli illegali. Il mercato degli antivirus legali è connesso fisicamente – non sappiamo quanto sottotraccia – con le reti nere che sono i grandi *bazar* di strumenti informatici per fare qualunque cosa: violare, decifrare e cifrare in modo da sottoporre al riscatto la ditta che è stata presa in ostaggio.

L'altra cosa importante da capire, come ci hanno mostrato i nostri amici russi, anche se credo che insomma anche gli altri abbiano più o meno seguito la stessa regola, è quella di servirsi di *contractor* privati. In effetti, non c'è attività statale senza *contractor* privati. Peraltro, un esempio italianissimo è il Tiger team. Studiamo per favore le faccende che facciamo noi perché spesso siamo all'avanguardia. L'Italia è uno straordinario laboratorio politico e quello che succede nel politico, nel sociale e nell'economico poi regolarmente si scambia con la dimensione *cyber*.

Questo porta alla produzione di strumenti che sono chiaramente strumenti ideati da persone, ma che hanno larga autonomia. Ecco perché li ho chiamati « *avatar* » o vengono chiamati « *avatar* ». Non dimentichiamoci che l'*high frequency trading* è totalmente robotizzata, cioè c'è l'omino o la donnina nel *loop*, ma per premere il pulsante d'emergenza, secondo me, con grande ritardo. Certo, la dimensione di Skynet di Terminator era mitica nel film, ma realissima per la finanza a ombra e per la finanza ad alta frequenza di commercio e scambio, cioè di *high frequency trading*. Questo si dovrebbe trascolorare nell'atto illegale. Dunque, che cosa fare ?

Innanzitutto, dire che è una faccenda puramente di mercato significa assolutamente ficcare la testa sotto la sabbia, fare cioè la politica dello struzzo. Noi abbiamo già fatto delle cose, per cui non partiamo dall'anno zero in Italia. Tuttavia, è importante fare un passo in più e capire che è la dimensione del partenariato pubblico-privato e non più solo a « umma umma » perché per ora è la dimensione personalistica che rappresenta la struttura. È importante che ci sia una dimensione, invece, strutturata, non so quanto da un punto di vista legale che è una dimensione importante, ma sicuramente da un punto di vista di strutture che vadano oltre le persone, altrimenti con Tavaroli si chiude un'esperienza giudiziaria e si chiude anche un'esperienza pratica.

Questo, giusto o sbagliato, è un *know how* che si disperde. Dobbiamo stare attenti, invece, a saper mantenere uno spazio privato sano, in modo da fare *partnership* decenti col pubblico perché, altrimenti, succede che si fanno *partnership* anche con elementi mafiosi. Cina e Russia credo che siano esempi abbastanza interessanti, ma non sono affatto i soli.

Ci vuole una dimensione digitale della geopolitica, cioè bisogna pensare questa dimensione e bisogna capire che le catene di fornitori che sono globali sono esposte a questo tipo di rischi.

Vi do un solo esempio, non informatico, ma molto fisico. Abbiamo una marea di grandi imprese in Messico e mi chiedo quanto sia controllata e certificata la catena dei fornitori locali e dei flussi finanziari. Si tratta di una domanda semplice.

Io, a questo punto, lascio spazio alle domande e vi ringrazio per l'attenzione.

PRESIDENTE. Grazie da parte nostra al professor Politi per la ricchezza della sua presentazione. Autorizzo la pubblicazione in allegato al resoconto stenografico della seduta odierna delle slide di tale presentazione *(vedi allegato)*.

Do la parola ai colleghi che intendono intervenire per porre quesiti o formulare osservazioni.

MASSIMO ARTINI. Ringrazio il professor Politi perché la sua presentazione è stata indubbiamente inusuale, anche se è un po' quanto mi aspettavo.

Effettivamente, soprattutto con riguardo, alla parte geopolitica e agli eventuali futuri aspetti di criticità ci sono delle cose che al momento non avevamo trattato.

Uno spunto che mi piace vedere riportato anche in questa presentazione e che mi preme sottolineare, come ho già fatto con altri esperti che l'hanno preceduta, è che questo mondo distrugge le alleanze reali.

Mi riferisco ai fatti relativi al Datagate che lei ha riportato, ma anche all'ormai nota capacità da parte di Paesi alleati di introdursi formalmente nei nostri sistemi informatici per acquisire determinate informazioni. Tutto ciò distrugge quel mondo su cui erano basate tutta una serie di relazioni e che, successivamente, ha portato in questi anni a quella disfunzionalità di cui parlava.

In primo luogo, è molto interessante il ragionamento sul fatto che il 67 per cento delle casistiche di danni cibernetici sono per crimini, quindi, tendenzialmente nel mondo privato. Essendoci questo grande impatto sul mondo privato, mi chiedo come lo Stato possa agire su questo e se ci sono esperienze efficaci. Il ragionamento è che si può strutturare il sistema in modo che sia tarato per poter suppor-

tare un attacco di tipo informatico da un punto di vista statuale, ma la domanda riguarda come si possa reagire per quanto riguarda l'economia, cioè la parte che impatta sul privato.

L'altra domanda si riferisce alla valutazione che lei ha fatto, anche su molti Paesi, rispetto a chi ne è competente. Vedo che in Italia c'è una valutazione sulla catena di comando, mentre in altri Paesi è coinvolta in particolare la parte della difesa. Le chiedo di esplicitare questo concetto perché è importante comprendere come il partenariato pubblico-privato deve essere regolamentato.

Ritengo che – magari su questo si può anche discutere – non si possa lasciare al privato la facoltà di autoregolamentarsi, altrimenti nessuno pubblicherà mai le informazioni sensibili su eventuali attacchi; piuttosto è il settore pubblico che deve svolgere un ruolo fondamentale di garanzia.

Abbiamo perso, e questo probabilmente è un po' colpa della mancanza di concretezza della politica in questi anni, la volontà di verificare questo mondo. Mi ricordo che già nel 2007, quando era Presidente del Consiglio il Presidente Prodi, ci fu una forte diatriba e un momento in cui si volevano riportare nella sfera pubblica le dorsali informatiche italiane. Ci troviamo oggi come uno dei pochi Stati del G7, o comunque del G20, a non avere una dorsale nazionale di cui possiamo avere un controllo.

Concludo, così lascio spazio anche gli altri colleghi, con una considerazione che riguarda un punto fondamentale, ossia la *supply chain*, la catena di forniture. Per un Paese, per esempio, come il nostro, in cui le forniture sono basate solamente su tecnologie che vengono da fuori, questo aspetto costituisce un problema. Quali studi, quali possibilità e quali sistemi occorrono per iniziare ad avere un controllo delle nostre catene di approvvigionamento informatico e un eventuale futuro in cui almeno alcune componentistiche (siano esse *software*, *hardware* o *firmware)* provengano da produzioni o sviluppi italiani ?

GEA SCHIRÒ. Grazie, presidente, anche per l'ospitalità. L'audizione del professor Politi era un'occasione troppo interessante per perderla. Da profana, le pongo due domande, professore.

Lei cita di passaggio il TTIP, ma non parla dell'intenzione della Cina di diventare un'economia di libero mercato. È la tenaglia che schiaccia l'Europa. Da un lato, c'è un Paese che vuole accedere non essendo un'economia di mercato statale, finanziata e non regolata. Dall'altro, c'è un trattato, il TTIP, su cui ci sono molte polemiche, a mio avviso spesso infondate.

Per esempio, in Italia c'è una grande polemica sull'agroalimentare. Vediamo, invece, che un Paese come la Francia, che vive di agroalimentare, non pone problemi, perché ne vede con lungimiranza anche alcuni vantaggi, mentre un Paese che sarebbe meno vocato, come la Germania, è quello che ha posto più problemi. Qui torniamo a uno dei gangli che lei aveva posto fra i *root*, ossia alla tecnologia, alle materie prime e alla finanza. Mi riferisco al problema della Germania nell'accettare il TTIP. L'Italia è su una posizione saggiamente di mediazione su queste due questioni, ma sta in Europa e, in prima battuta, da una parte, è vincolata a questo sistema a tenaglia.

Dall'altra parte, vedo che nella *slide* intitolata « Che fare ? » arriva ai rischi legati alla gestione delle *supply chain*, in pratica alla cornice di sicurezza attorno ai prodotti. Questo punto è un po' legato a quello che il collega Artini ha detto prima.

La domanda è un po' metafisica: non crede che, oltre alla produzione e a tutto quello che è il *cyber* della produzione – penso, per esempio, alla Volkswagen e all'alterazione, dell'*engine* – sia anche il controllo sul prodotto a creare l'anello di passaggio, la catena che lega il « consumatore » del materiale, sia esso buono o cattivo, alla provenienza ?

Lei ha fatto l'esempio dei beni prodotti in Messico. Non crede che il consumatore sia davvero l'ultimo anello e non ancora la fase di produzione ?

Aggiungo che sono d'accordo che si debba chiarire anche, come diceva il col-

lega Artini, il rapporto pubblico-privato, che può essere solo virtuoso, avendo però dei ruoli e delle vocazioni definite.

ANGELO TOFALO. Grazie, professore, per l'ottima analisi, che credo sia il sunto di uno studio e di un lavoro molto più approfondito. Vorrei partire dalle conclusioni. Al di là della *partnership* tra settore pubblico e privato, vorrei che spiegasse un po' di più questa creazione della dimensione digitale della geopolitica come base di partenza, sulla quale concordo.

Ho trovato molto significativa la *slide* intitolata « Le faglie », cioè quella sugli interessi economici primari. È un po' la mappa del disequilibrio mondiale. Siamo passati, come lei ha detto, da un mondo bipolare fino alla competizione tra blocchi e alla copetizione ingarbugliata. Prevede in questa creazione della dimensione digitale un'analisi su larga scala per riequilibrare un po' le risorse ? La politica italiana è quasi ininfluente ed è chiaro che bisogna ragionare a livelli europei, occidentali e globali.

L'obiettivo della politica, dunque, può essere quello di ridistribuire le risorse ?

PRESIDENTE. Do ora la parola al professor Politi per la replica.

ALESSANDRO POLITI, *Direttore della NATO Defense College Foundation*. Comincio subito dalla questione della NATO e dello scandalo NSA PRISM. Innanzitutto io non sono tra quelli che dicono: « Che cosa c'è da stupirsi ? ». No, evidentemente c'è da stupirsi, e anche parecchio. È interessante notare che due leader donne sono state molto stupite e molto seccate. Mi riferisco alla cancelliera Merkel e alla presidentessa Dilma Rousseff. Credo che avessero le loro ottime ragioni. Tanto solide sono tali ragioni che il prossimo cavo interoceanico brasiliano verrà realizzato escludendo sistematicamente dei fornitori americani.

Che questa sia una dichiarazione di principio che sotto banco poi può venire modificata è un altro paio di maniche. Siamo italiani, ragion per cui non abbiamo bisogno di perdere molto tempo su queste cose. Tuttavia, chiaramente l'uso più che spregiudicato, direi non politico, degli strumenti di *intelligence* ha creato un grosso danno politico. Questo è un punto.

La prova del nove è data dalla legislazione che propone il Presidente Obama, che è il primo presidente democristiano degli Stati Uniti, e si vede. Nonostante tutto quello che qualunque tecnico del mondo informatico e del mondo di *intelligence* possa dire – va bene, ci mettiamo il contentino – nel frattempo, passa un principio legale per cui il *cives romanus* non è soltanto quello statunitense, il che a livello informatico non è banale.

È vero che si possono ammazzare un sacco di persone con i droni avendo una procedura legale inappuntabile. Se andate a vedere un poco la catena di comando e di autorizzazione per ammazzare un singolo terrorista, notate che è impressionante. Nel frattempo, però, è passato il principio che l'uso disinvolto di strumenti di *intelligence*, soprattutto a strascico, non è accettabile. Questo è un punto su cui poi si può vedere come ricostruire il senso politico delle alleanze.

Peraltro, le cose sono collegate. Se si è arrivati a questo, il senso politico delle alleanze si è indebolito già un bel po' prima. Oggi guardiamo l'ultima causa, lo spostamento a Est, ma è chiaro che, finita la Guerra fredda, sono cambiate alcune cose. È cambiata l'Europa, sono cambiati gli Stati Uniti e la qualità delle decisioni politiche ha portato a questi frutti. La scelta di avere una guerra al terrore è stata una scelta controproducente per una serie di interessi, tanto per cominciare per quelli nazionali statunitensi, ma – abbiamo visto qual è stato il rapporto costo-benefici – anche per quelli degli alleati. Questo è frutto pieno, perché con il *Patriot Act* si è permesso di tutto e di più. Si tratta di un problema non solo di astratta civiltà giuridica, ma anche di priorità di valori, almeno laddove si spera che le democrazie abbiano dei valori operanti, e della loro traduzione pratica. È un punto che va senz'altro ripreso.

Quanto alla catena di comando, qui abbiamo portato degli esempi militari, perché sono quelli più facili, in fondo, da tracciare. Ho l'impressione che ogni Paese – penso a quelli anglosassoni, a un Paese come la Francia o anche a quello tedesco – abbia voglia di strutturare una serie di idee molto chiare e di divisioni di competenze. Nella realtà, credo che avvenga molto spesso una capacità di *pooling* e di condivisione delle risorse che, anche se si avvale di strutture leggibili, è più fluida. Non lo cito necessariamente come caso dei brutti e cattivi, ma quello russo è un caso che ci dovrebbe far riflettere molto e, secondo me, anche quello cinese. Eppure sono due Paesi che pretendono di avere una politica chiara, forte, univoca e statale. Non è così.

Ho l'impressione che, come italiani, dovremmo seguire il meglio delle nostre tradizioni e non il peggio. Il peggio è la creazione *ad personam*, un male che, peraltro, si è ormai diffuso, un fatto italiano che il mondo invidia. Più giro all'estero, più mi ritrovo pezzi d'Italia che non avrei voluto ritrovarmi. Sono molto franco su questa faccenda. Il mondo si è molto globalizzato, nei due sensi. Il meglio, invece, è la capacità di saper trovare i punti di equilibrio tra interessi, che è veramente una grande capacità della politica italiana, e la capacità di saper trovare delle soluzioni non genericamente creative e flessibili, ma capaci di sapersi muovere con la realtà.

Non è infrequente nella nostra capacità politico-legislativa e poi operativa degli apparati, tanto di Stato, quanto privati. Tale capacità non va dispersa. Non voglio usare un'altra parola molto più colorita. Si può fare ed è una possibilità presente anche oggi. Questo è ciò su cui penso che sia opportuno riflettere, alla fine.

Perché ? Perché è vero che siamo l'Italia, ma è altrettanto vero che oggi l'Italia conta di più che in passato proprio perché c'è un allentamento, purtroppo dannoso, dei quadri multilaterali. Se l'Italia decide di mettersi di traverso, lo può fare e, secondo me, anche con una certa efficacia. Bisogna capire dove, come, perché, con che costi politici e in che condizioni.

Sicuramente – questo è un aspetto che non posso che sottolineare – l'Italia ha bisogno di un solido sistema di istruzione pubblica, perché il mondo nuovo ha bisogno di gente molto istruita di base. Ha bisogno, quindi, di un sistema di ricerca che funzioni e non di uno sottofinanziato e gestito in modo baronale. Sono figlio di professori universitari e, quindi, ho visto arrivare determinati danni da decenni in anticipo.

Ci vuole poi una capacità di saper evitare i costi della politica, che sono determinati dalle cattive decisioni, non dai costi dei deputati che è una questione ridicola. Si può fare e siamo in grado di farlo anche oggi. Qualche volta ci siamo riusciti.

Perché dico questo ? Perché l'Italia ha un estremo bisogno di essere ben informata. Già i *mass media* dovrebbero fare un lavoro molto serio di autoriforma, se ne sono capaci, perché altrimenti verranno soppiantati da un algoritmo che scriverà tanto gli articoli, quanto i pastoni politici, quanto anche i commenti. C'è una marea di opinionisti che sono cestinabili, non importa di che colore. Non ci mettono niente dentro. È questo il punto.

Perché ? Perché l'Italia ha bisogno di essere molto informata, in senso aperto e anche in senso occulto. Ha bisogno di una buona *intelligence*. Perché ? Perché non siamo un dinosauro. Siamo un mammifero e, quindi, o siamo svegli e svelti, oppure ci schiacciano. È la famosa tenaglia di cui parlavamo prima.

Da questo punto di vista le discussioni sull'*intelligence* sono discussioni strategiche nel vero senso della parola. Abbiamo il potenziale umano per poterlo fare e abbiamo anche un potenziale di ricerca, che però non va mortificato, altrimenti faremo esattamente come faceva l'Aeronautica militare: formava i piloti, che poi passavano in Alitalia e ciao. Il guaio è che adesso l'Alitalia si è globalizzata. Ci perdiamo dei ragazzi molto formati per nulla. Peccato.

Veniamo adesso alle dorsali e alle *supply chain*, così rispondo a due domande in una. Se dal lato del fisico determinate cose si possono fare e, secondo me, vanno fatte, è ormai tempo di ripensare al ruolo dello Stato, sapendo benissimo che lo facciamo in condizioni di vecchiaia della macchina Stato da quattrocento anni e anche di indebolimento globalizzante. Le partecipazioni statali sono finite malissimo – qui siamo in un posto che conosce a memoria come è finita la storia – ma le partecipazioni statali sono state l'unica cosa che abbia conferito un'infrastruttura seria a questo Paese, non il privato. Mi spiace e, se vedo quello che succede nel privato, non solo in Italia ma globalmente, mi dispiace doppiamente, perché è un problema serio.

Mentre per le dorsali determinate cose si possono fare, sulle catene di fornitori siamo più legati alla dipendenza e all'interdipendenza. Finché si tratta di un'interdipendenza grosso modo equilibrata, va bene, ma spesso non lo è. Abbiamo degli oligopoli. In campo informatico e in tutti i campi economici che contano il libero mercato è uscito dalla finestra, con tanti saluti ad Einaudi. Non sono tanti i compratori e tanti i venditori. Sono pochissimi i venditori, con una concentrazione di ricchezza dell'1 per cento contro il 99 oggi nel 2016, il che dimostra che non c'è creazione di valore, ma anzi c'è aspirazione di valore ed estrazione di valore. Abbiamo questo problema qui.

È chiaro che lottare contro questo tipo di potentati è complesso, ma non impossibile. Cito due casi su tutti. Quando Microsoft è stata costretta a sganciare il *browser*, Internet Explorer, dal sistema operativo, ovviamente non è stata una vittoria del consumatore, ma è stata una vittoria di Google. Alla fine, l'abbiamo capito. È possibile, però. Adesso c'è tutta la battaglia che fa la Commissione europea, che non ha certo più quel livello di terzietà di dieci anni fa, sul fatto che Google stesso vada spacchettato. Ancora una volta, è chiaro che abbiamo fili interstatali, o meglio attori interstatali e fili molto privati.

Questo è, però, purtroppo l'ambiente in cui per ora dobbiamo operare. Perché ? Perché no capacità impositiva, no Stato. C'è questo problema, che, per carità, non è nuovo. Tutti gli Stati del Rinascimento hanno subìto esattamente gli stessi problemi e la stessa crisi che viviamo. La crisi del tardo Cinquecento è in *reload* oggi ed è micidiale per tutti.

Arriviamo alla tenaglia dei trattati e delle ammissioni. Penso che i grandi trattati a guida statunitense siano un'eccellente idea che si è tramandata da due presidenze (Bush e Obama), il che dà l'idea della continuità degli interessi delle classi politiche, ma penso anche che questo tipo di impostazione, tutto sommato, risenta di una filosofia che rischia di essere superata. La filosofia è che ci voglia per forza un leader.

Mi colpisce che un Friedman di STRATFOR, che non mi pare esattamente un pacifista in gonna a fiori e *klompen*, dica che è il momento di immaginare un mondo con una distribuzione di potere non multipolare. Lui la chiama « eterarchica », con un uso del greco su cui, peraltro, possiamo discutere. Si tratta comunque di un potere distribuito con pesi, contrappesi e retroazioni a livello globale, con una condivisione in un arco più ampio.

Un altro modo per chiamare questo sistema, sempre in ambito americano, è « penarchico », il che vuole dire di nuovo non una concentrazione, ma il concetto è che forse bisogna prepararsi a una *leadership* più condivisa. Perché ? Perché siamo sempre su questo pianeta, che è un pulviscolo di nulla perso nell'immenso con scarse risorse rinnovabili.

In questo senso, la *Laudato sì'*, sfrondata di tutti i riferimenti religiosi, è assolutamente un documento di grande strategia. Parte da Al Gore e va oltre. Perché ? Perché l'ha fatta un Capo di Stato con interessi globali, punto. Non mi interessa che sia Papa Francesco, che poi è molto simpatico. Questo va oltre la mia natura personale di credente. È un dato politico.

Questo documento è assolutamente interessante perché pone il passaggio dal-

l'interesse nazionale al bene comune, che non è un bene comune irenico e astratto, ma un cambio di paradigma politico. In questo tipo di cambio di paradigma, noi abbiamo dei trattati dove si sa benissimo chi tiene il mazzo di carte in mano. Sono trattati pensati per escludere la Cina. Tuttavia, prima di pensare se vogliamo i cinesi dentro o fuori, anche se è un'ottima domanda...

GEA SCHIRÒ. Ma alcuni Paesi del Pacifico l'hanno già approvato.

ALESSANDRO POLITI, *Direttore della NATO Defense College Foundation*. Sì, ma innanzitutto bisogna vedere cosa succederà nella ratifica e poi c'è un tipico gioco di occupazione degli spazi all'occidentale e di Go alla cinese.

I cinesi hanno visto arrivare il TTIP e hanno cominciato una strategia di accordi minori che occupano delle intersezioni della scacchiera. Guarda caso, in questi accordi minori c'entrano il Giappone e l'Australia; e la banca, la zona di libero scambio del nord-est del Pacifico e la zona fatta con l'ASEAN. Si tratta di un modo per contrastare questo tipo di taglio esclusivo dove, peraltro, la prima a rimetterci le penne è l'America Latina; solo tre Paesi su quattro sono del TTIP.

Quello che è uscito del TTIP francamente non è incoraggiante. Noi siamo i creatori della diplomazia segreta, almeno dai tempi di Metternich, se non prima. Tuttavia, temo che questo metodo abbia dei problemi e che le ratifiche speditive siano assolutamente una cosa da evitare, perché la domanda è: che razza di *partnership* facciamo con il Paese più indebitato al mondo? « *I'm sorry, money is money* », ma chi è che paga i debiti? Finora li hanno pagati i cinesi, ma, se sono in fase recessiva, chi li paga? I tedeschi e noi?

Gli accordi di libero scambio sono una gran bella cosa, ma facilitano il commercio, come mi ha spiegato un diplomatico messicano, non creano posti di lavoro e credo che, da messicano che peraltro ha negoziato parte di quel grande trattato, sapesse di che cosa parlasse. Abbiamo una domanda di fondo, per cui è bene non nasconderci dietro formule, come « la NATO del commercio estero », che personalmente mi preoccupano.

Tutto questo ci porta a capire qual è, in questo momento, il nostro interesse nazionale, visto che stiamo lavorando per un bene comune, pur sapendo di lavorare con quello che passa il convento. Noi non siamo mediatori per inerzia né per vocazione, ma per dura necessità. L'*agrobusiness* è uno dei nostri *business*, ma non è l'unico.

Abbiamo delle posizioni finanziarie. UniCredit ha ancora un valore nelle prime 50 entità a grande controllo azionario che sono tutte finanziarie, tranne la petroliera cinese. Mi riferisco a dati del 2007-2008 che non sono stati aggiornati, purtroppo. Dobbiamo chiederci seriamente come negoziare nei dettagli. Lo dico perché quello che sta uscendo dal TTIP è un'esautorazione piuttosto spinta dello Stato, ma mi chiedo se è a favore di una regolazione più morbida, flessibile ed efficace del privato.

Arriviamo di nuovo alle catene di prodotti e al consumatore. È chiaro che un consumatore avvertito è un consumatore che ha più capacità di scelta, il che è importante. Tuttavia, quando noi sappiamo da decenni che una serie di *software* hanno degli accessi privilegiati chiamati « porte di servizio, *backdoor* », ci troviamo in una situazione piuttosto diseguale perché se voglio iPhone, mi becco l'iPhone com'è, per cui, anche se Apple si rifiuta di fornire chiavi di accesso allo Stato, iPhone è capace di guardare dentro al mio telefono quando vuole. Questo è un dato di fatto, non è che l'iPhone si autoesclude dal sistema operativo che crea.

Questo accade anche per necessità di manutenzione. Quante volte vi siete trovati col *computer* bloccato e vi siete affidati alla manutenzione remota? Quando uno è in remoto, potenzialmente può aprire le viscere e vedere tutto quello che vuole.

Siamo in questa situazione e la Cina a suo tempo ha fatto una scelta, che non so quanto sia stata realmente implementata, di usare Linux, perché essendo un *open*

software è veramente aperto. Sono sicuro che i programmatori cinesi avranno fatto i loro piccoli intrugli per fare qualcosa di più adattato alla realtà del partito, ma questo è un altro paio di maniche. Comunque, un *software* aperto è un *software* che appunto non permette questo tipo di *backdoor*, a meno che non vengano aggiunte. Non prendo nessuna percentuale da Linux, su questo potete stare tranquilli, anche se ci sono versioni commerciali.

Vengo alla domanda su che cos'è la dimensione digitale della geopolitica, quindi su cosa deve fare la politica. Posso dirvi che una dimensione digitale della geopolitica è una dimensione che ha la consapevolezza di quello che ho cercato di dire in questa presentazione. È chiaro che questa presentazione è solo un primo passo, nel senso che poi una rappresentazione pienamente integrata e coerente di questa concezione va sviluppata. Ci vuole capacità non solo di pensiero e di esperienza, ma anche di rappresentazione grafica che ci permetta di cogliere con categorie vecchie quello che è un mondo molto nuovo.

Sicuramente i nostri giovani che smanettano di più hanno un'idea più dettagliata di questa nuova dimensione digitale della geopolitica, ma anche molto pratica; forse non riescono a vedere tutto il mondo, ma vedono pezzi di operatività.

È chiaro che parte di questa dimensione digitale è data dalla dimensione comunicativa, ma bisogna imparare a vedere l'insieme degli strumenti e non soltanto dei pezzi. Nella comunicazione, ormai tutti sappiamo che *Twitter* è importante, ammesso che lo sia, e che poi c'è l'antivirus, eccetera. Adesso, bisogna essere capaci di dare una visione sintetica. Per carità, ci devono essere tanti saperi specialistici, ma la possibilità di una sintesi c'è.

Qui, la domanda è: l'universo digitale è un universo di ridistribuzione delle risorse e delle ricchezze, sì o no? Così come è stato concepito finora o meglio così come è stato impiegato finora, non lo è. C'è uno *sharing* di informazioni che è senza precedenti e senz'altro liberatorio. In effetti, ci sono intere professioni, inclusa la mia, che senza internet non esisterebbero e, come un bravo monaco medievale, sarei legato alle biblioteche di pochi istituti. Questo è un fatto.

C'è una possibilità di comunicazione, di diffusione e anche, in una certa misura, di disintermediazione senza precedenti perché non devo più andare alla cattedrale di Worms per postare il fatto che il prodotto dei *futures* delle indulgenze è *non-compliant* con la dottrina cattolica, ma lo faccio su internet e raggiungo molto più gente. Questo è assolutamente vero.

Parallelo a questo processo di liberazione dell'informazione, c'è stato un processo di concentrazione del controllo delle piattaforme che è stato spietato. In effetti, se andate a vedere quante sono le piattaforme di *social media*, vedrete che sono molto poche: siamo duecento Paesi e le piattaforme saranno dieci o quindici.

I grandi Paesi si fanno le loro piattaforme, come per esempio l'Iran e il Brasile. Questo accade perché, nonostante *Facebook* sia un esperanto o comunque una lingua franca che si è adattata alle varie lingue, mi faccio la mia. Lo faccio perché si tratta una concentrazione di informazioni che vengono assorbite e utilizzate; poche storie: è un finto patto conveniente del diavolo perché tu scrivi quello che vuoi, ma mi dai tutto quello che hai scritto, il che è insomma interessante come equità di scambio.

La misura più concreta della concentrazione non è soltanto negli oligopoli, ma è a livello di ricchezza mondiale. Siamo arrivati al fatto che l'1 per cento è più ricco del 99 per cento. Mi spiace, questa è l'evoluzione degli ultimi trent'anni. Come diceva Warren Buffett, abbiamo fatto la guerra di classe e l'abbiamo vinta. Meglio così? A me pare di no.

Ecco perché Trump ha successo. Trump non è meglio di Catilina: vuole utilizzare le classi svantaggiate dalla globalizzazione negli Stati Uniti per dire: « ragazzi, siete stati spogliati, ma io vi rappresenterò ». *He has a point*. Brutto, sporco, non ci piace, però questa è la conseguenza della concentrazione di ric-

chezza. È possibile invertire questa cosa ? Sì, però questo richiede una serie di politiche coerenti per un primo quinquennio, in attesa che diventi un ventennio. Certo, si può fare.

Noi siamo sulla cuspide esattamente come i sovietici dopo i primi trent'anni del loro sistema: lascia o raddoppia ? Io sono contrario al raddoppio, come avrete capito, perché le conseguenze si toccano. Questo richiede un'inversione che significa una ridefinizione dei rapporti economici e quindi anche sociali e politici nel loro insieme. Tuttavia, senza una decisione politica, questo non si può fare. In questo momento, il fenomeno di cattura dello Stato non è soltanto un fenomeno nei Paesi dell'Est, per niente !

Abbiamo questa grande sfida che, però, è assolutamente affrontabile, si può fare. Questa è forse la mia parola di asciutta speranza, con cui io posso rispondere alla sua impegnativa ma sostanziale domanda.

PRESIDENTE. Ringraziamo il professor Politi per queste sue considerazioni.

Dichiaro conclusa l'audizione.

La seduta termina alle 12.45.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI ESTENSORE DEL PROCESSO VERBALE

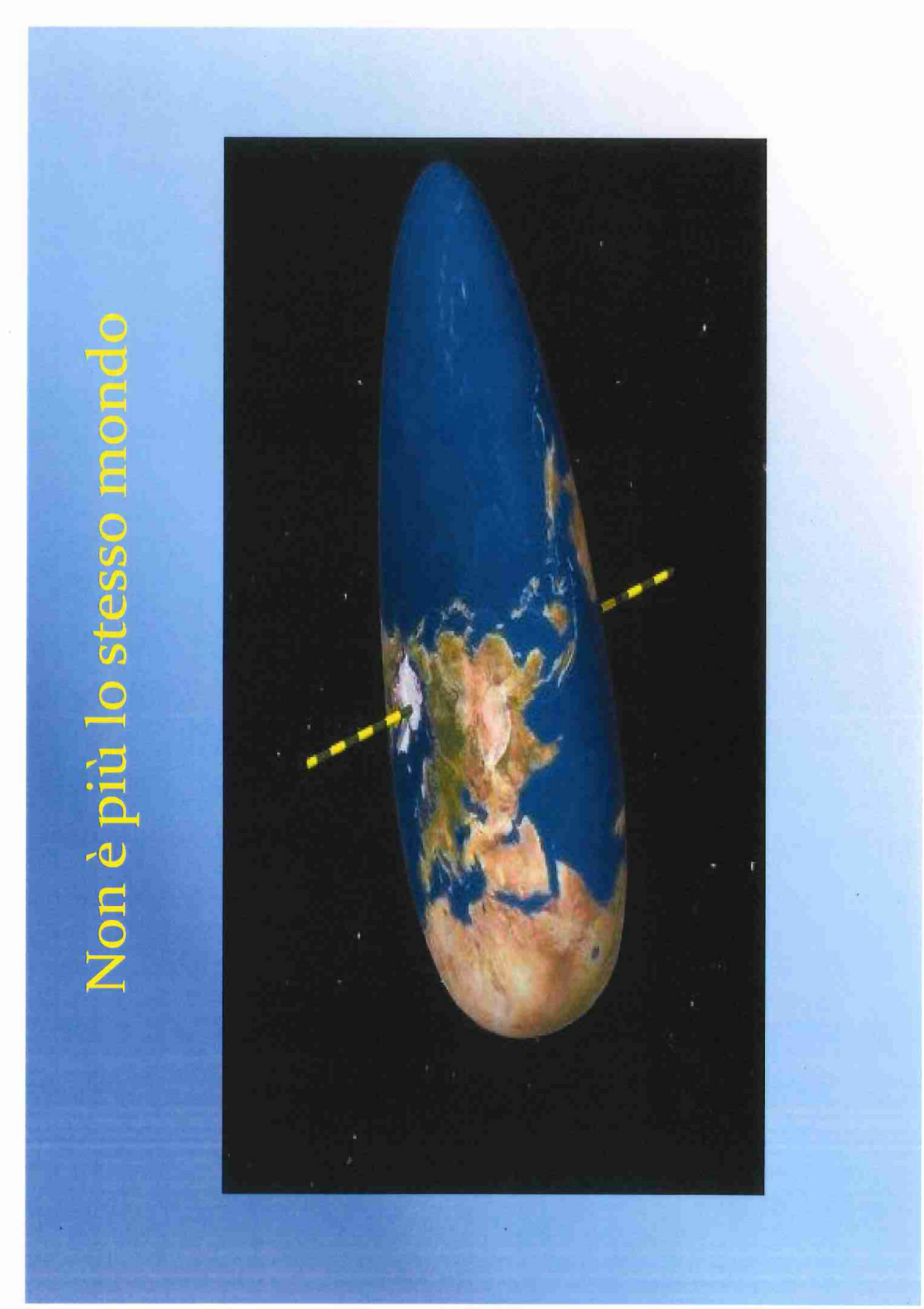
DOTT. RENZO DICKMANN

Licenziato per la stampa il 29 aprile 2016.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

ALLEGATO

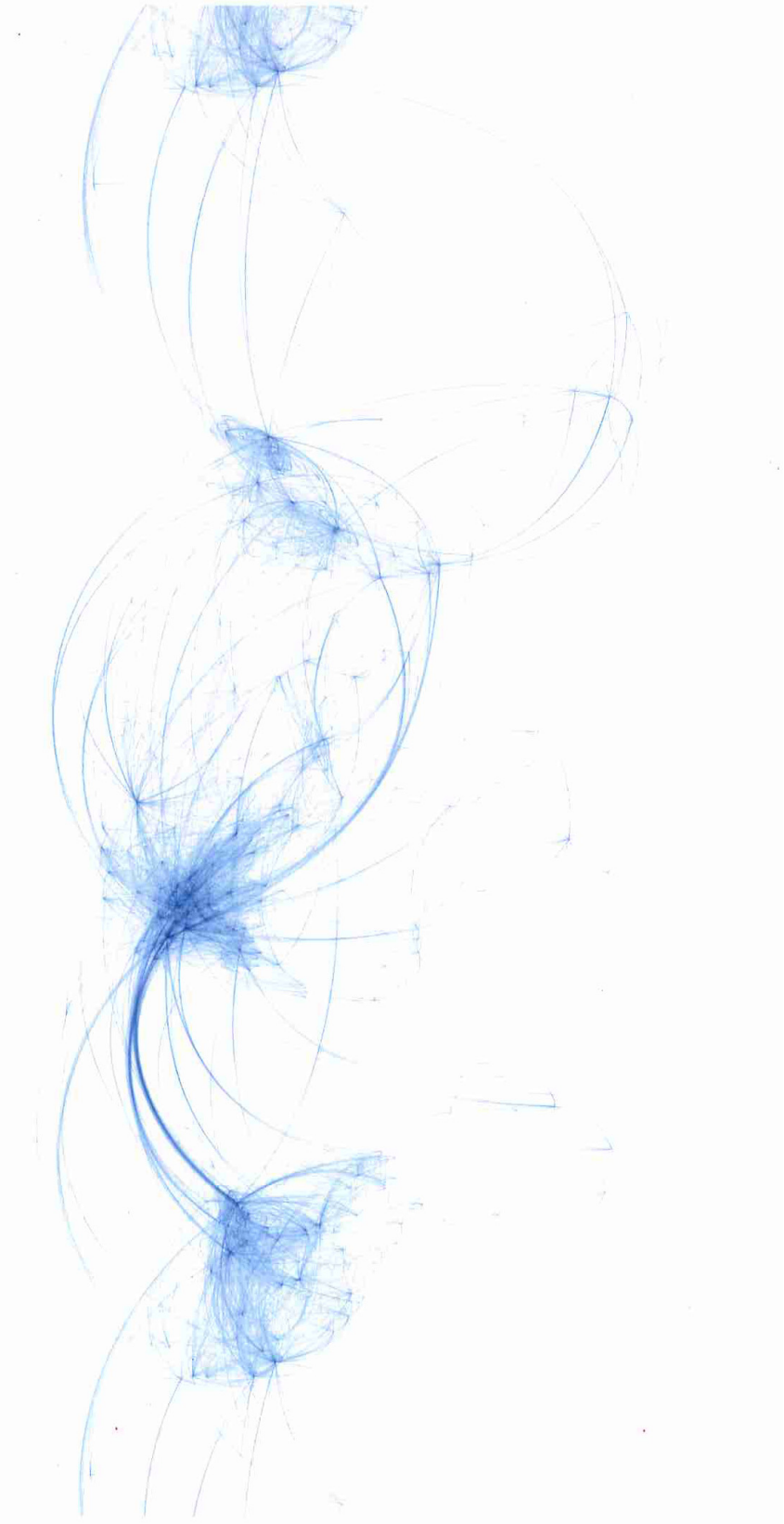
NATO DEFENSE COLLEGE
FOUNDATION
Geo- e cybernetworks
La liquefazione della geopolitica
Audizione Comm Difesa
Camera Deputati
NDCF Director
Roma, 08/03/2016
NATO Foundation
Defense College

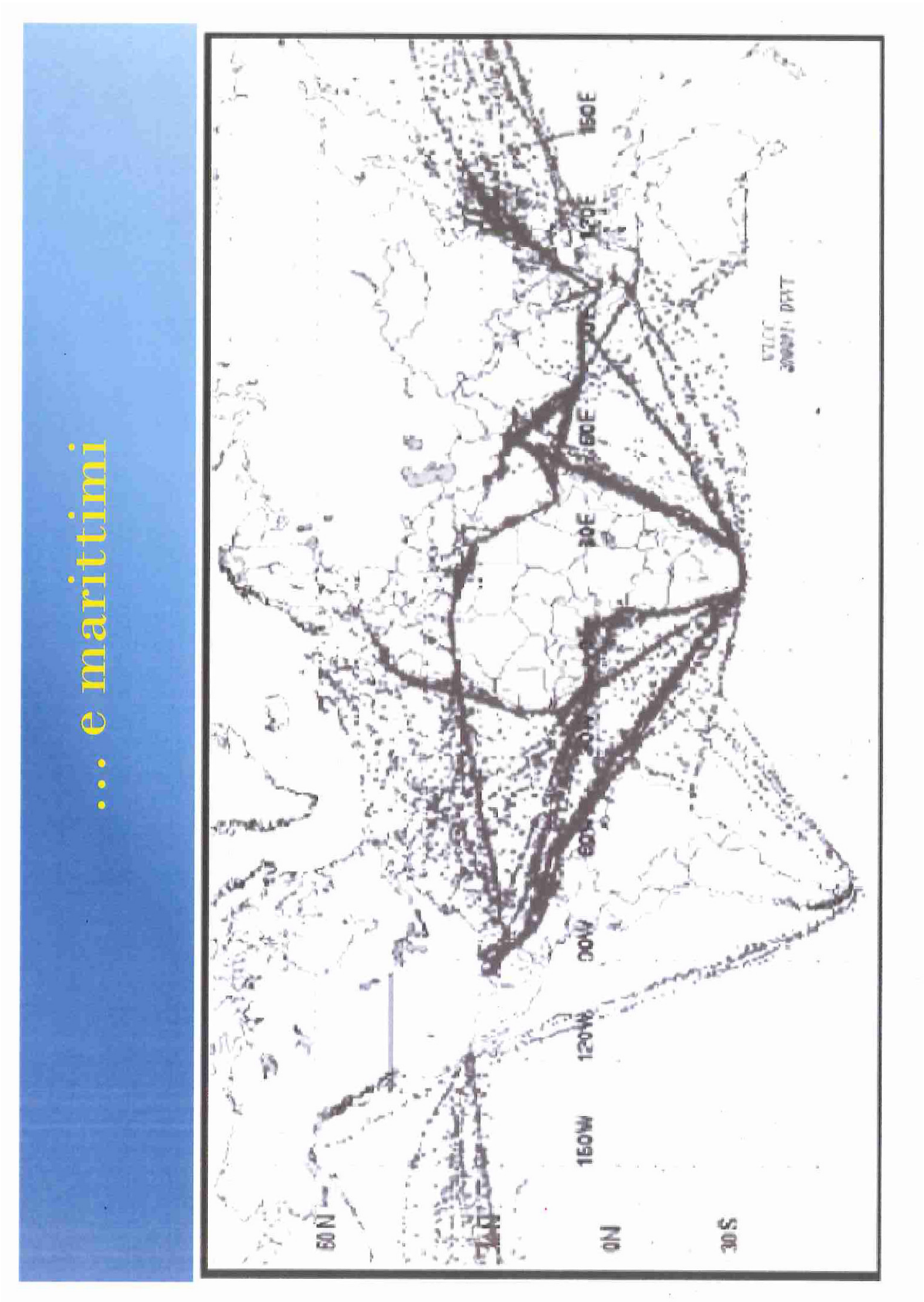

Non è più lo stesso mondo

Frontiere vere e finte

- Tutte quelle linee che vedete sono più o meno immaginarie
- In un mondo liquido perché la frontiera dovrebbe essere una barriera?
- Se lo stato è intelligente, la usa piuttosto come una spugna, capace di scambiare attivamente con l'esterno e di filtrare intelligentemente (avviene molto di rado)

La realtà dei traffici legali aerei




... e marittimi
180E
120E
60E
30E
60W
90W
120W
150W
60 N
0N
30S

Qualcuno vede frontiere?

- Teoricamente esistono nei porti ed aeroporti
- Ma la storia di ogni contrabbando dimostra quanto siano permeabili o violabili
- Vediamo allora quali sono i fattori che cambiano il traffico di stupefacenti partendo dal legale per arrivare all'illegale

Mondo e poteri

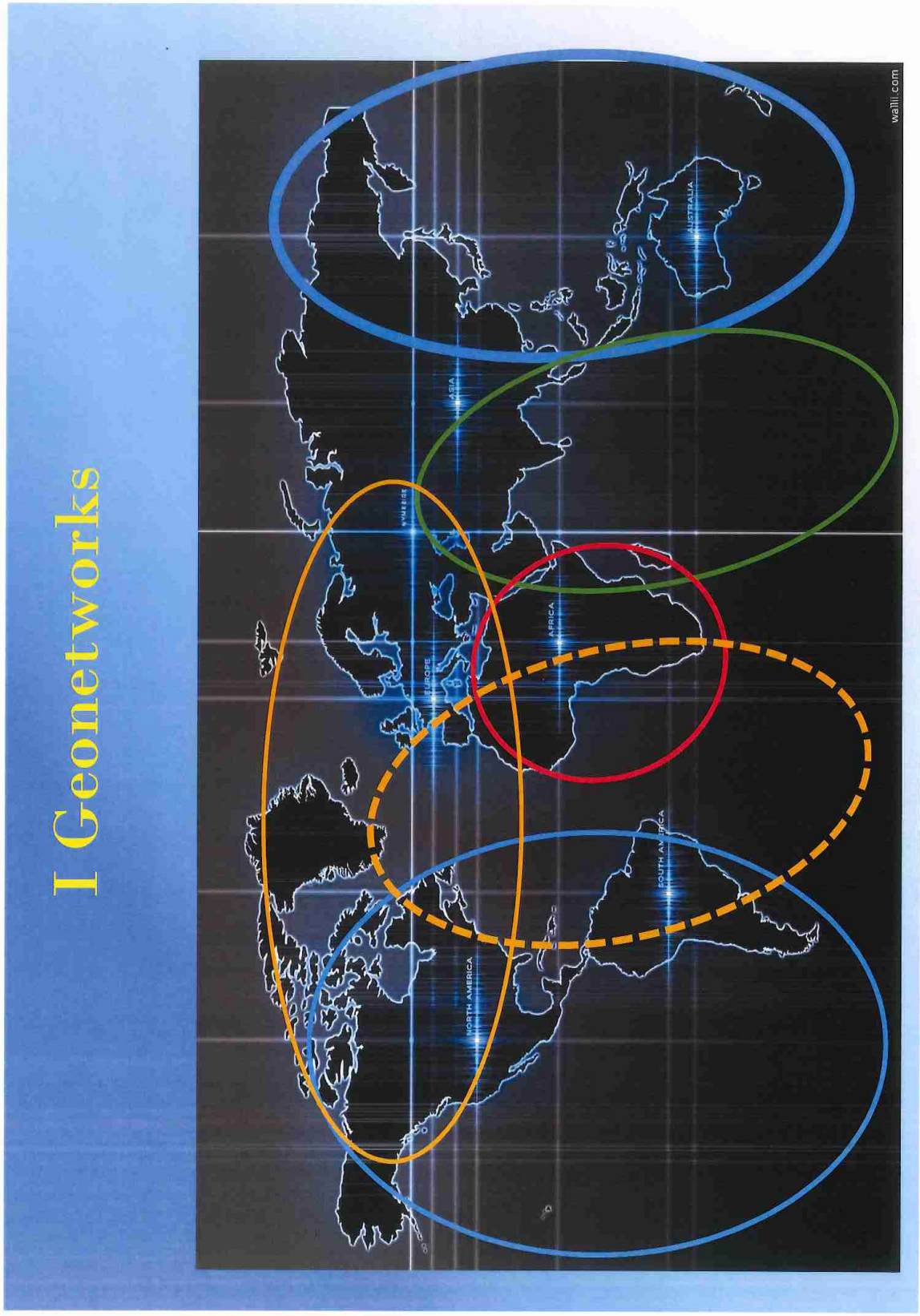
- **Lo stato è in sfarinamento o svuotamento finanziario** (tenaglia finanza ombra, banche ombra, finanza islamica, crisi finanziaria ed economica globale)
- **I poteri emergenti o forti non sono statali**: mafie, galassie finanziarie, oligopoli economici, ***mutazioni del ciberspazio***
- **Le concorrenti visioni geoeconomiche** hanno facce statali e fili non statali

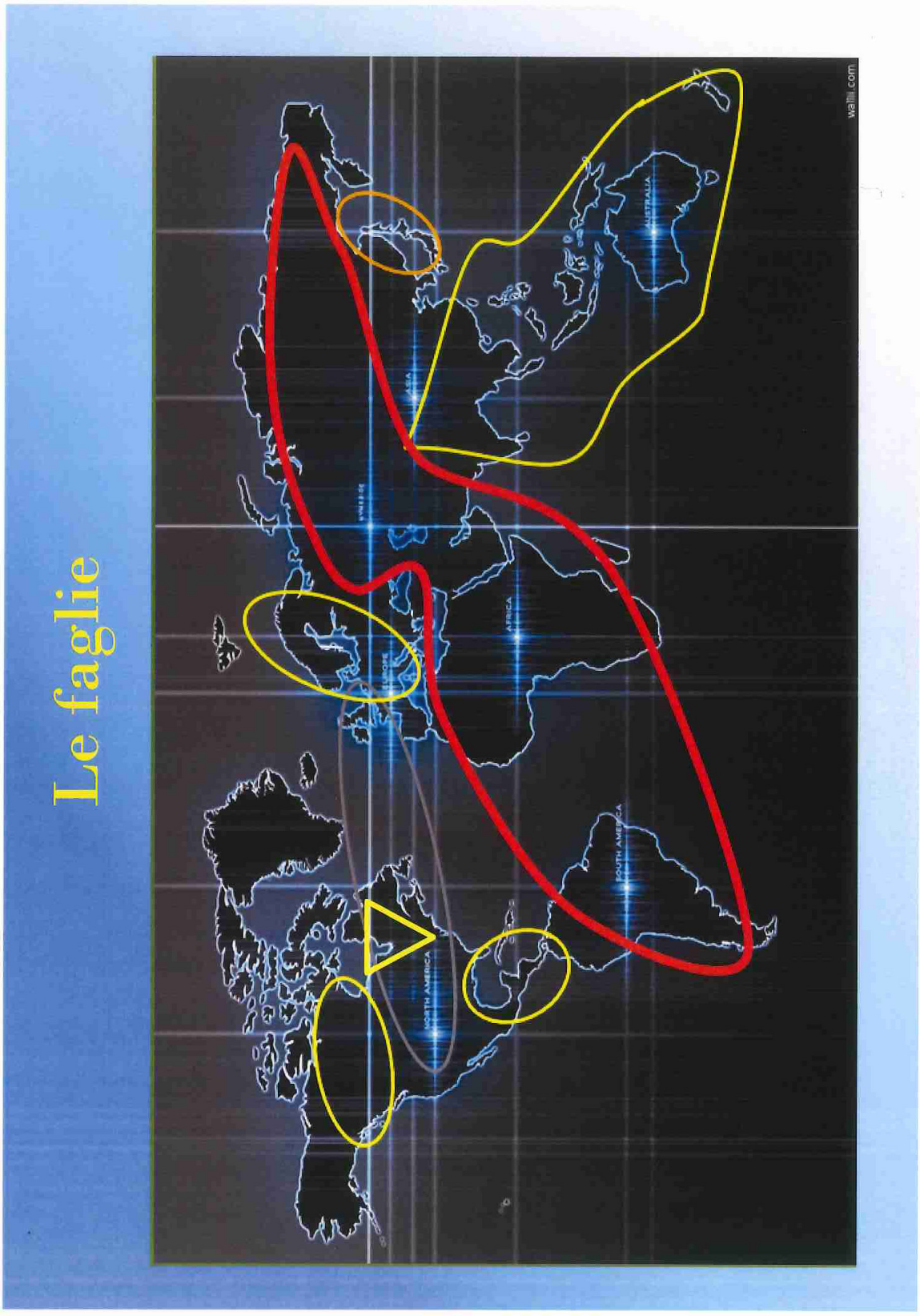
Equilibri e poteri

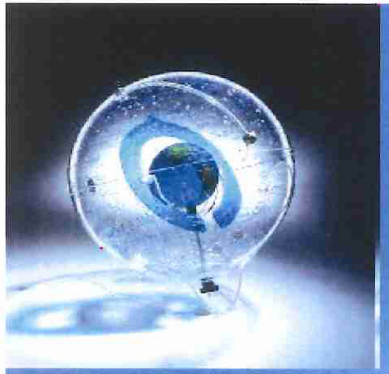
- Mondo bipolare
- Unipolarismo consociativo
- Unipolarismo coercitivo
- Multipolarismo disarchico
- Multipolarismo disfunzionale

- Guerra Fredda
- G.H. Bush – Clinton
- G.W. Bush
- Bush – Obama 04-09
- Obama

- Dal dominio dello stato allo scolorimento
- Dagli assi agli equilibri liquidi
- Scolorimento statale progressivo da Clinton ad Obama
- Dai blocchi ai network
- Dalla competizione tra blocchi alla copetizione ingarbugliata


I Geonetworks
AUSTRALIA
ASIA
EUROPE
AFRICA
NORTH AMERICA
SOUTH AMERICA
walili.com


Le faglie
AUSTRALIA
ASIA
EUROPE
AFRICA
NORTH AMERICA
SOUTH AMERICA
walltti.com



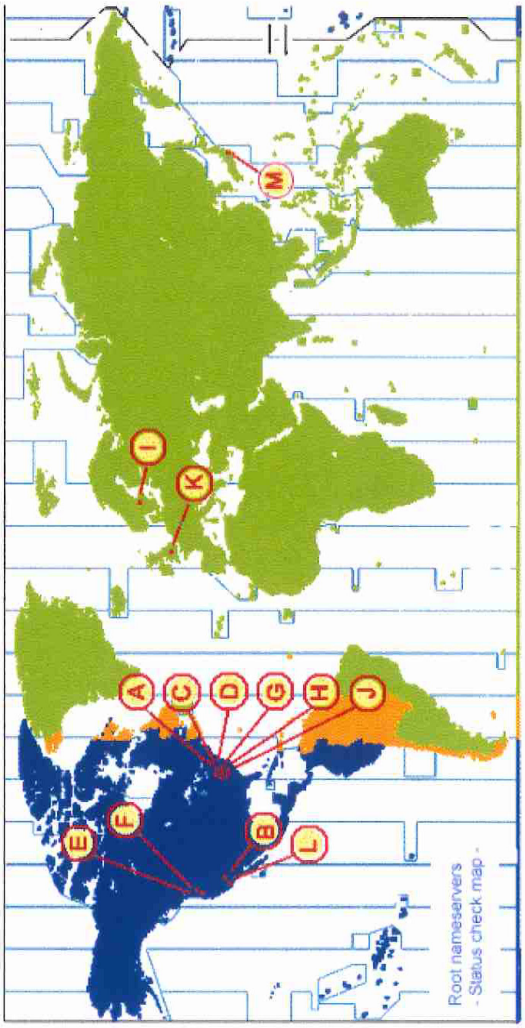
THE 7 SHAPING FLOWS

- Knowledge
- Invested/financial capital
- Conventional-non conventional-digital energy
- Real/virtual migrations
- Food/Agrotech
- Drinking water
- Eco-system (e.g. the level of sea, climate change)

- Eco-system (e.g. the level of sea, climate change)
- Drinking water
- Food/Agrotech
- Real/virtual migrations
- Conventional-non conventional-digital energy
- Invested/financial capital
- Knowledge

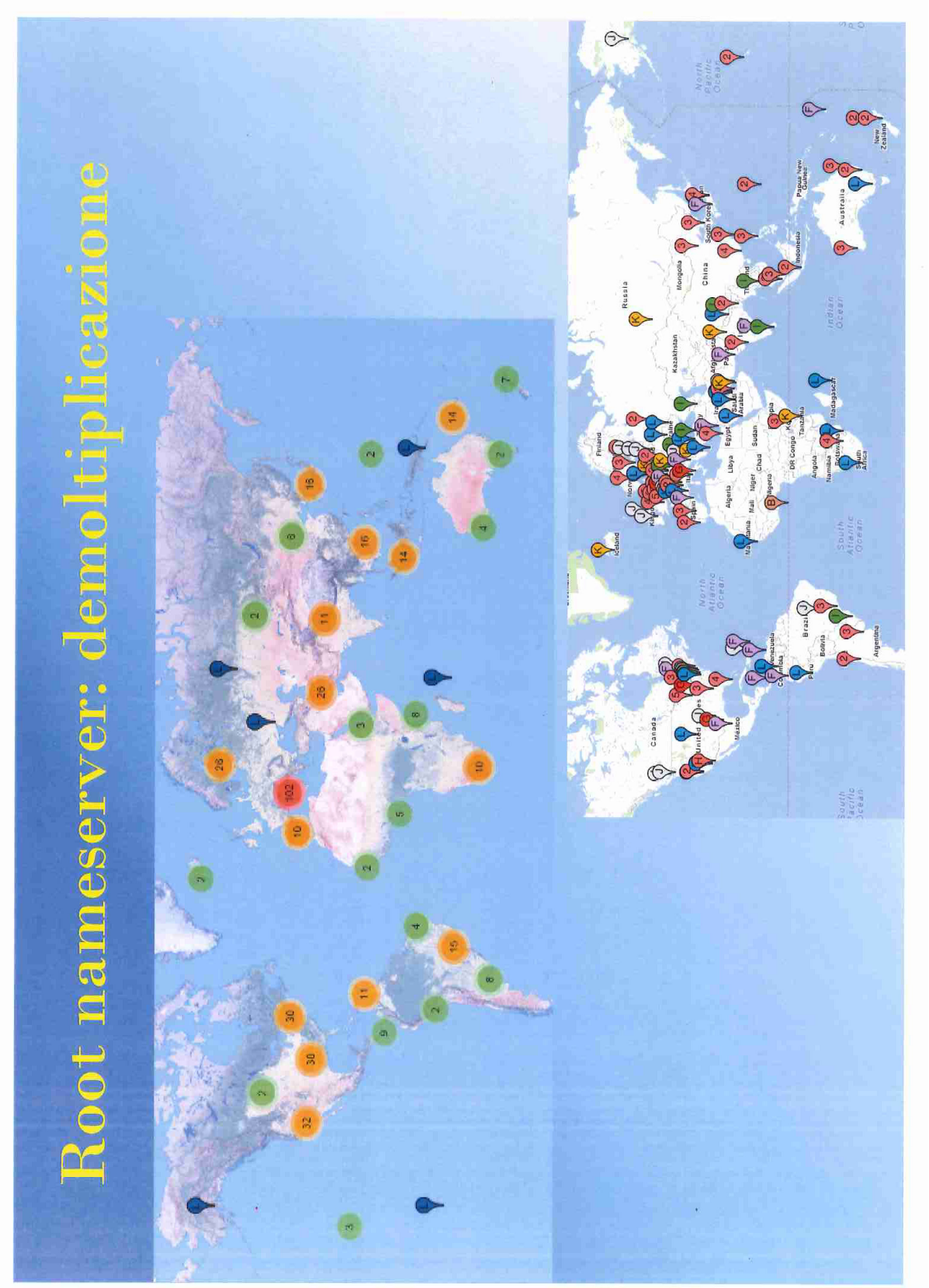
Root nameserver: residenza iniziale

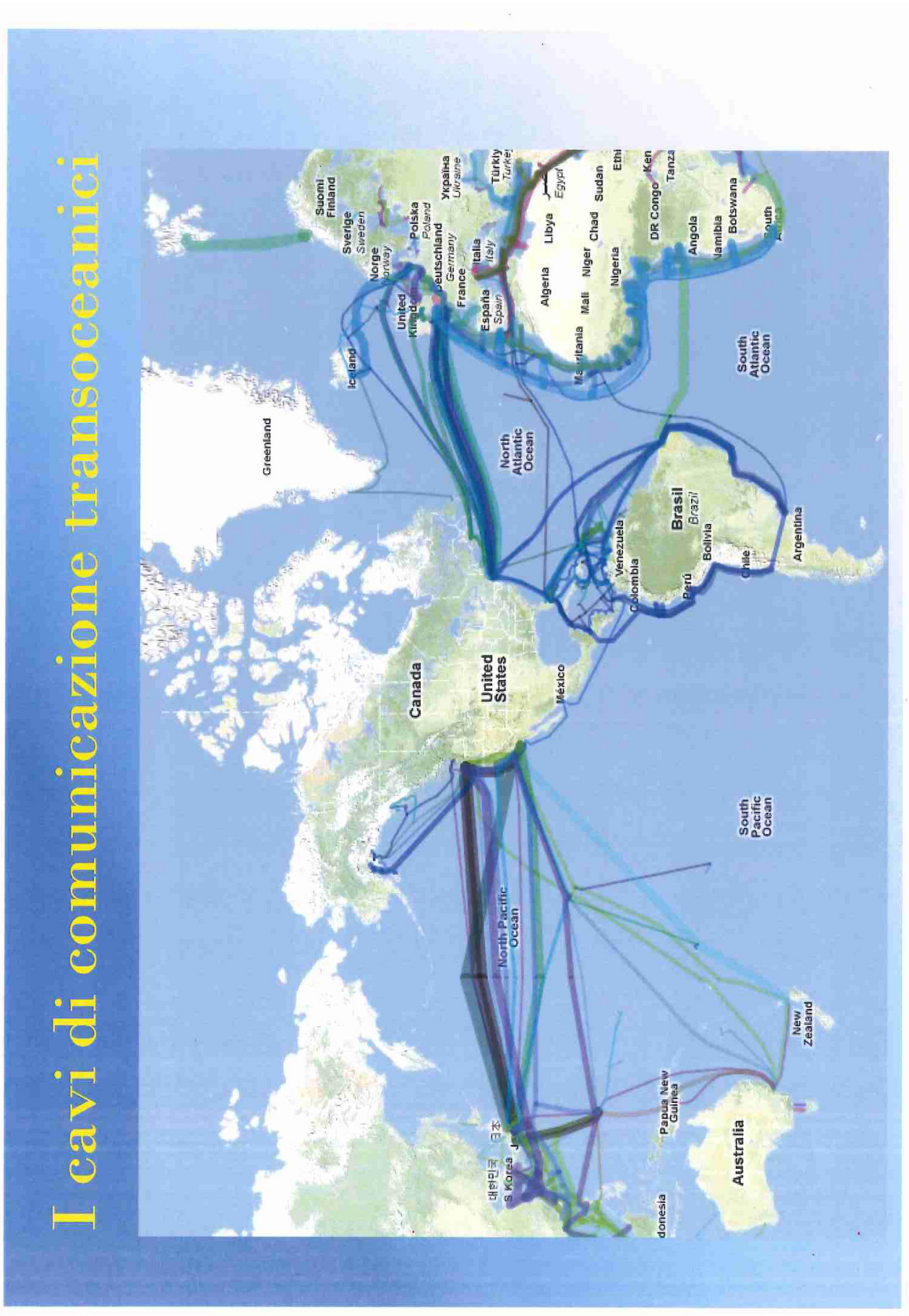
Map of the Root Servers



Root nameserver: demoltiplicazione

Lettera	Vecchio nome	Indirizzo IPv4	Operatore	Luogo geografico
A	ns.internic.net	198.41.0.4	VeriSign	Dulles, Virginia, USA
B	ns1.isi.edu	192.228.79.201	USC Information Sciences Institute	Marina del Rey, California, USA
C	c.psi.net	192.33.4.12	Cogent	distribuito in *anycast*
D	terp.umd.edu	199.7.91.13	University of Maryland	College Park, Maryland, USA
E	ns.nasa.gov	192.203.230.10	NASA	Mountain View, California, USA
F	ns.isc.org	192.5.5.241	ISC	distribuito in *anycast*
G	ns.nic.ddn.mil	192.112.36.4	NIC del DoD USA	Vienna, Virginia, USA
H	aos.arl.army.mil	128.63.2.53	U.S. Army Research Lab	Poligono di Aberdeen, Maryland, USA
I	nic.nordu.net	192.36.148.17	Autonomica	distribuito in *anycast*
J	–	192.58.128.30	VeriSign	distribuito in *anycast*
K	–	193.0.14.129	RIPE NCC	distribuito in *anycast*
L	–	198.32.64.12	ICANN	Los Angeles, California, USA
M	–	202.12.27.33	Progetto WIDE	distribuito in *anycast*


Root nameserver: demoltiplicazione


I cavi di comunicazione transoceanici
Greenland
Iceland
Suomi Finland
Sverige Sweden
Norge Norway
United Kingdom
Polska Poland
Deutschland Germany
France
Україна Ukraine
Italia Italy
España Spain
Türkiye Turkey
Egypt
Libya
Algeria
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Ethi
DR Congo
Ken
Tanza
Angola
Namibia
Botswana
South Africa
South Atlantic Ocean
North Atlantic Ocean
Canada
United States
México
Brasil Brazil
Venezuela
Colombia
Perú
Bolivia
Chile
Argentina
South Pacific Ocean
North Pacific Ocean
대한민국 S. Korea
日本
Papua New Guinea
Australia
New Zealand

Dimensione cyber-statale

A BRIEF HISTORY OF CYBER WEAPONS

1982 r. **Siberian pipeline explosion**

Blast rumored to have been caused by a logic bomb in the pipeline's automated control software.

1997 r. **Operation Eligible Receiver**

First full-scale cyber-warfare exercises conducted by US intelligence services that saw attacks on the servers of several other US government bodies.

1998–2000 rr. **Operation Moonlight Maze**

Computers systems at the Pentagon, NASA, US Department of Energy, private universities and research labs were subjected to attacks for nearly two years.

2003–2005 rr. **Operation Titan Rain**

Coordinated attacks on computers at NASA, Lockheed Martin, Sandia National Laboratories, and Redstone Arsenal.

2006 r. **Israel uses cyber weapons during conflict with Hezbollah**

Countries that have officially acknowledged the existence of special agencies responsible for cyber security and for carrying out cyber attacks:

2007 r. **A series of hacker attacks on governmental and military institutions in the US, Germany, India**

April:
DDoS attack on Estonia

The NATO Cooperative Cyber Defence Centre of Excellence is set up in response to the attack.

September:
Operation Orchard

Israeli airstrike on a nuclear facility in Syria. A military computer program is used prior to the bombing in order to neutralize Syrian radar defenses.

2008 r. **Massive cyber attacks compromise Georgian governmental and public Internet resources**

during the eight-day conflict in South Ossetia.

2010 r. **Operation Myrtus**

The Stuxnet worm was detected in Iran. The worm targeted programmable logic controllers operating high-frequency convertor drives installed in uranium enrichment facilities in Natanz, Iran.

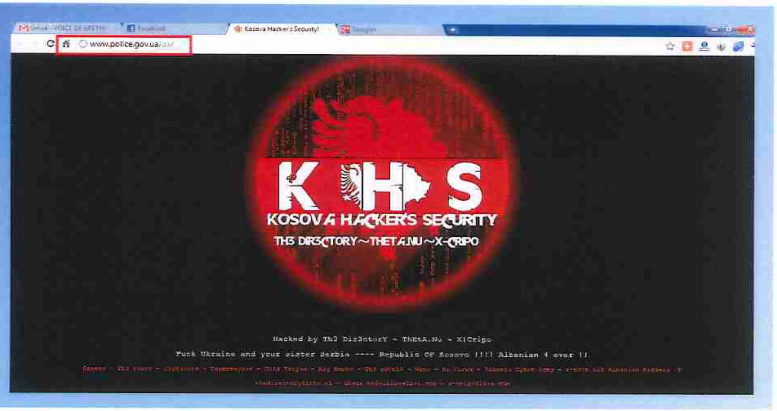
© 1997 – 2011 Kaspersky Lab ZAO

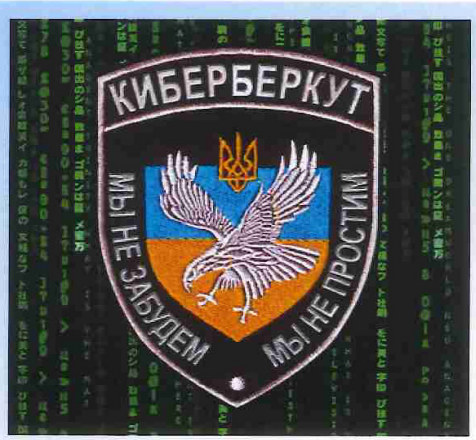
Dimensione cyber-statale II

	NATO	2012	Upgrading the cyber defence capabilities and enable the NATO Computer Incident Response Capability (NCIRC) to achieve full operational capability by the end of 2012.	58M €
		2013 - 2017	With a cyber budget of $1.54 billion from 2013 to 2017, DARPA will focus increasingly on cyber-offence to meet military needs	1.54B $
	UK	2012	Extra Investment to develop deterrents to hostile viruses and hackers	650M £
	Israel	From 2012	Expense of more than $13 million in the coming years to develop new technologies for cyber defence.	13M $
	China		Estimating actual PLA military expenditures is difficult because of poor accounting transparency and China's still incomplete transition from a command economy. Using 2011 prices and exchange rates, DoD estimates China's total military-related spending for 2011 ranges between $120 billion and $180 billion. China's cyber security market will expand remarkably in the coming years, from a valuation of $1.8 billion in 2011 to $50 billion by 2020, representing a dramatic compound annual growth rate (CAGR) increase of 44.7%	?
	Iran	2012	On December Tehran announced an ambitious plan to improve its cyber-warfare capabilities developing new technologies and creating new team of cyber experts.	1B $

Ucraina

- 3/2/12 attacco generale a siti in Ucraina: Presidenza Consiglio Ministri, Servizio di Sicurezza, Banca Nazionale, Amministrazione Tasse, Comitato Antimonopolio, sito del partito di governo



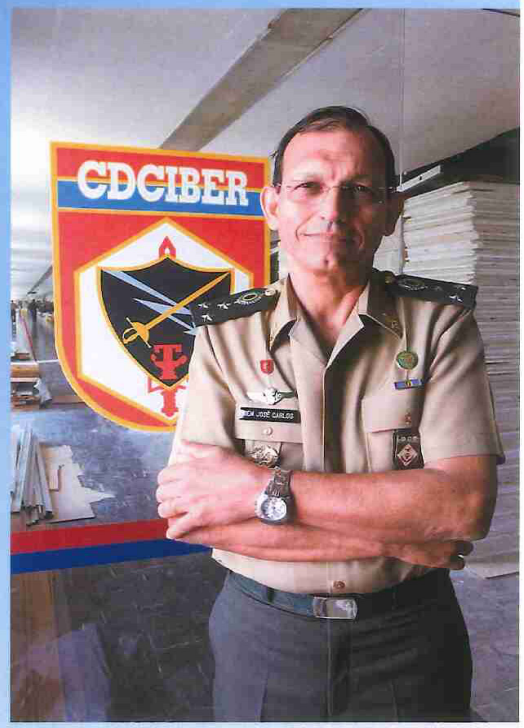


Ucraina: II

- 2014 idem
- RO nazione guida per supporto difesa cyber
- Manca ancora un comando difensivo identificabile
- Russia ancora molto (auto)limitata, ma non gruppi privati o «spontanei»

Altri governi II

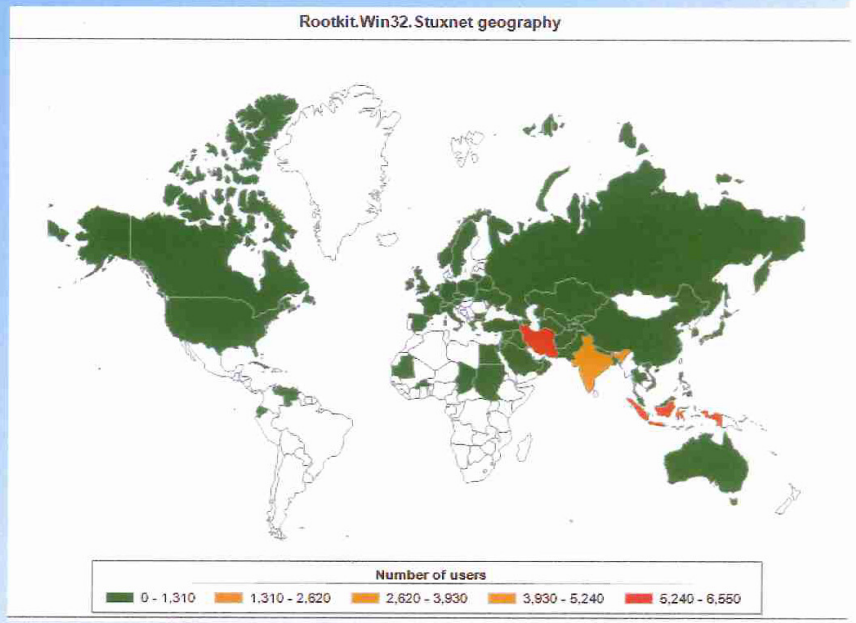
- 1° attacco a BR (IBGE, BM Rio Grande, Petrobras e siti grandi istituzioni)
- "Segurança Cibernética no Brasil" (Presidência da República 2010)
- CDCiber (Centro de Defesa Cibernética)



Altri governi III

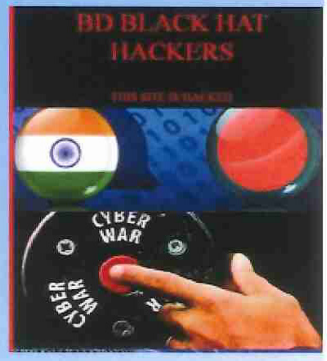
- Iran Stuxnet (2010) e Viper
- Duqu e Privateer
- Unità crisi informatica,

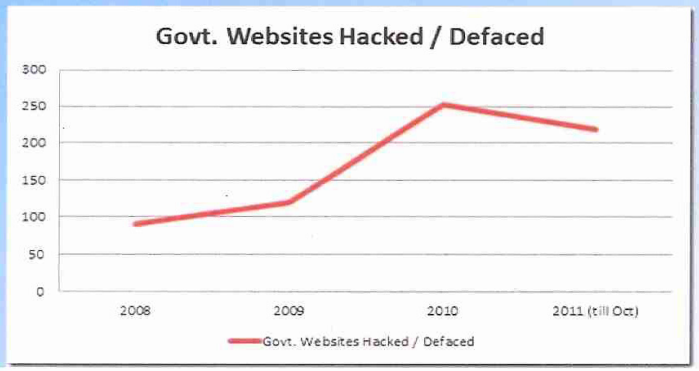
poi Cyber Defence Command

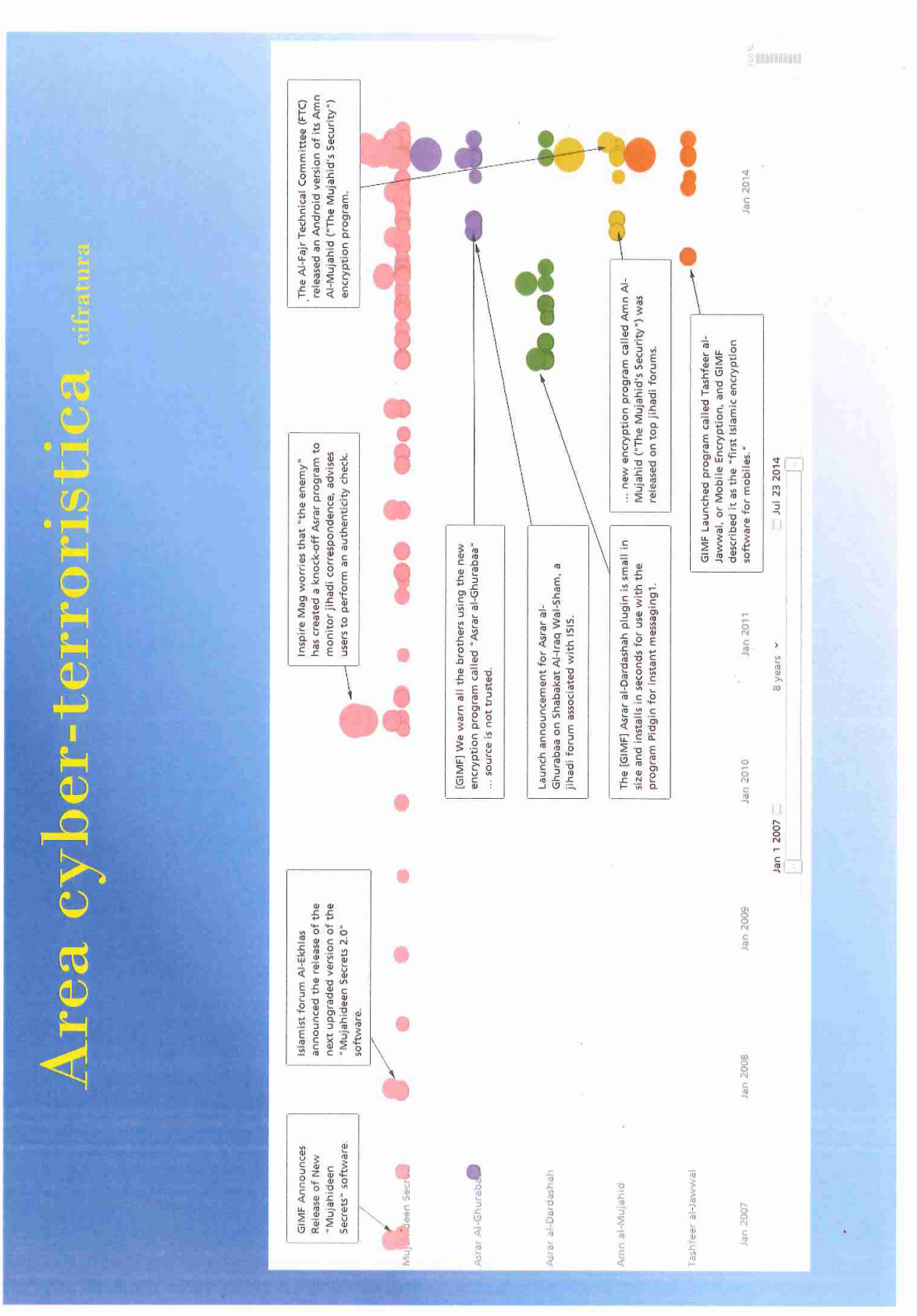


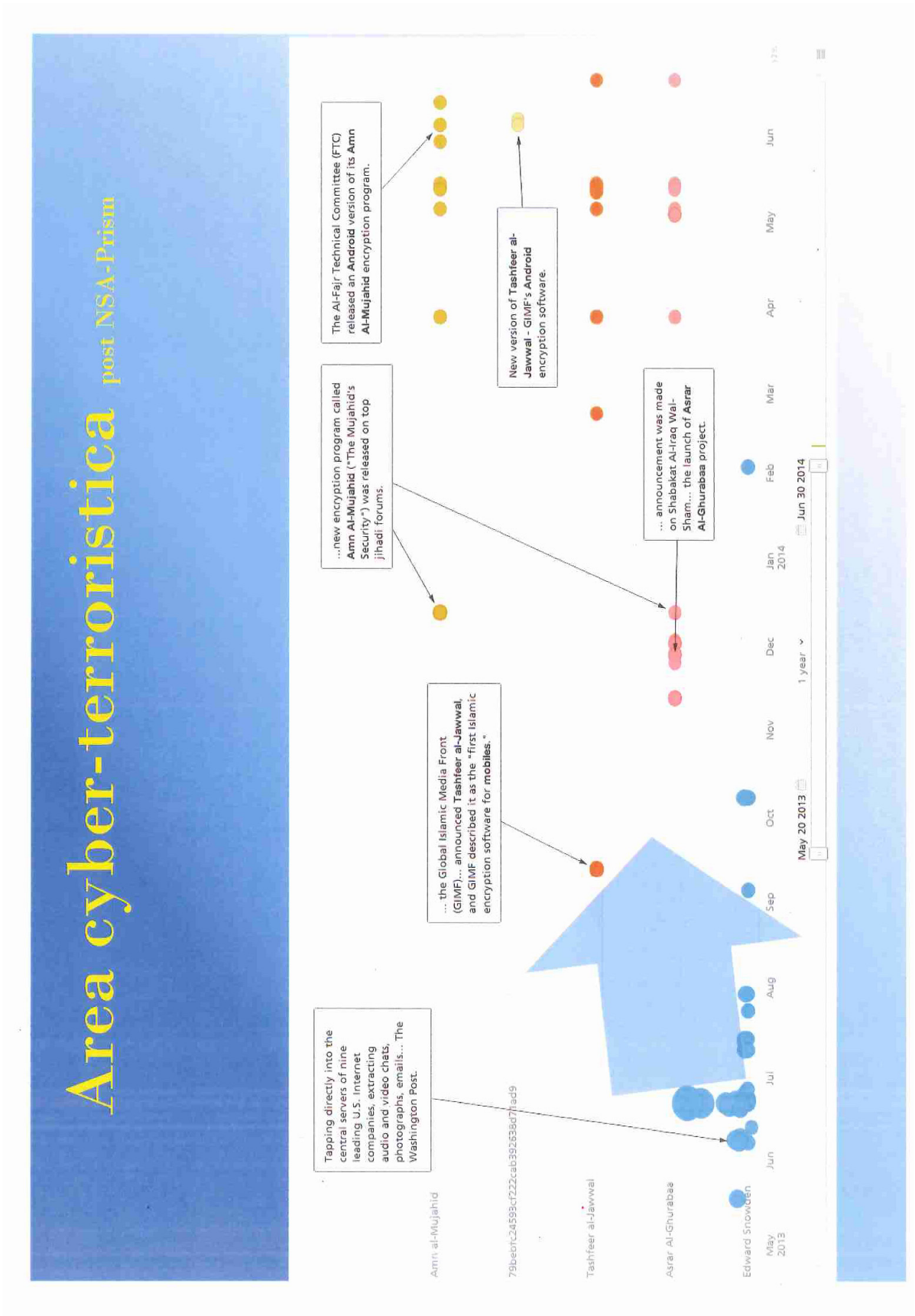
Altri governi IV

- India DRDO
- IDSA TF report 2012
- 5 paese per frequenza attacchi cibernetici
- India-Bangladesh cyberconflict






Area cyber-terroristica
cifratura
GIMF Announces Release of New "Mujahideen Secrets" software.
Islamist forum Al-Ekhlas announced the release of the next upgraded version of the "Mujahideen Secrets 2.0" software.
Inspire Mag worries that "the enemy" has created a knock-off Asrar program to monitor jihadi correspondence, advises users to perform an authenticity check.
The Al-Fajr Technical Committee (FTC) released an Android version of its Amn Al-Mujahid ("The Mujahid's Security") encryption program.
[GIMF] We warn all the brothers using the new encryption program called "Asrar al-Ghurabaa" ... source is not trusted.
Launch announcement for Asrar al-Ghurabaa on Shabakat Al-Iraq Wal-Sham, a jihadi forum associated with ISIS.
The [GIMF] Asrar al-Dardashah plugin is small in size and installs in seconds for use with the program Pidgin for instant messaging1.
... new encryption program called Amn Al-Mujahid ("The Mujahid's Security") was released on top jihadi forums.
GIMF Launched program called Tashfeer al-Jawwal, or Mobile Encryption, and GIMF described it as the "first Islamic encryption software for mobiles."
Mujahideen Secrets
Asrar Al-Ghurabaa
Asrar al-Dardashah
Amn al-Mujahid
Tashfeer al-Jawwal
Jan 2007
Jan 2008
Jan 2009
Jan 2010
Jan 2011
Jan 2014
Jan 1 2007
8 years
Jul 23 2014

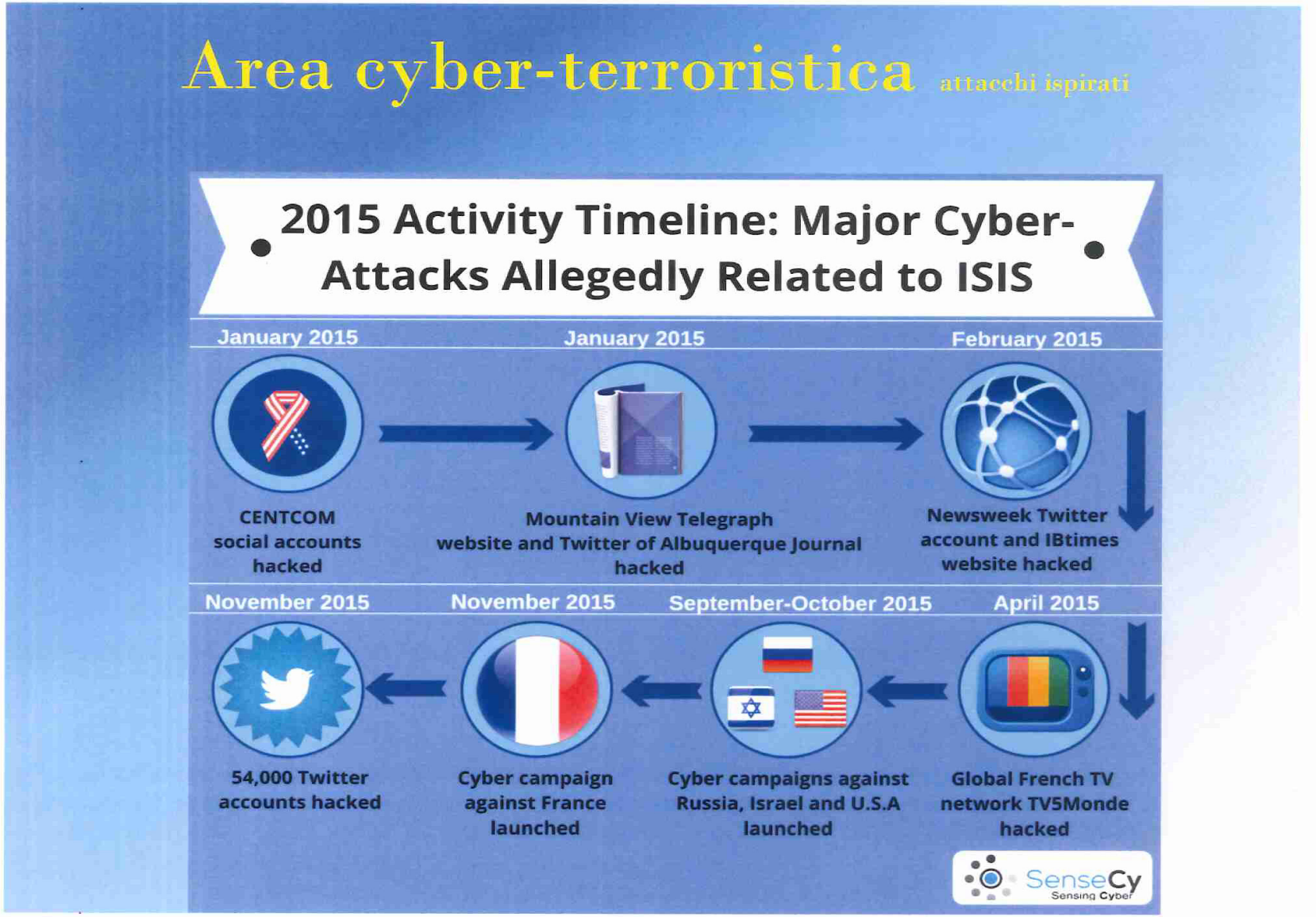

Area cyber-terroristica post NSA-Prism
Tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, emails... The Washington Post.
... the Global Islamic Media Front (GIMF)... announced Tashfeer al-Jawwal, and GIMF described it as the "first Islamic encryption software for mobiles."
...new encryption program called Amn Al-Mujahid ("The Mujahid's Security") was released on top jihadi forums.
The Al-Fajr Technical Committee (FTC) released an Android version of its Amn Al-Mujahid encryption program.
New version of Tashfeer al-Jawwal - GIMF's Android encryption software.
... announcement was made on Shabakat Al-Iraq Wal-Sham... the launch of Asrar Al-Ghurabaa project.
Edward Snowden
Amn al-Mujahid
79beorc24593cf222cab392638d7bad9
Tashfeer al-Jawwal
Asrar Al-Ghurabaa
May 2013
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan 2014
Feb
Mar
Apr
May
Jun
May 20 2013
Jun 30 2014
1 year

Area cyber-terroristica

metodi cifratura

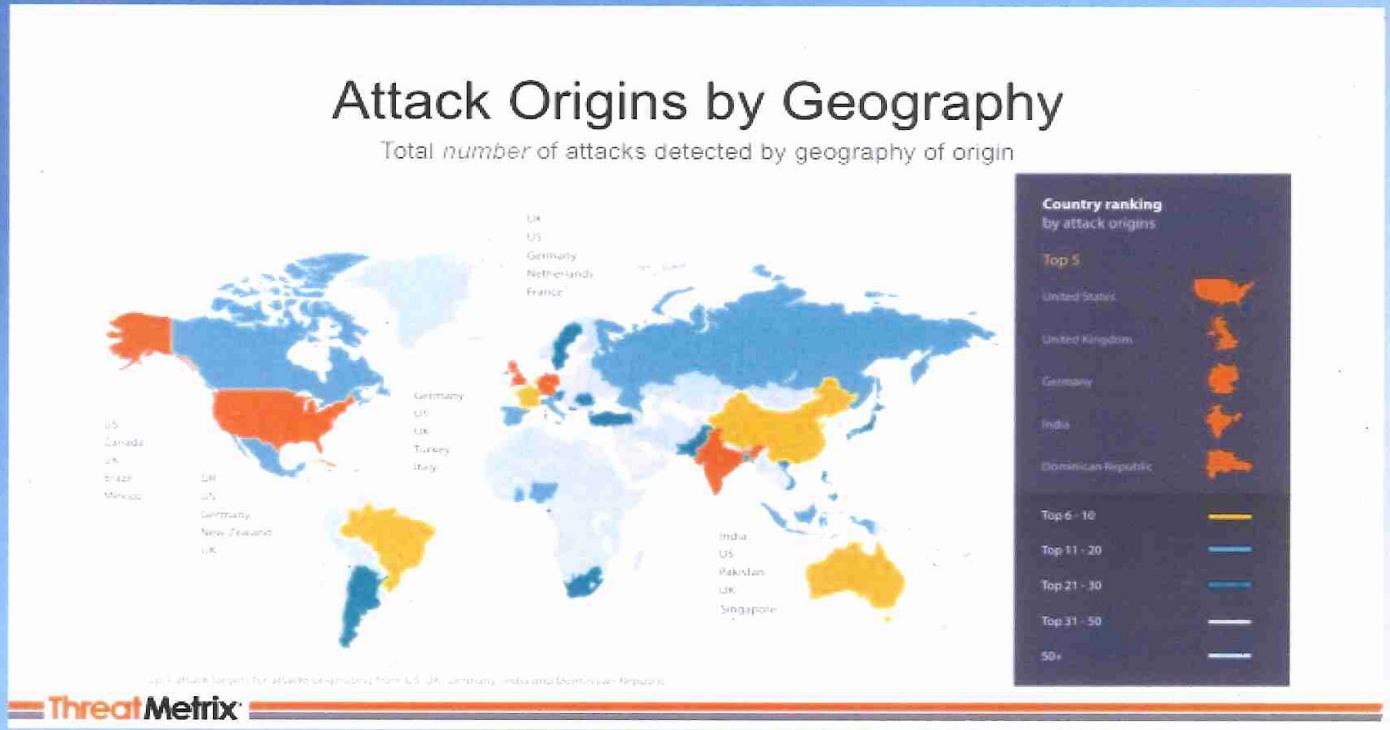
Product	Release Date	Organization	Key Feature	Execution Platform	Messaging Platform	Crypto Method	Delivery
Mujahideen Secrets (Asrar al-Mujahideen)	2007	GIMF (AQ main)	Encryption of messages or file exchange	Windows with recent instructions for Mac porting	Primarily email	Public/Private key, RSA based, 2048 bit	Windows app
Asrar al-Dardashah	February 6, 2013	GIMF (AQ main)	Encryption of instant message traffic	Pidgin platform, Windows installer	Messaging (Pidgin): Yahoo, Google, AOL, etc.	Based on Mujahideen Secrets encryption	Pidgin plugin
Tashfeer al-Jawwal (Mobile Encryption Program)	September 4, 2013	GIMF (AQ main)	Encryption of SMS traffic	Android/Symbian	SMS	Twofish, use SSL for transport	Android/Symbian apps
Asrar al-Ghurabaa	November 27, 2013	ISIS (AQ adversary)	Pure text encryption	Website, accessible via Tor	Platform independent, just encrypts	"A special or unique encryption algorithm"	Website
Amn al-Mujahid	December 10, 2013	Al-Fajr Technical Committee (FTC)	Text encryption	Windows OS	Email, SMS, instant messaging	AES/Twofish	Windows app
Amn al-Mujahid (Mobile)	June 7, 2014	Al-Fajr Technical Committee (FTC)	Text encryption	Android	SMS	AES/Twofish	Android app

Area cyber-terroristica attacchi ispirati

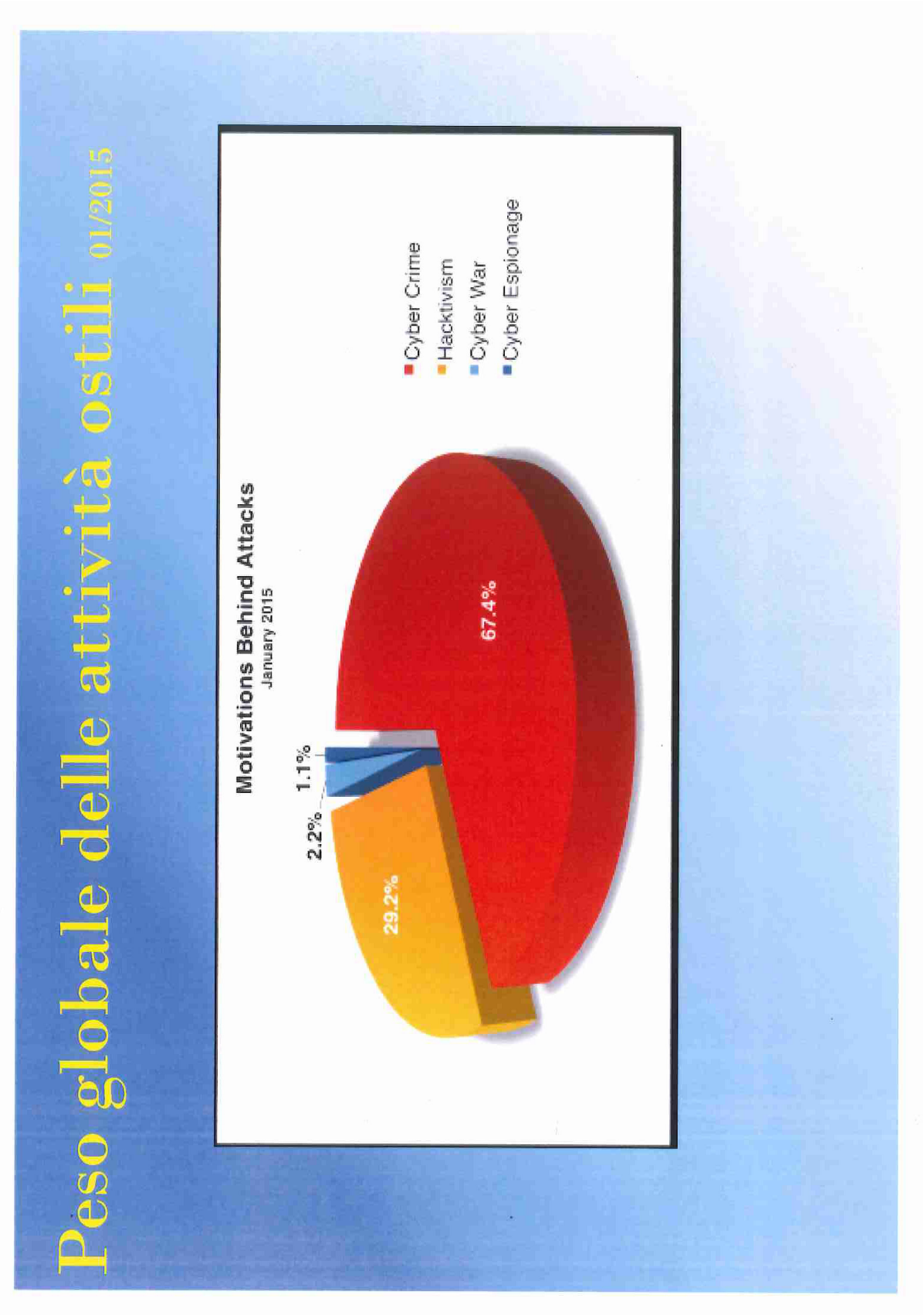


Cybercrime
Cybercrime: Top 20 Countries
1. United States of America 23%
2. China 9%
All Other Countries 19%
3. Germany 6%
4. Britain 5%
5. Brazil 4%
6. Spain 4%
7. Italy 3%
8. France 3%
9. Turkey 3%
10. Poland 3%
11. India 3%
12. Russia 2%
13. Canada 2%
14. South Korea 2%
15. Taiwan 2%
16. Japan 2%
17. Mexico 2%
18. Argentina 1%
19. Australia 1%
20. Israel 1%
EU makes 24% together!

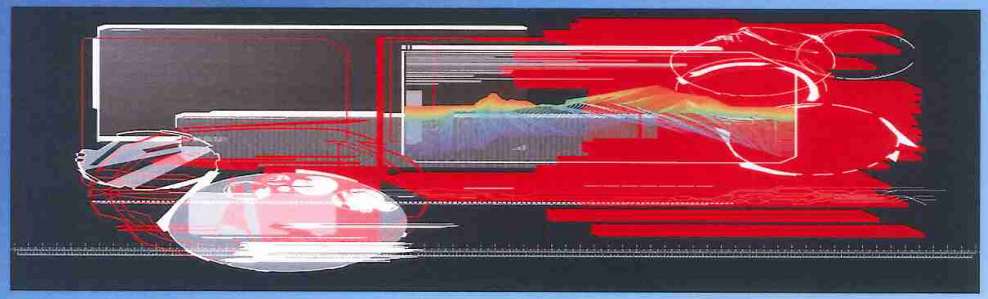
Cybercrime II



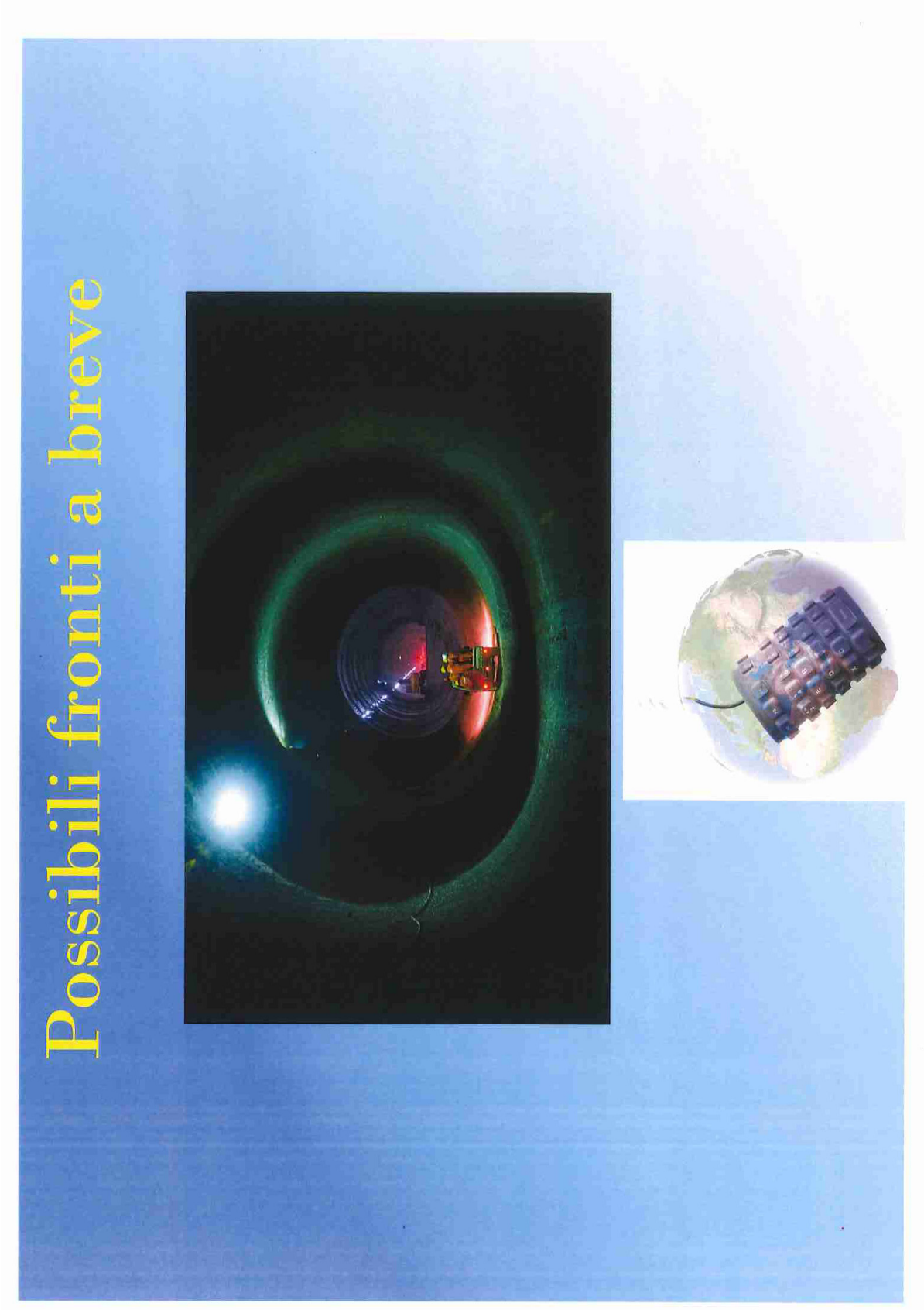
Mid-2015 Top cybercrime sources are "friends": USA, UK, GE
Followed by usual and unusual suspects: BR, FR, PRC, AU
Russia is in the third league

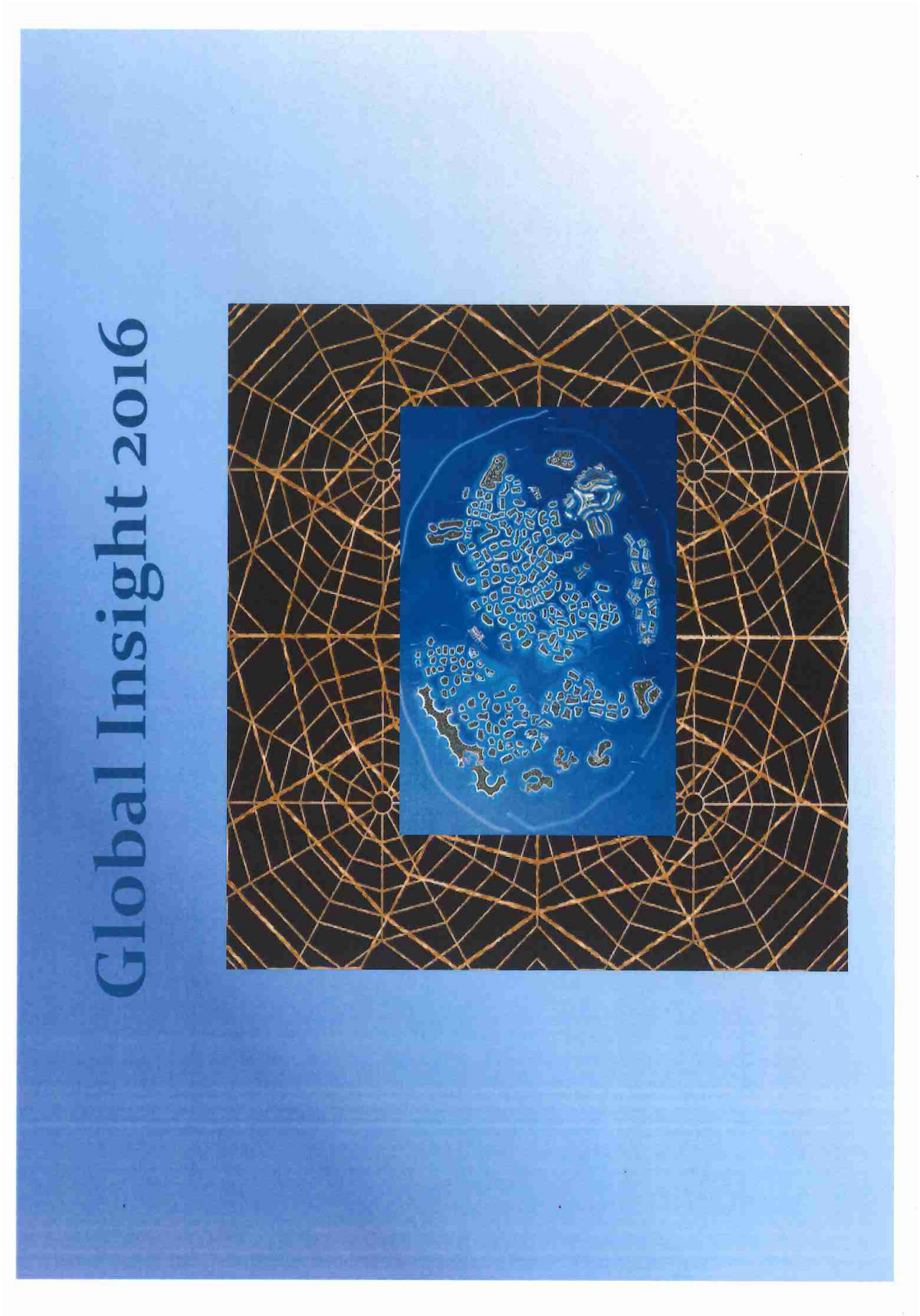

Peso globale delle attività ostili 01/2015
Motivations Behind Attacks
January 2015
Cyber Crime
Hacktivism
Cyber War
Cyber Espionage
67.4%
29.2%
2.2%
1.1%

Situazione techno-cyber a breve



- Corsa contro il tempo fra diffusione legale/illegale di tecnologie ed il mantenimento del vantaggio tecnologico "dell' Occidente"
- I paesi euroatlantici e quelli pro-USA nel Pacifico Occidentale sono ancora forti, ma la crisi taglia le spese R/S
- Emergenti: Brasile, Cina, India, Israele, Messico, Turchia, Sud Africa
- La cibersicurezza è un aspetto di questa corsa: non a caso tutti i BRIC e l'Iran si sono dotati di comandi cibernetici
- Tuttavia la «guerra» informatica è meno seria del crimine informatico


Possibili fronti a breve

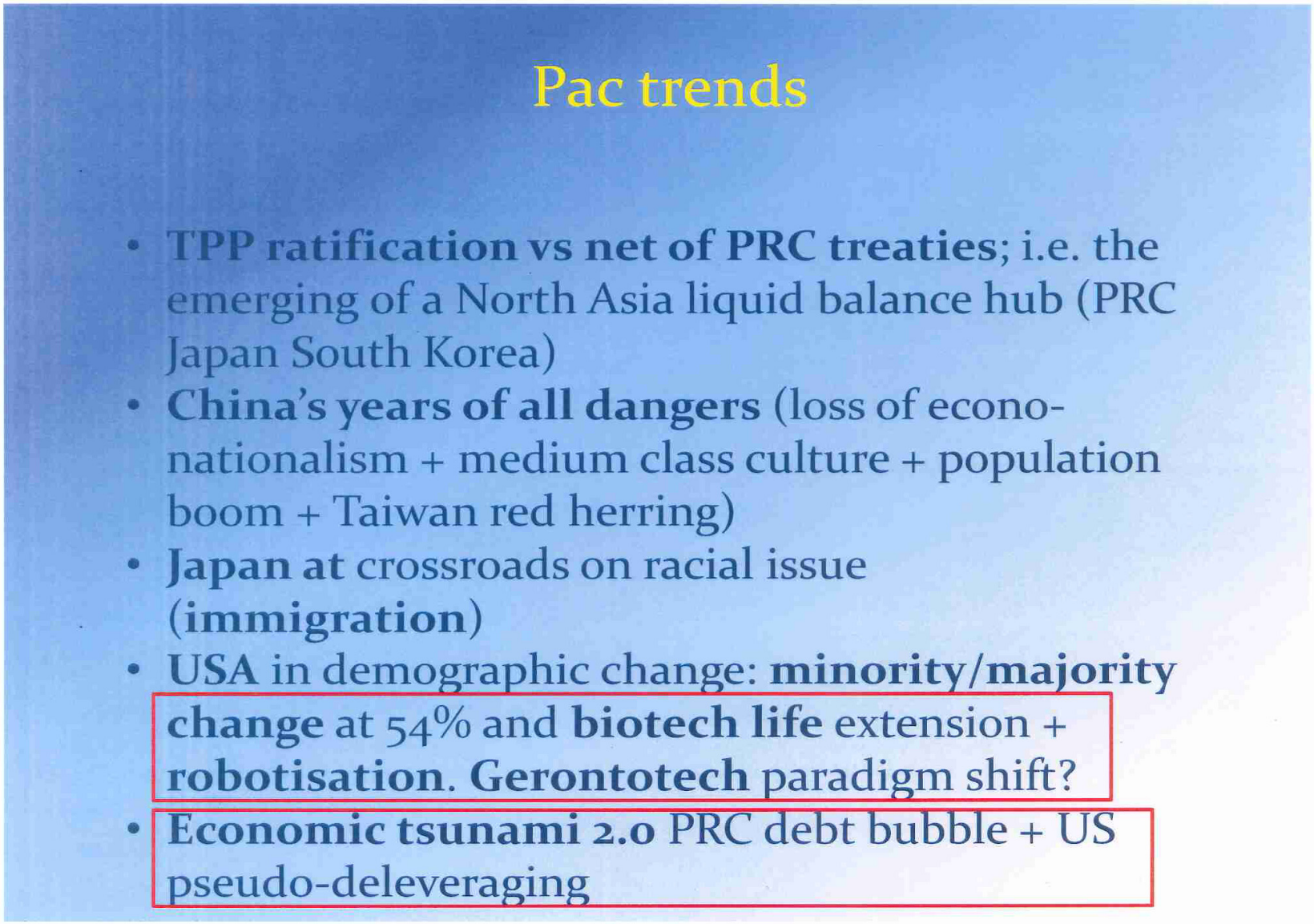

Global Insight 2016

Relevant Major Issues 2016

- From criminal convergence to criminal parasiting: TOC hosts, terrorism is guest = Coca – Heroin convergence over EU and finally **global drug conveyor belt**
- Dangerous weakening of **Pac-Twin Towers** (PRC and USA);
- Failure of the **second war against Iran** and consequences for the petro-monarchies in a low energy price environment
- Failure of economic stimuli and **increased socio-political instability from San Francisco to Vladivostok** (Euraslantic area)
- **Burden on global economy of a locked Africa**

Serious GloPac trends

- The **race to the treaty** US (TPP TTIP TISA)
- TPP ratification vs net of PRC treaties
- World Bank signals the end of advantages of competitive devaluation = **race to the bottom**
- 1% of the world richer than 99% = **race to the most (+ debt backlog)**
- Risks of the Pivot to East with Silk Swing to West = **race around**


Pac trends
• TPP ratification vs net of PRC treaties; i.e. the emerging of a North Asia liquid balance hub (PRC Japan South Korea)
• China's years of all dangers (loss of econo-nationalism + medium class culture + population boom + Taiwan red herring)
• Japan at crossroads on racial issue (immigration)
• USA in demographic change: minority/majority change at 54% and biotech life extension + robotisation. Gerontotech paradigm shift?
• Economic tsunami 2.0 PRC debt bubble + US pseudo-deleveraging

Indo trends
• HDD crisis (Hydrological Desalination and Desertification) for SYRAQ, Jordan, Gulf, Yemen
• India – Pakistan competition destabilising SCO SAARC and Gulf. From TAPI to TII
• Shift Iran Turkey Egypt Pakistan towards Silk Road (i.e. PRC and Russia): from Sunni-Shi'ite competition to ME dislocation to East
• The Islamic trio Islamabad-Riyadh-GCC: Islamic banking and terrorist financing
• Dawla goes East: splintering of AQ and Taleban

Afro trends

- The great South and East Africa famine and drought = **food + oil instability**
- **A leaderless Africa** (South Africa increasing fragility, Nigeria paralised by low intensity civil war, Egypt on the brink of failure)
- **More strategic value of the continent**: Djibouti (FR, USA, JP and PRC bases); AFRICOM Spice Route operation
- **Increasing investment value** +38% RoE
- **Race for investments and free trade** (Tripartite Free Trade Area (TFTA) with COMESA EAC SADC)
- **Long term conflict areas** (Sahel+Lake Tchad system Nile strip, wider HoA, Great Lakes-DRC system)

Atlan-trends
• South Atlantic weak integration BR-RSA
• Brexit and TTIP risk of political cohesion (fault line between industry/commerce vs finance)
• Germany – USA competition on industry (Industrie 4.0 vs Industrial Internet Project) and cyber defences
• Declining Russia and Ukraine and the pull of SCO/Silk Road
• Israelo-Egyptian crisis (Gaza inhabitable, IL end of two state solution, Egypt low resources Canal)
• Death and fragmentation of Middle East

1995 – 2015 – 2035: *Next 20 Years*

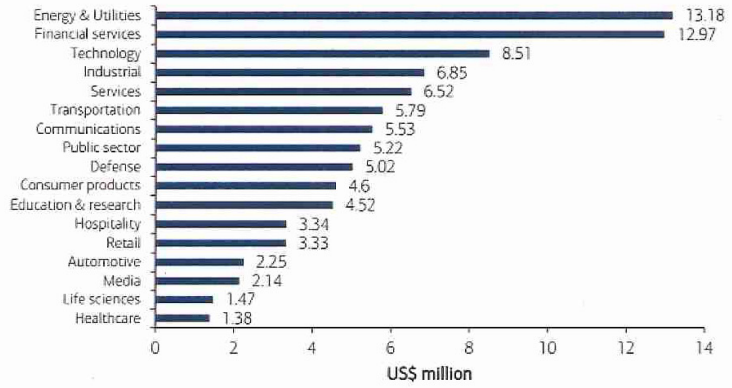
- ***IoT:*** Global Connected "Internet of Things" – All On-Line Intelligent Devices across most sectors & geographies.
- ***"The Bad Cyber Guys" :*** Professionally Trained Cyber Criminals and Cyber Terrorists operating WorldWide!
- ***Augmented Reality:*** Emergence of 4D Immersive Virtual Augmented Reality *(a la Matrix Movies)*
- ***Universally Embedded Security:*** Need for Cybersecurity in ALL intelligent devices, servers, data & network nodes
- ***On-Line CyberPolice:*** CyberBot Avatars patrolling as Virtual CyberPolice Force across "Internet of Things"

NATO Foundation
Defence College

Conclusioni

- Il geocyber liquida le vecchie categorie geopolitiche. Esistono dimensioni fisiche e statali, ma sono molto permeabili a reti bianche, nere e grigie (concetto di Netchwork)
- I fronti sono individuabili principalmente per asimmetrie informative da mantenere o da creare: finanza, movimenti di valuta e flussi energetici sono i primi soggetti

Chart 23: Average annualized cost of cyberattacks by industry sector (US$mn)



Source: Ponemon

Conclusioni II

- Non ci sono comodi cassetti, né amici stabili, ma un continuum da una dimensione all'altra (concetto di Pericòresi informatica)
- Si passa dalla finanza visibile alla shadow finance a riciclaggio, cibercrimine, cibermafie, ciberattivismo, ciberterrorismo a spionaggi privati e pubblici
- In collegamento di fatto mercati e fornitori legali sono connessi a quelli illegali (darknets)
- Gli attori statali intelligence si servono regolarmente di «contractor» privati, i quali a loro volta produrranno sempre più programmi simili ad avatar

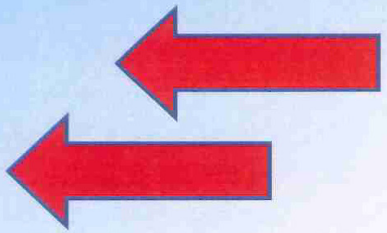
Che fare?

La protezione delle Infrastrutture Critiche (IC) e dei nostri *asset*, reali e virtuali, non può dipendere dal semplice meccanismo della domanda e dell'offerta che caratterizza il mercato.

Nei sistemi economico-istituzionali moderni gran parte delle infrastrutture che gestiscono servizi pubblici essenziali e quelle di rilevanza strategica per il sistema-Paese, sono affidate all'iniziativa di operatori economici privati. Al fine di migliorare la sicurezza delle informazioni e di sviluppare dei *risk-based standards*, è necessario creare una *partnership* fra settore pubblico e privato, stabilendo meccanismi di *information sharing*. Il Partenariato Pubblico-Privato (PPP) costituisce, pertanto, un principio imprescindibile per il successo di ogni strategia di sicurezza cibernetica, che deve essere, per sua natura, dinamica.

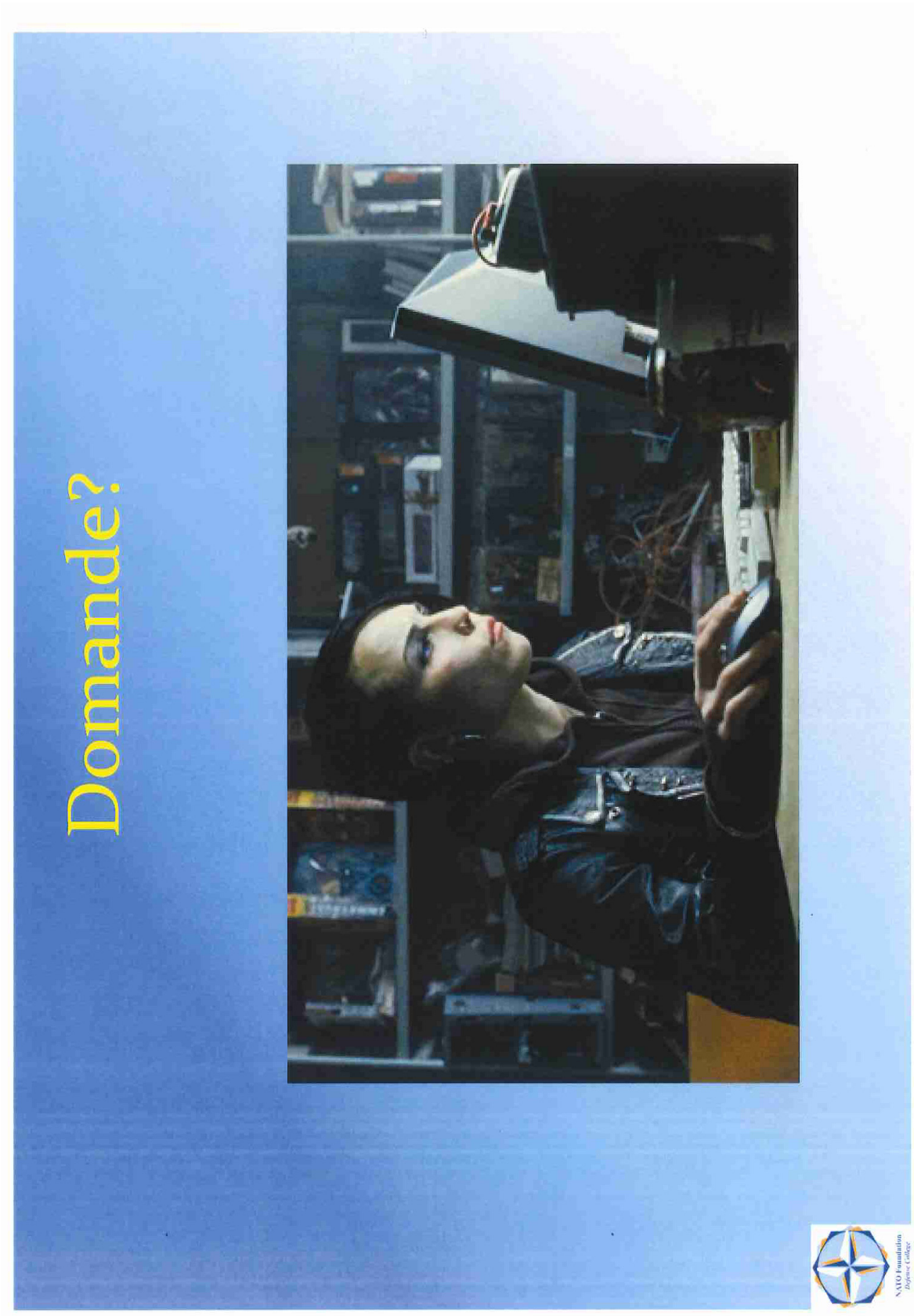
a) la creazione di una dimensione digitale della geopolitica, caratterizzata da confini liquidi, in cui si estrinsecano equilibri di potere non sempre coincidenti con quelli della sfera fisica e della conflittualità cibernetica.

b) i rischi legati alla gestione della *supply chain* di operatori pubblici e privati, laddove una non adeguata cornice di sicurezza potrebbe esporre i prodotti e la componentistica IT a potenziali manipolazioni nei passaggi dal fornitore all'utente finale.



La protezione delle Infrastrutture Critiche dagli attacchi cibernetici: esigenze di sicurezza nazionale e regole di libero mercato.

L. Rosa – Policy Analyst – SIOI Master


Domande?

NDCF: Contacts

Prof. Alessandro Politi

NDCF Director

E-mail: alepolca@iol.it

Web: http://www.ndc-foundation.org

17STC0016690