Attenti allo Stato Etico

Alessandro Guarino

e-Privacy XXI - *Lucca 23/6/2017*

The Speaker

15+ Years in Information/Cyber Security Consultancy

StudioAG
Consulting & Engineering

Speaker Author

Digital Forensics Alumni — 2011

CyCon International Conference on Cyber Conflict — 2013

ISSE 2016 — 2013-2016

E-PRIVACY XX — 2016

pirate security conference psc
IET Events The Institution of Engineering and Technology
Università di Roma Tor Vergata — 2017

Standards

UNINFO

CS·CG CEN/CENELEC/ETSI Cyber Security Coordination Group

ETSI

CEN CENELEC

2011 →

Parole (e fatti) ostili

Vs.

- Una opinione molto diffusa vede i cosiddetti "giganti del web" come la maggiore minaccia alle libertà della rete.
- Il potere degli stati-nazione invece è (e sarà in futuro) incomparabilmente maggiore delle corporation.

La posta

- A cosa serve Internet?
  - Libertà di espressione
  - Libertà di comunicazione (privata)
  - Libertà economiche
    - Nuove opportunità di impresa svincolate dalla geografia
    - Movimento dei capitali

Il dilemma della sovranità

- Le poste sono percepite da molti stati nazionali non come opportunità ma come minacce alla sovranità.
- Viviamo adesso in un periodo storico in cui il revival della sovranità è diffuso (e sostenuto da regimi e anche parti politiche molto diverse)
- Di fatto anche gli stati “liberali” stanno esercitando il loro potere per riprendere il controllo di quello che è percepito (o comunicato…) come un ambito senza legge.
- Le motivazioni espresse sono “I quattro cavalieri dell’apocalisse”
  - Terrorismo - Criminalità
  - Pedopornografia - Evasione fiscale

  (+1 adesso, le “*fake news*”)

Rewind

- L’esplosione dell’accesso a Internet alla fine del secolo scorso fu il risultato di fattori convergenti, sia tecnici che politici e sociali.
- Probabilmente nessuno degli attori coinvolti era pienamente consapevole di cosa sarebbe avvenuto e di quanto la diffusione di Internet sarebbe stata dirompente.
- Lentamente, governi e regolatori hanno iniziato a percepire le potenzialità della rete come una minaccia e non come un’opportunità.
- La tendenza si accelera a partire dal 2001 (che sia un luogo comune non significa che non sia vero)

Internet Governance – Un po' di storia

- Distruzione dei monopoli delle telecomunicazioni negli USA
- La FCC (Federal Communications Commission) decide di riclassificare le trasmissioni di dati come un "servizio a valore aggiunto", quando le telco erano interessate ai servizi voce, creando di fatto un mercato aperto e libero per i servizi digitali (in Nord America)
- Il Free Software Movement – Le licenze libere furono paradossalmente un fattore abilitante per i servizi Internet commerciali.
- Le caratteristiche tecniche della rete (architettura e protocolli).

La tensione

- I poli opposti:
  - Cyberspace as an immaterial realm, where geography (and laws) do not matter
    - *“Governments of the Industrial world, you weary giants […], I come from Cyberspace, the new home of Mind […], You have no sovereignty where we gather.”*
  - The Sovereignty Argument
    - Cyber is only an extension of telecommunications networks, just a new telehgraph, a matter for inter-governmental fora…
    - One of the oldest modern international organizations was established just for that purpose.

Governance in concreto

- La prassi:
  - Formalmente la tensione tra le due concezioni si è tradotta in differenti modelli di governance.
  - La classiche organizzazioni intergovernative (ITU)
  - I modelli di governance “a rete”, che includono attori non-statuali

- Il governo “a rete” era già in essere quando i governi iniziarono a realizzare le potenzialità del cyberspace e a ristabilire le forme tradizionali di sovranità. ICANN *(Internet Corporation for Assigned Names and Numbers)* e la gestione decentralizzate del sistema dei nomi a dominio sono esempi di successo.

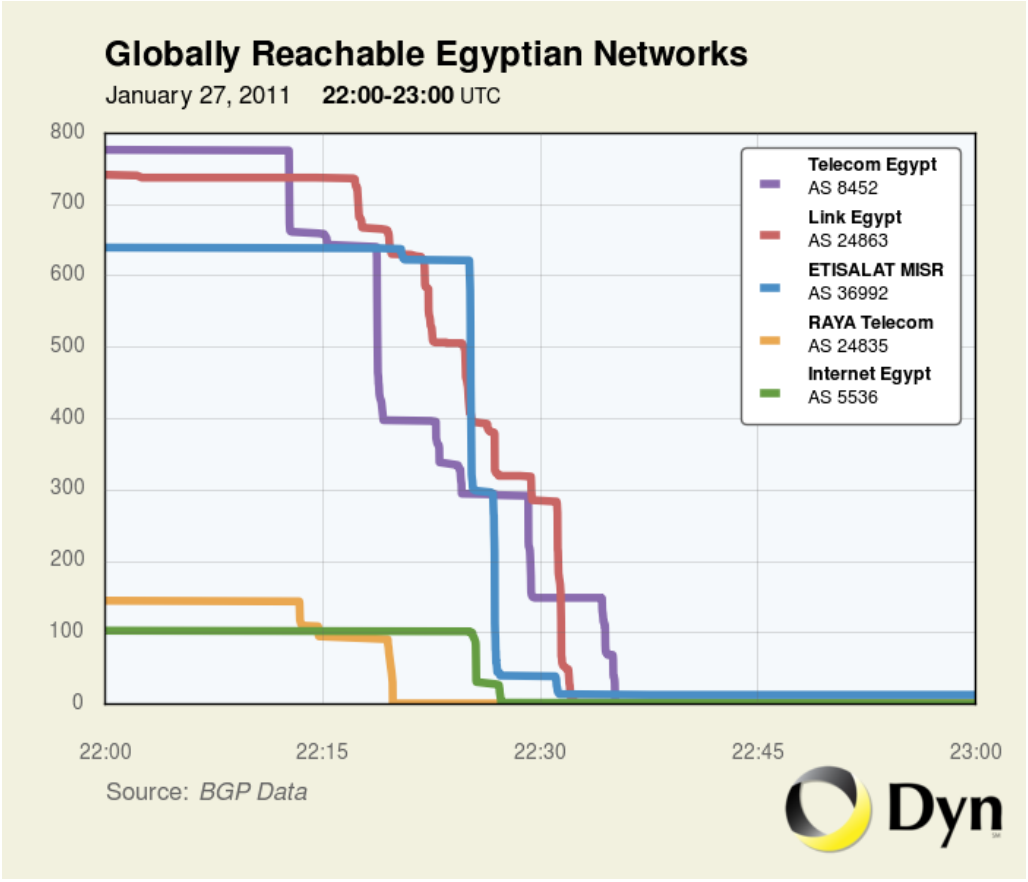
State of the art

- Stiamo assistendo a un ritorno degli stati nazionali a tutti I livelli e alla crisi delle strutture della globalizzazione.
- Esempi:
  - La crisi dell'Unione Europa e Brexit
  - Isolazionismo e protezionismo americano
  - L'avanzata della Cina
  - La Russia "Imperiale"

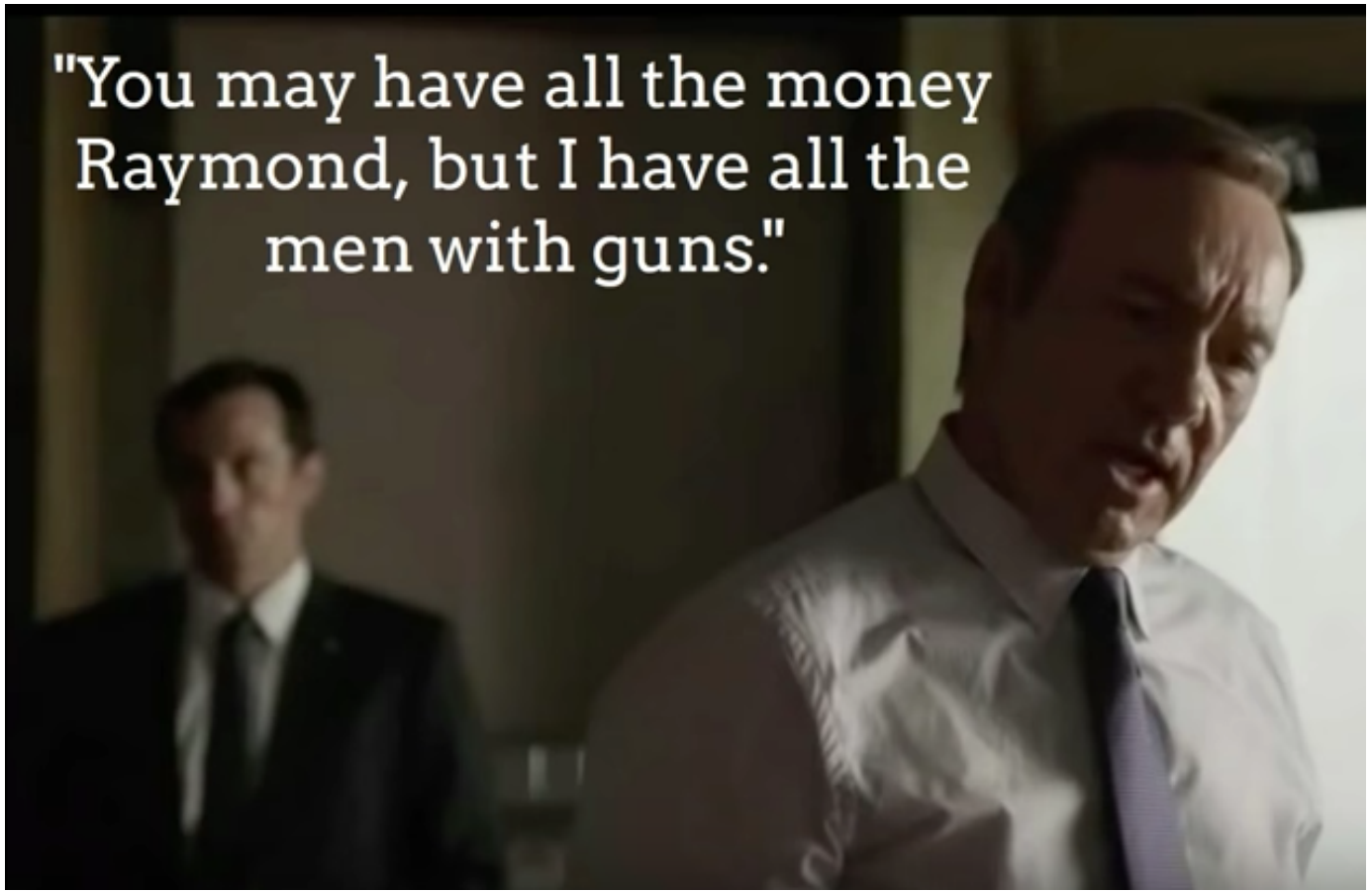
- Nel dominio cyber gli stati (tutti) tendono a riaffermare potere e sovranità, controllare la loro fetta di rete e anche la loro popolazione.

Cyber?

- Il “Cyber” non esiste in realtà.
- E’ realizzato da elementi e infrastrutture ben presenti nello spazio fisico e quindi soggetti al potere dei governi.
- Si può “spegnere Internet” se solo lo si vuole...

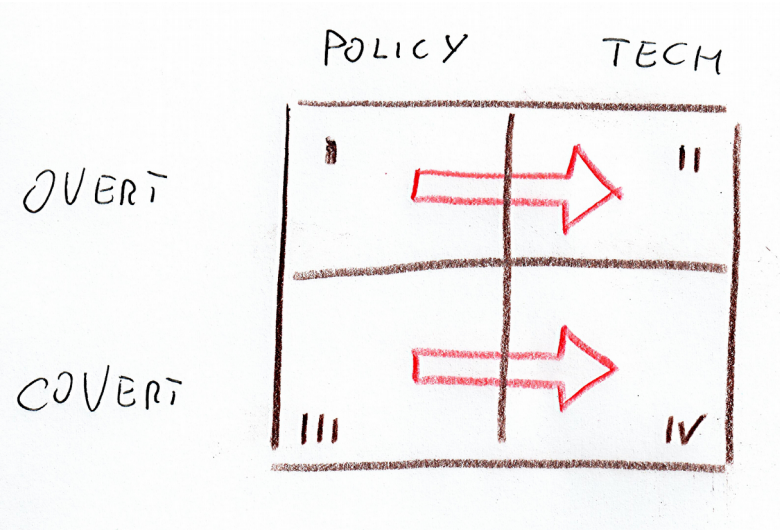


Balance of power



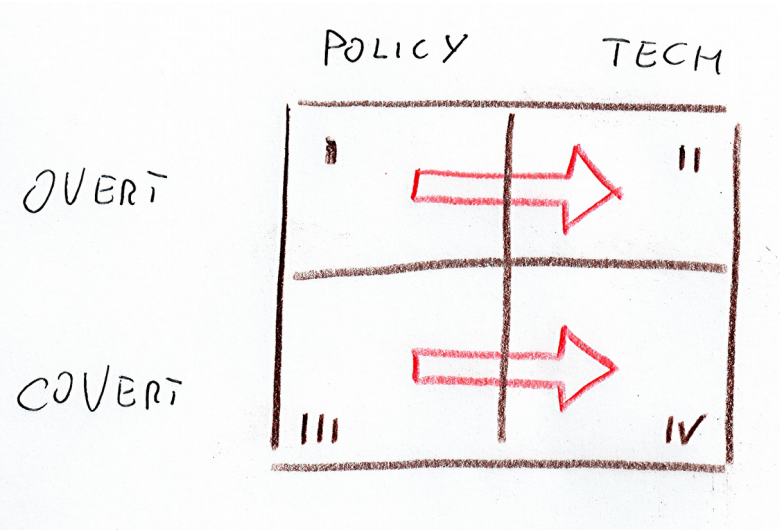
Gli strumenti

- In pubblico...



  - All attempts to bring back cyber governance under state control
  - Controllo dei contenuti e censura
  - Control of the “physical” (e.g. Egypt Block of the Internet in 2011)
  - Policies informing technical means (e.g. “The Great Firewall)

Gli strumenti



- E in privato...
  - Content monitoring on the web and social networks by security agencies
  - “Moral Suasion” (And National Security Letters) on ISPs and network operators.
  - Mass surveillance and bulk collecting
  - Cyber defence of public and private networks

Cina

- The People's Republic could well be considered the champion of the sovereignty argument.
- Beijing sought to establish as clear lines of sovereignty in cyberspace as there were for land, sea, and air, since at least 2010.
- Countries should respect other countries' rights in developing a cyber governing path forward for its own citizens (Position expressed by Xi and also by the Chinese ambassador to the UK at Chatham House Cyber Conference in 2016, inter alia).
- Cyber sovereignty is a fundamental part of national sovereignty and also a mean to counteract perceived "cyber hegemonic" behaviours by other powers.

Cina

- China has been leveraging the UN Charter as justification to extend the principle of sovereign equality to cyberspace.
- Chinese experts were part of the international group of experts that developed Tallinn Manual 2.0
- This achieves two important objectives for Beijing: it demonstrates China's intent on using existing applicable international law to support its proposal, and it shows China's desire to raise such issues to a government level and in an international forum.
- La legge sulla cybersecurity 2017

Cina

- 2015 – Anti Terror Law
  - Compels technology companies to help decrypt information
- 2015 – National Security Law
  - Provides a framework for China's security considerations in the face of emerging threats - national security is an inherently integrated process.
- July 2016 – Overseas Non-Government Organisation Management Law
  - All NGOs are required to get approval from a supervisory unit to operate in China.
- November 2016 – Cyber Security Law

Cina ?

ItaliaOggi Sette
IL PRIMO GIORNALE PER PROFESSIONISTI E IMPRESE

Dio ti vede. E anche il giudice

Con i trojan di Stato può ordinare l'accesso a computer, smartphone, radio, tv, trasformarli in micidiali strumenti d'intercettazione e acquisire tutti i dati

DI MARINO LONGONI
mlongoni@class.it

Nella riforma del processo penale, varata in via definitiva dalla Camera il 14 giugno, c'è un aspetto, passato sottotraccia, che rischia invece di avere effetti dirompenti. Si tratta del comma 84, lettera e), con la quale si legalizzano i captatori informatici, più noti come trojan di Stato. Si tratta di malware che possono essere inseriti in smartphone, computer, apparecchi tv, perfino automobili e in tutti gli altri strumenti connessi a internet e che consentono di assumere il totale controllo da remoto dell'apparecchio infettato con conseguente possibilità di accedere a tutto il suo contenuto (contatti, email, dati di navigazione, comunicazioni telefoniche, chat, file, foto ecc.) e di attivare, sempre da remoto, il microfono o la telecamera, trasformando il cellulare o la playstation in uno strumento di intercettazione. In pratica questi virus una volta iniettati possono intercettare tutte le conversazioni, email o qualsiasi altro tipo di dato, possono anche prendere documenti, foto e video e sparire senza lasciare traccia. Infine possono modificare i contenuti dei file e dei dati presenti negli strumenti informatici. Le intercettazioni telefoniche via cavo sono ormai preistoria. Queste tipologie di indagine potranno essere attivate non solo per la ricerca di prove relative ai reati più gravi (mafia, terrorismo, concorrenza sleale), ma anche per attività criminali minori, collegate a sostanze stupefacenti, reati di ingiuria o minaccia, frode commerciale e vendita di prodotti alimentari non genuini. Praticamente sempre.

Di fatto con questa norma si finisce per dare una copertura giuridica molto ampia a una prassi già da tempo adottata dai tribunali e legittimata finora, ma in modo parziale e incompleto, da poche sentenze della Corte di cassazione. La più importante è la Sezioni unite n. 26889/16, con cui la Corte ha sancito la legittimità, limitatamente ai procedimenti di criminalità organizzata, dell'uso dei captatori informatici al fine di effettuare intercettazioni di conversazioni tra presenti in luoghi di privata dimora.

Naturalmente ad occuparsi di queste attività saranno società private delegate dal tribunale. Società commerciali che, una volta sperimentato il potere enorme che le conoscenze informatiche mettono a loro disposizione, potrebbero essere anche tentate (loro o qualcuno dei loro dipendenti) di prestare i loro servigi non solo ai tribunali. I clienti non mancano di sicuro. Quello che una volta gli investigatori privati facevano con grande impegno e dispendio di tempo, e con risultati spesso modesti, ora si può fare a costi contenuti e con la garanzia di ottenere una quantità di informazioni sterminata. E certamente già lo si fa su larga scala in tutto il mondo. Basti questo caso, ovviamente non di pubblico dominio: una grande azienda italiana del fashion si accorge che i suoi modelli, dopo due o tre giorni dalle sfilate sono già in vendita su internet, identici, ovviamente taroccati. Chiede la consulenza di un esperto in cybercrime e si accorge che, grazie a un trojan, tutto quella che passava sui suoi computer veniva immediatamente girato a un server cinese, dove aziende specializzate riuscivano a produrre e commercializzare in tutto il mondo i suoi modelli subito dopo la presentazione ufficiale.

Secondo Europol, la bassa probabilità di identificare e perseguire i crimini informatici li colloca tra le attività più redditizie e a basso rischio da un punto di vista criminale. Nel 2016 il tasso di crescita di queste attività ha superato il 70%. Nel Regno Unito la criminalità informatica rappresenta il 53% di tutti i crimini commessi. Il costo del cybercrimine nell'economia globale si aggira tra i 375 e i 575 miliardi di dollari. E non fa che crescere.

Oggi ancora poche persone sono consapevoli dei rischi connessi all'uso degli strumenti elettronici (ma i manager delle più importanti società americane hanno già l'accortezza di lasciare i propri smartphone in un'altra stanza, quando devono partecipare a riunioni importanti). Non c'è dubbio che di qui a pochi anni la consapevolezza di questi rischi sarà generale. A quel punto la libertà di comunicazione, che ha costruito la più forte spinta all'espansione della rete, si potrebbe ribaltare nel suo contrario.

Come le strade romane nel medioevo, sempre più infestate di briganti, finirono per non essere più utilizzate, sarà questo, a breve, anche il destino delle autostrade informatiche?

La manovra correttiva taglia il traguardo: nuove regole su acquisti e importazioni e da luglio split payment allargato

SECURITY
Bitdefender

SMART HOME SECURITY | TIPS AND TRICKS | SECURITY VIDEOS

INDUSTRY NEWS

Mexican Government Accused of Illegally Using Mobile Spying Software on Local Journalists and Activists

4 hours ago · 2 Min Read

Sicurezza 2017

Draft Regulations laid before Parliament under section 267(3)(i) of the Investigatory Powers Act [illegible] roval by resolution of each House of Parliament.

DRAFT STATUTORY INSTRUMENTS

2017 No.

INVESTIGATORY POWERS

vestigatory Powers (Technical Capability) Regulations 2017

Made - - - - ***

Coming into force - - ***

The Secretary of State, in exercise of the powers conferred by section 253(3) and (5) of the Investigatory Powers Act 2016(a), makes the following Regulations:

In accordance with section 253(4) of that Act, the Secretary of State considers that the obligations in the Schedules to these Regulations are obligations that are reasonable to impose on those

Democracy

Thomas Rid ✓
@RidT

Following

Theresa May's comments on the London Bridge attack—predictably—include comments on the internet. I footnoted this section in plain English:

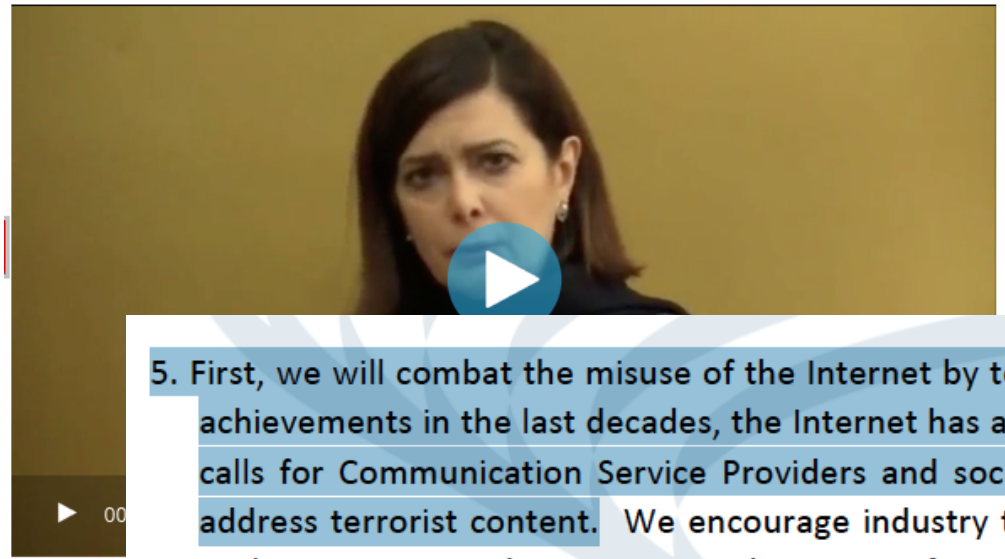
Traduci dalla lingua originale: inglese

> Second, we cannot allow this ideology the safe space[1] it needs to breed. Yet that is precisely what the internet – and the big companies[3] that provide internet-based services – provide. We need to work with allied, democratic governments[4] to reach international agreements that regulate cyberspace[2] to prevent the spread of extremism and terrorist planning. And we need to do everything we can at home to reduce the risks of extremism online.
>
> Third, while we need to deprive the extremists of their safe spaces online,[5] we must not forget about the safe spaces that continue to exist in the real world. Yes, that means taking military action to destroy ISIS in Iraq and Syria. But it also means taking action here at home. While we have made significant progress in recent years, there is – to be frank – far too much tolerance of extremism in our country.

RETWEET 74 MI PIACE 71

Meno seriamente...

Facebook, Boldrini: “Basta con fascismo e odio sui social. Zuckerberg dica da che parte sta”



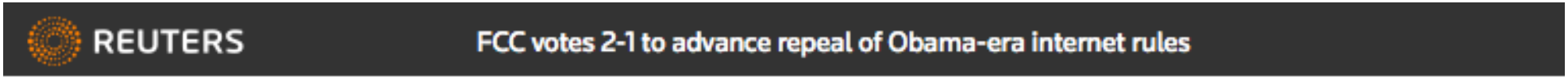
di Gisella

G7 2017 TAORMINA

G7 Taormina Statement

5. First, we will combat the misuse of the Internet by terrorists. While being one of the most important technological achievements in the last decades, the Internet has also proven to be a powerful tool for terrorist purposes. The G7 calls for Communication Service Providers and social media companies to substantially increase their efforts to address terrorist content. We encourage industry to act urgently in developing and sharing new technology and tools to improve the automatic detection of content promoting incitement to violence, and we commit to supporting industry efforts in this vein including the proposed industry-led forum for combatting online extremism. We will support the promotion of alternative and positive narratives rooted in our common values and with due

Anche i livelli più bassi...



INNOVATION AND INTELLECTUAL PROPERTY | Thu May 18, 2017 | 5:42pm EDT

FCC votes 2-1 to advance repeal of Obama-era internet rules

- Vuol dire modificare uno dei fattori che negli anni 1990 ha permesso la diffusione di Internet – la classificazione come “utility” della trasmissione dei dati.

- La discussione sulla Net Neutrality è in corso anche in Europa

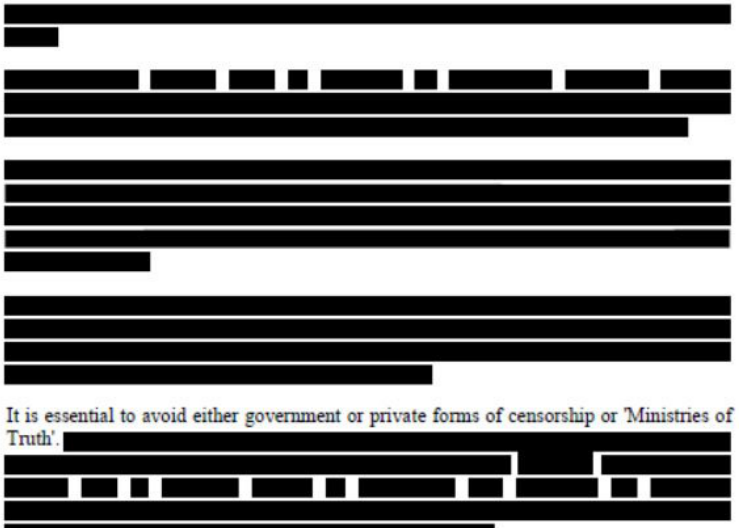
Qualche conclusione

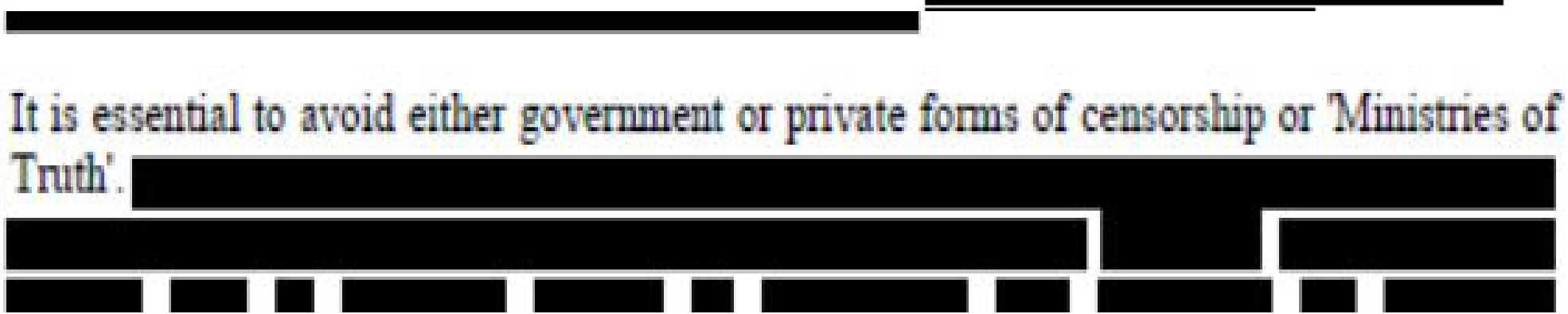
- Nella regolazione della rete non si prescinde dai governi
- La sovranità è un principio chiave
  - Il substrato hardware is soggetto ad essa (oppure regolato)
  - Anche I dati stessi (dibatttito sulla definizione di “object” con tutte le conseguenze del caso - duty to protect, forbidden attacks...)
- La prassi dei paesi “liberali” è sempre più simile a quella dei paesi non democratici
- Dove è possibile, gli attori non statuali devono essere coinvolti per preservare quello che rimane della libertà della rete (Imprese, NGO, gruppi di interesse, anche I singoli).

Postilla Europea...

A new Hope?
La Commissione LIBE ha emendato il regolamento “ePrivacy” raccomandando l’adozione della crittografia “end to end”

The Empire Strikes Back
Arne Semsrott – Richiesta di accesso documenti alla Commissione sulle “*fake news*” – 1/ 2017





Grazie

a.guarino@studioag.eu

@alexsib17

Slides available on:
www.studioag.pro

StudioAG – Consulting & Engineering
www.studioag.eu

Riferimenti e Link

J.P. Barlow – A Declaration of the Independence of Cyberspace – Crypto Anarchy, Cyberstates and Pirate Utopias, ed. Ludlow, Cambridge 2001

Alessandro Guarino – Cyberspace Does not Exist – Strange Loops 15/1/2015 - http://www.strangeloops.pro/en/2015/01/la-nuvola-non-esiste

M.L. Mueller – Networks and States – MIT Press – Cambridge 2010

AskTheEU – Richiesta sulle “fake news”- Tutti i documenti - https://www.asktheeu.org/en/request/concepts_against_fake_news?nocache=incoming-13625#incoming-13625

Alessandro Guarino - Imposing and Evading Cyber Borders - The Dilemma of Sovereignty – Presentazione – Pirate Security Conference 2017 – Monaco

Alessandro Guarino e Emilio Iasiello - “Imposing and Evading Cyber Borders - The Dilemma of Sovereignty” - Cyber, Intelligence, and Security Vol 2. Giugno 2017 – INSS Tel Aviv