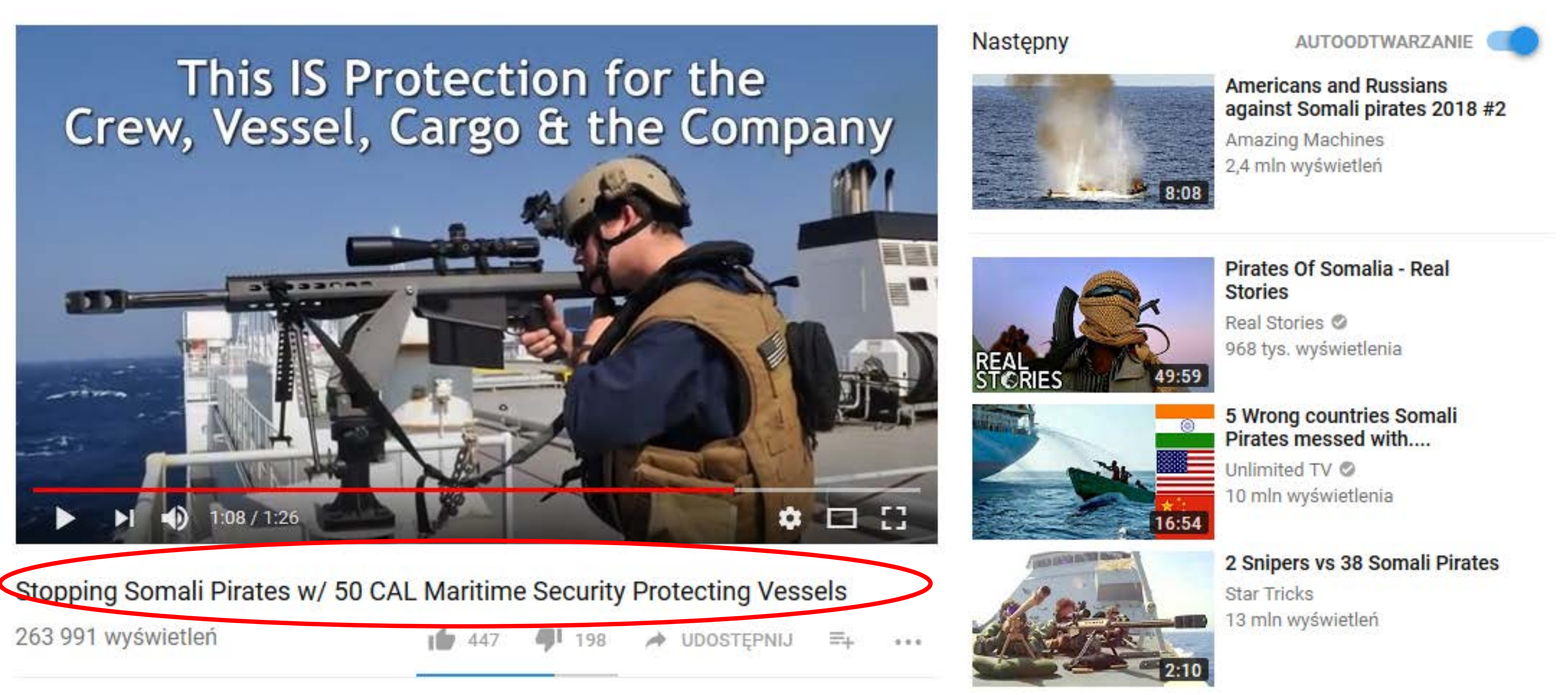
Protecting
the Public Core of the Internet

Joanna Kulesza

University of Lodz, Poland



Stopping Somali Pirates w/ 50 CAL Maritime Security Protecting Vessels

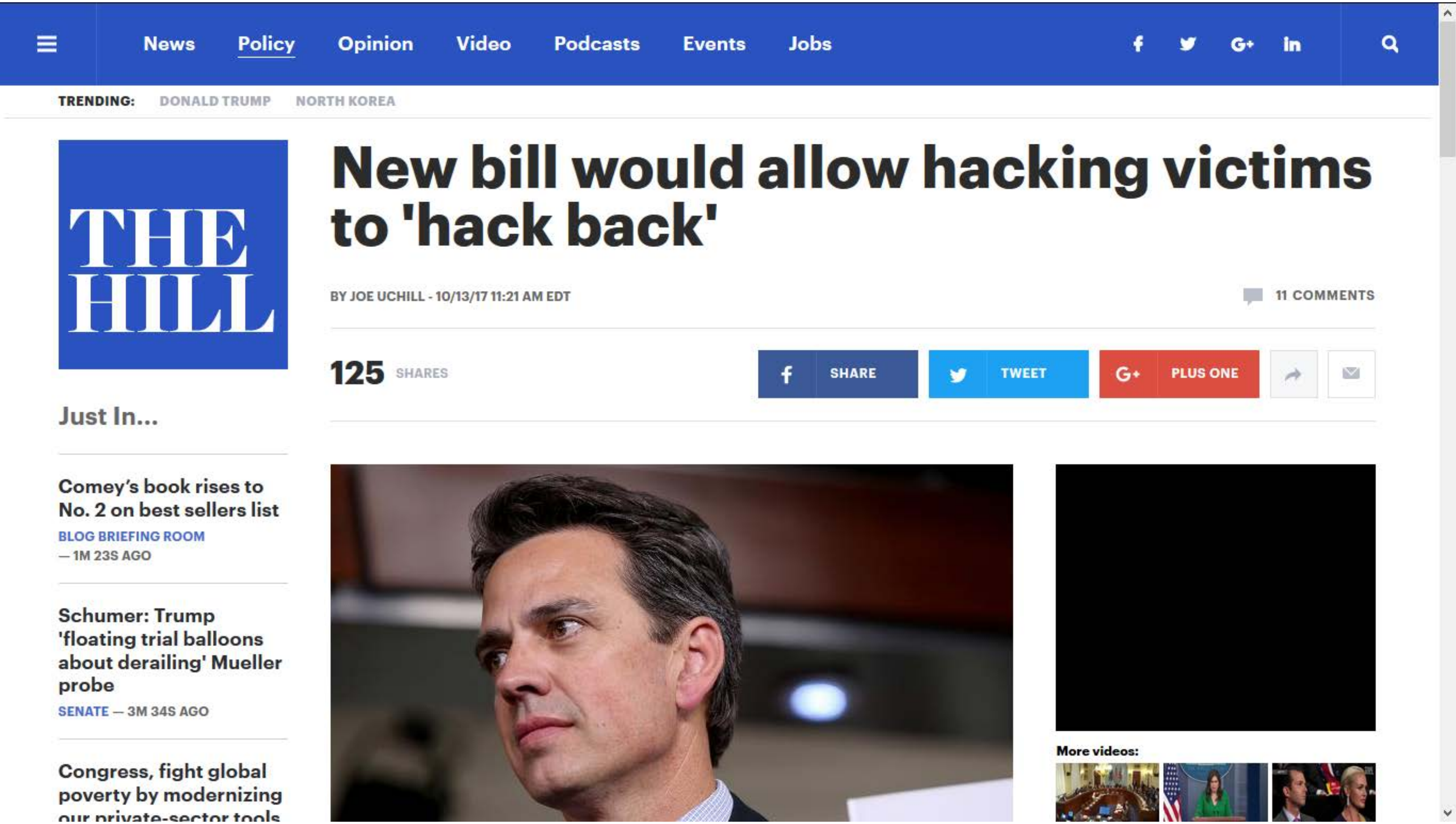
263 991 wyświetleń

Americans and Russians against Somali pirates 2018 #2
Amazing Machines
2,4 mln wyświetleń

Pirates Of Somalia - Real Stories
Real Stories
968 tys. wyświetlenia

5 Wrong countries Somali Pirates messed with....
Unlimited TV
10 mln wyświetlenia

2 Snipers vs 38 Somali Pirates
Star Tricks
13 mln wyświetleń



New bill would allow hacking victims to 'hack back'

BY JOE UCHILL - 10/13/17 11:21 AM EDT

11 COMMENTS

Just In...

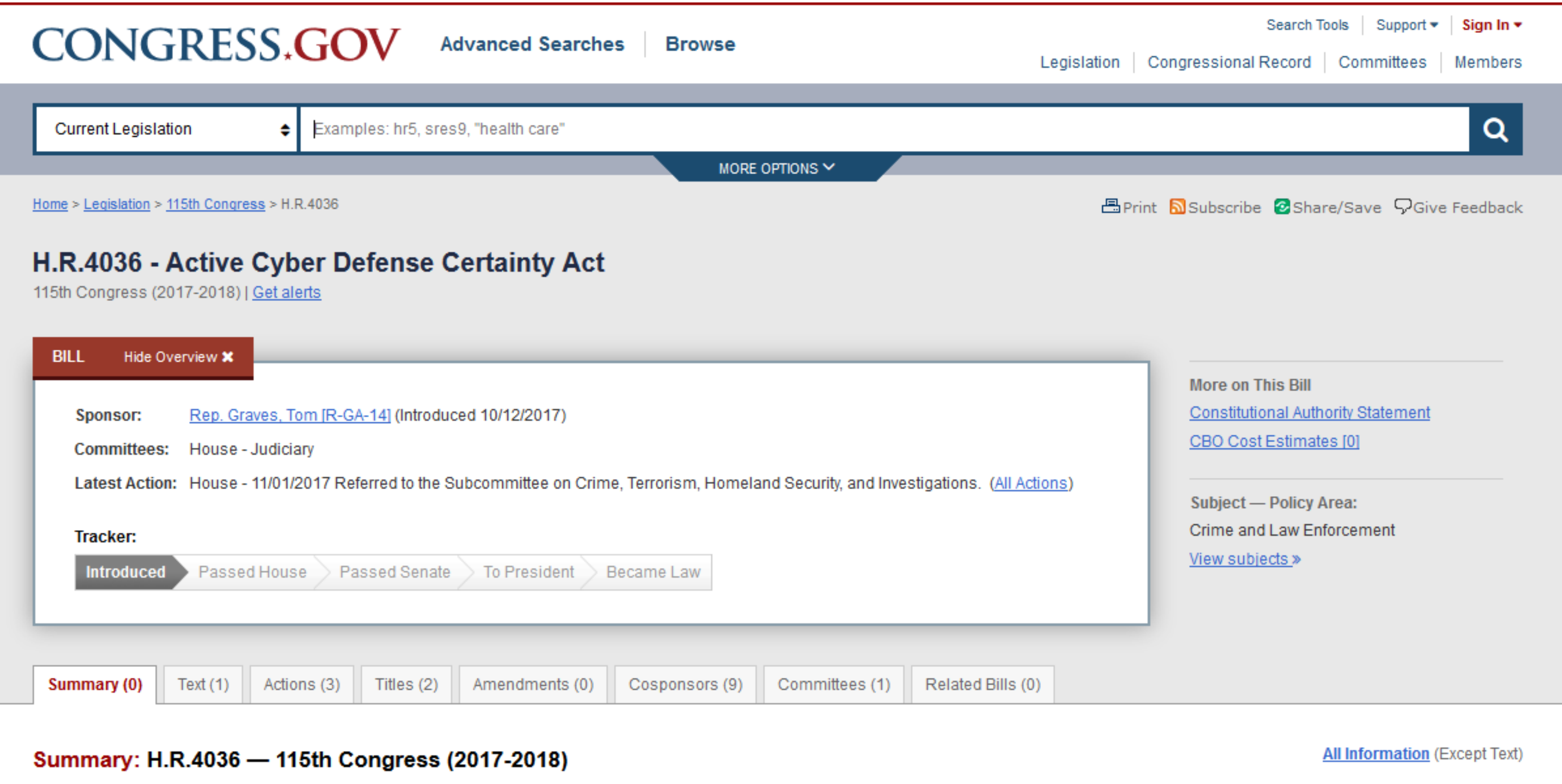
Comey's book rises to No. 2 on best sellers list

BLOG BRIEFING ROOM — 1M 23S AGO

Schumer: Trump 'floating trial balloons about derailing' Mueller probe

SENATE — 3M 34S AGO

Congress, fight global poverty by modernizing our private-sector tools



Home > Legislation > 115th Congress > H.R.4036

H.R.4036 - Active Cyber Defense Certainty Act

115th Congress (2017-2018) | Get alerts

Sponsor: Rep. Graves, Tom [R-GA-14] (Introduced 10/12/2017)

Committees: House - Judiciary

Latest Action: House - 11/01/2017 Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. (All Actions)

Tracker:

Introduced > Passed House > Passed Senate > To President > Became Law

More on This Bill

Constitutional Authority Statement

CBO Cost Estimates [0]

Subject — Policy Area:

Crime and Law Enforcement

View subjects »

Summary: H.R.4036 — 115th Congress (2017-2018)

All Information (Except Text)

Internet policy development reference frameworks

	non-enforceable policy concepts	enforceable norms recognized within international law (of peace)
global public goods	X	
global commons (Ostrom's „common pool resource"; „imperfect public good")	X	
international spaces and shared resources		X
critical infrastructure protection		X

Other referenced areas of international law

Areas of international law that can be used for reference with regard to protecting the core of the Internet include:

- law of the sea
- air law
- space law
- diplomatic and consular law
- international human rights law
- international telecommunication law
- environmental law
- law on international liability
- law of treaties
- international trade law
- antiterrorist laws and policies
- international sports law and policies
- Global Administrative Law (GAL)

shared principles

Overarching international law principles relevant to all those specified regimes:

1) sovereignty
2) jurisdiction
3) state responsibility
4) due diligence.

Recommendation: enhance further debate on protecting Internet Public Policy on the appriopriate appliaction of those principles

venues for further debate

organization/ characteristics	ICANN	ITU	IGF	ISOC	IETF	NATO	NetMundial
multistakeholder	X		X				X
bottom-up model of governance	X		X	X	X		X
standard setting	X	X			X		
operates based on contractual compliance	X						
governmental		X				X	
sets internationally enforceable obligations for states		X				X	

Recommendations
(need for enhanced cooperation)

- Uniform, universal standards of protection for all networks and services recognized as fundamental to the global networks' stable and reliable operation are to be identified through 1) international cooperation, 2) exchange of good practices and 3) benchmarking.
- States must facilitate the **creation and support the maintenance of international forum/fora for IG and cybersecurity practice and experience exchange**, either within existing specialized organizations (dealing with e.g. energy supply or air transportation) or within a separate, Internet-focused venue.

Recommendations
(treaties and contractual compliance)

The multistakeholder model of Internet governance necessitates the transposition of international norms on Internet governance onto national laws, regulations and sanctions for any protection of this global asset to be effective.

It is possible that the Internet's multistakeholder model with its unique distribution of power and authority will help to better enforce private obligations among various actors. The international community may consider **one of the two following scenarios**:

1) traditional international law making through a treaty (e.g. an Internet framework convention) effective against all signatories, necessitating its transposition onto national laws;
2) a novel approach to international lawmaking, inclusive of non-state actors, in particular open to ICANN and RIRs, who could use the conventional framework as a point of departure for their contractual compliance mechanisms.

Recommendations (norm building)

Contemporary international landscape lacks one venue where pertaining issues of protecting Internet's key resources can be discussed.

It is therefore **to be recommended for the existing venues to continue their work, aiming to ensure a coherent approach to cybersecurity**.

As has been the case with the law of the sea or, more recently, environmental law, the principles shared among those dispersed initiatives may serve as a foundation for a comprehensive customary framework, later to be transposed onto an international, contractual compromise.

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

IGF
GENEVA 2017

www.cyberstability.org | info@cyberstability.org | cyber@hcss.nl | @theGCSC

THE PUBLIC CORE PRINCIPLE

SUBMISSION TO THE 2017 IGF-BPF CYBERSECURITY BY THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

The Internet was described in the 2003[1] as being a "global facility". What this means has never been adequately determined, although a number of prominent statements have been made over the past years that have described the Internet as representing in whole or in part a "global commons". The Global Commission on the Stability of Cyberspace (GCSC) has investigated the question, and is favoring the concept of a "Public Core" of the Internet.[2] We are open to expanding this concept to that of an operational principle, such as those that have been put forward as Core Values by the IGF Dynamic Coalition on Core Internet Values[3] or described as Internet Invariants by ISOC.[4]

The GCSC submits that the Internet is a common good for humanity.[5] Parts of the Internet further conform to the notion of a "global public good", providing essential functionality to the Internet as a whole and which underpins its normal operation. If one or more of these core functionalities are undermined or disrupted, then the security and stability of the Internet can be significantly impacted, decreasing trust and confidence in the domain amongst all stakeholders. These core functionalities are encapsulated in the concept of the "Public Core".

Following the original WRR study on the Public Core, the author of the concept Dennis Broeders sketched out some further ideas at a public hearing of the GCSC Full Commission Meeting in Tallinn in May 2017. At his hearing, Broeders defined the core as encompassing two elements: (i) a clearly distinguishable "Inner Core" which consists of the core functionality underpinning the Internet (in particular the forwarding and naming functions and infrastructure of the Internet and those actors responsible for their day to day management[6]), and (ii) a less clearly distinguishable "Outer Core" of

For the basic definition, the GCSC has largely concluded it deliberations around a proposed norm[7] of behavior to be considered by all stakeholders in its "Call to Protect the Public Core of the Internet"[8]:

> *"Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace".*[9]

The GCSC welcomes feedback on this norm, both in terms of wording as well as possible levers for implementation. Many different variants of the above were considered. The present wording of the protective norm above is considered wide enough that it would encapsulate both clearly identifiable core functions (such as the naming and forwarding functions) but also allow other definitions to take root. Indeed, one interpretation of the norm is that it gives rise to a general precautionary principle applicable to all actors to be exercised by all stakeholders whose standards, products, services, legislations or policy initiatives could reasonably become critical to the overall security and stability of the overall functionality of the Internet. This principle would encourage a higher standard of duty of care – for instance in considering security issues at the design stage – for all actors whose new standards, products, services, legislations or policies could reasonably be assessed as *potentially* becoming critical for the functioning of the Internet as a whole. In the best case, this could become known as the "Public Core Principle", the reinforcement of the "Do No Harm Principle" to all Internet stakeholders.

2017 consensus report on „Internet's public core"

While other elements might be considered as crucial for the network's operation, as for late 2017 the consensus on critical Internet resources amounts to a short list and includes:

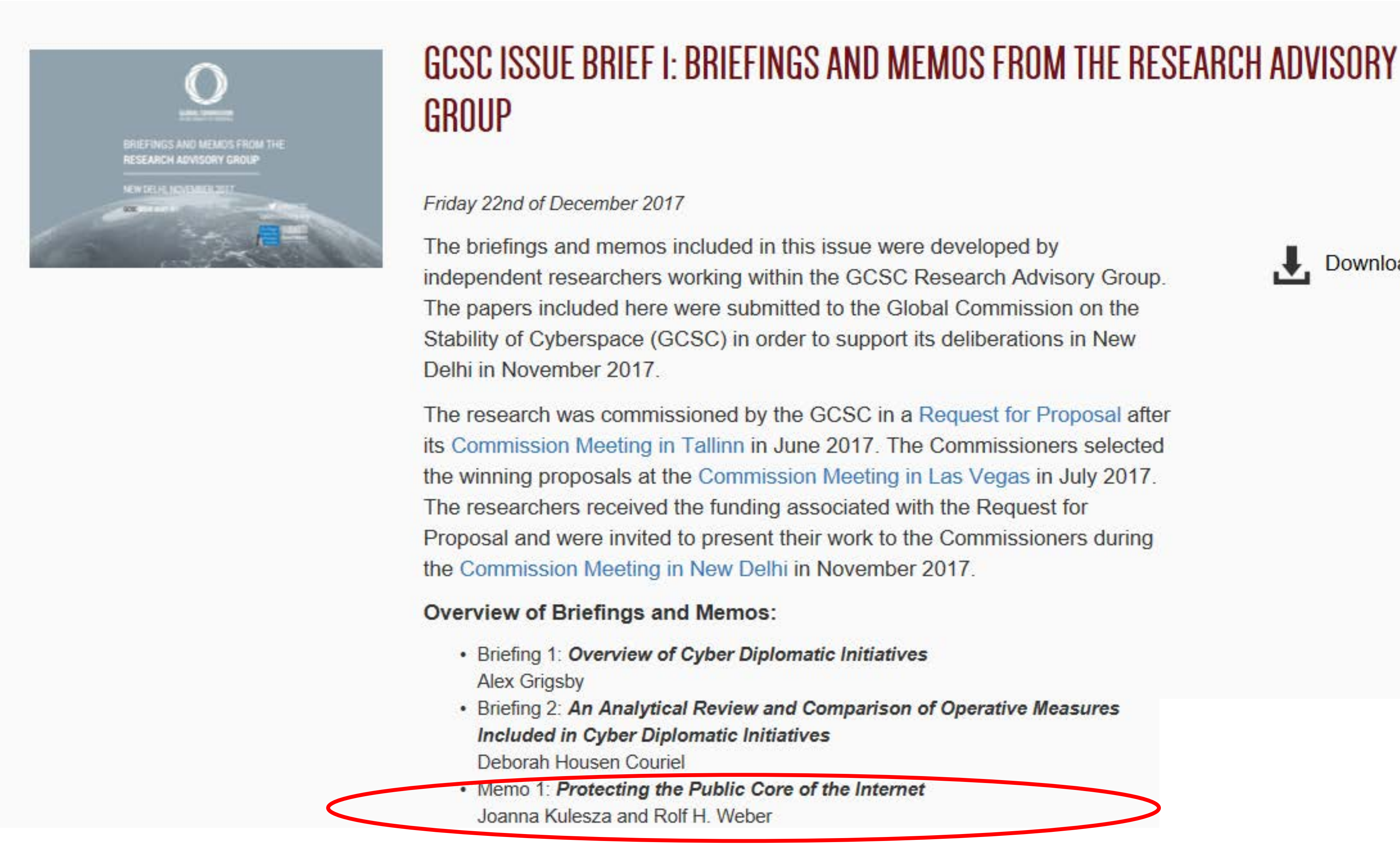
1) Internet backbone networks,

2) DNS servers,

3) Internet Exchange Points (IXPs) and

4) TLD related services (registries and registrars).

While a progressive, open, catalogue of critical Internet resources is to be identified through dialogue and diplomacy, the international need for its legal and organizational protection is beyond doubt.



GCSC ISSUE BRIEF I: BRIEFINGS AND MEMOS FROM THE RESEARCH ADVISORY GROUP

Friday 22nd of December 2017

The briefings and memos included in this issue were developed by independent researchers working within the GCSC Research Advisory Group. The papers included here were submitted to the Global Commission on the Stability of Cyberspace (GCSC) in order to support its deliberations in New Delhi in November 2017.

The research was commissioned by the GCSC in a Request for Proposal after its Commission Meeting in Tallinn in June 2017. The Commissioners selected the winning proposals at the Commission Meeting in Las Vegas in July 2017. The researchers received the funding associated with the Request for Proposal and were invited to present their work to the Commissioners during the Commission Meeting in New Delhi in November 2017.

Overview of Briefings and Memos:

- Briefing 1: ***Overview of Cyber Diplomatic Initiatives***
  Alex Grigsby
- Briefing 2: ***An Analytical Review and Comparison of Operative Measures Included in Cyber Diplomatic Initiatives***
  Deborah Housen Couriel
- Memo 1: ***Protecting the Public Core of the Internet***
  Joanna Kulesza and Rolf H. Weber

THANK YOU

JOANNA KULESZA
UNIVERSITY OF LODZ

JOANNAKULESZA@GMAIL.COM