GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

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

DEFINITION OF THE PUBLIC CORE, TO WHICH THE NORM APPLIES

Bratislava, May 2018

In November, 2017, the Global Commission on the Stability of Cyberspace (GCSC) issued its *Call to Protect the Public Core of the Internet*:

> ## NON-INTERFERENCE WITH THE PUBLIC CORE
>
> **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.**

As input to its process, a working group of the GCSC conducted a broad survey of experts on communications infrastructure and cyber defense to assess which infrastructures were deemed most worthy of protection. On a scale of zero to ten, with zero being "unworthy of special protection" and ten being "essential to include in the protected class," all surveyed categories ranked between 6.02 and 9.01. Accordingly, the Commission defines the phrase "the public core of the Internet" to include packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media. Specifically:

Packet routing and forwarding include, but are not limited to: the equipment, facilities, information, protocols, and systems which facilitate the transmission of packetized communications from their sources to their destinations. This includes Internet Exchange Points (the physical sites where Internet bandwidth is produced) and the peering and core routers of major networks which transport that bandwidth to users. It includes systems needed to assure routing authenticity and defend the network from abusive behavior. It includes the design, production, and supply-chain of equipment used for the above purposes. It also includes the integrity of the routing protocols themselves and their development, standardization, and maintenance processes.

Naming and numbering systems include, but are not limited to: systems and information used in the operation of the Internet's Domain Name System, including registries, name servers, zone content, infrastructure and processes such as DNSSEC used to cryptographically sign records, and the whois information services for the root zone, inverse-address hierarchy, country-code, geographic, and internationalized top level domains and for new generic and non-military generic top-level domains.

It includes frequently used public recursive DNS resolvers. It includes the systems of the Internet Assigned Numbers Authority and the Regional Internet Registries which make available and maintain the unique allocation of Internet Protocol addresses, Autonomous System Numbers, and Internet Protocol Identifiers. It also includes the naming and numbering protocols themselves and the integrity of the standardization processes and outcomes for protocol development and maintenance.

The cryptographic mechanisms of security and identity include, but are not limited to: the cryptographic keys which are used to authenticate users and devices and secure Internet transactions, and the equipment, facilities, information, protocols, and systems which enable the production, communication, use, and deprecation of those keys. This includes PGP keyservers, Certificate Authorities and their Public Key Infrastructure, DANE and its supporting protocols and infrastructure, certificate revocation mechanisms and transparency logs, password managers, and roaming access authenticators. It also includes the integrity of the standardization processes and outcomes for cryptographic algorithm and protocol development and maintenance and the design, production, and supply-chain of equipment used to implement cryptographic processes.

Physical transmission media include, but are not limited to: physical cable systems and installations for wired communications serving the public, whether fiber or copper. This includes terrestrial and undersea cables and the landing stations, datacenters, and other physical facilities which support them. It includes the support systems for transmission, signal regeneration, branching, multiplexing, and signal-to-noise discrimination. It is understood to include cable systems that serve regions or populations, but not those that serve the customers of individual companies.

Some experts believe that far more categories of Internet and ICT-enabled infrastructure are deserving of protection, so this definition may be broadened in the future.