

# SAC050 SSAC Advisory on DNS Block – Benefits Versus Harms Patrik Fältström, SSAC Chair



# Background



- Blocking or altering responses to Domain Name System (DNS) queries is increasingly prominent.
- Technical approaches to DNS blocking are intended to affect users within a given administrative domain, such as a privately or publicly operated network.

# Background, Continued



- Preventing resolution of the domain name into an IP address will prevent immediate connection to the named host, although circumvention techniques may allow connection to the intended host anyway.

# Principles



To avoid collateral damage or unintended consequences:

- Impose a policy on a network and users over which an organization exercises administrative control.
- Determine that the policy is beneficial to the organization's interests and the interests of its users.
- Implement the policy using a technique that is least disruptive its network operations and users.
- Make a concerted effort to do no harm to networks or users outside its policy.

# First, Do No Harm



- Consider the possible harm that an intervention might cause.
- Do not adversely affect Internet users outside of the organization's policy domain.

# Conclusion



- All technical approaches to DNS blocking and attempts to circumvent will impact:
  - Security and/or stability of users and applications; and
  - coherency or universal resolvability of the namespace.

# Role for the SSAC



## The SSAC:

- *Cannot* draw a line between "good DNS blocking" and "bad DNS blocking" in the DNS hierarchy.
- *Can* suggest guidelines to use in evaluating which approaches to blocking are likely to incur the fewest unintended consequences and least harm outside the blocked domain.