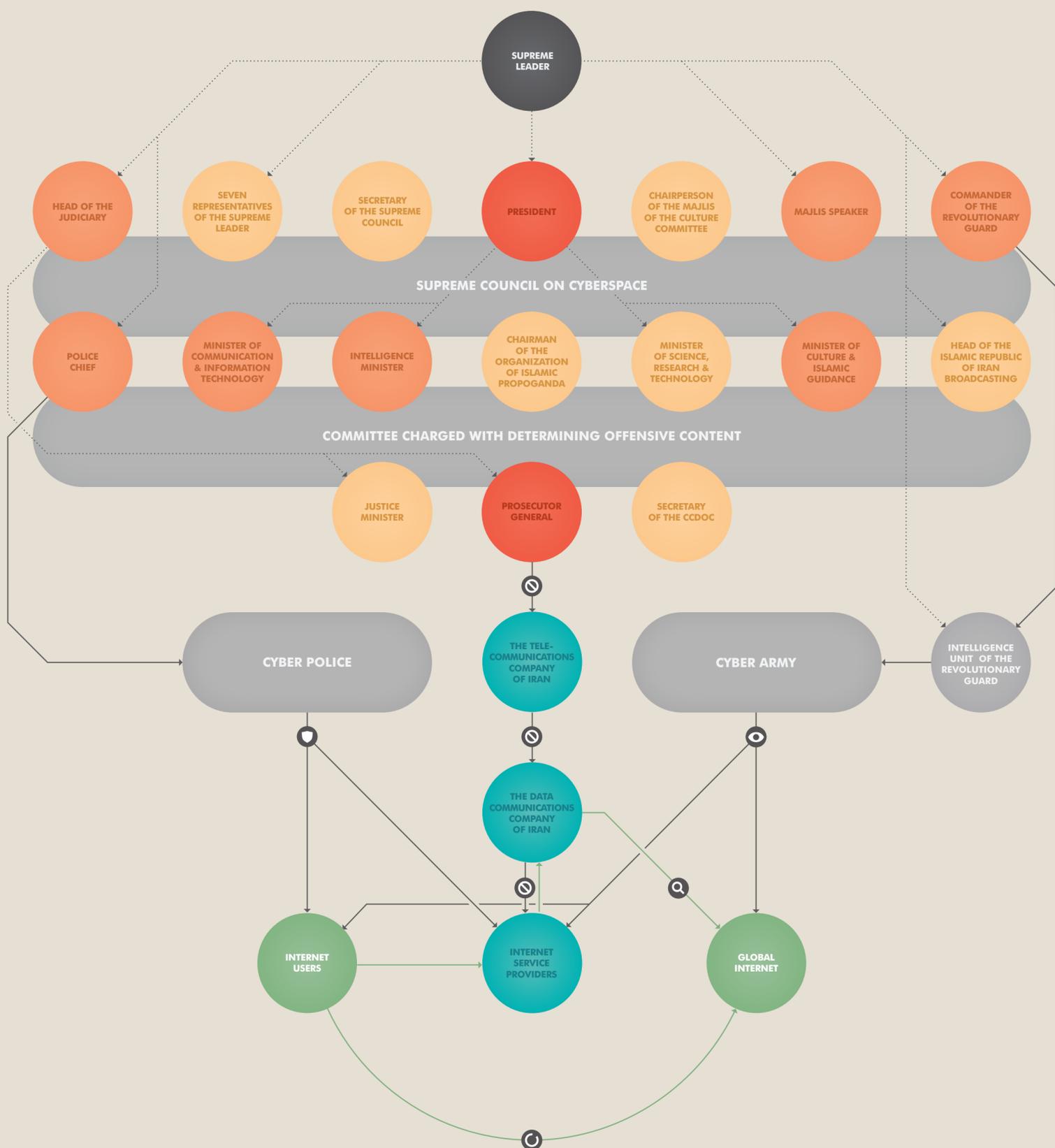




INTERNET CENSORSHIP IN IRAN

This graphic illustrates the constellation of bodies currently involved in Internet censorship in Iran. It attempts to show the complexity of Iran's Internet governance system by mapping the relationship between the different policy-making and enforcement bodies involved in Internet censorship and filtering. It spotlights four new bodies—the Supreme Council on Cyberspace, the Committee Charged with Determining Offensive Content, the Cyber Army, and the Cyber Police—that have emerged since 2009 as key institutions responsible for controlling the flow of online communications, both within Iran and between Iranians and the global cybersphere.



- CENSORING BODY CHAIRPERSON
- MAJOR DECISION MAKER
- MINOR DECISION MAKER
- TECHNOLOGY BODY
- CENSORING BODY
- FILTERS AND BLOCKS
- ARRESTS AND MONITORS
- MONITORS AND HACKS
- DEEP-PACKET INSPECTION
- CIRCUMVENTION TECHNOLOGY
- DIRECTLY APPOINTS
- OVERSEES
- FLOW OF WEB TRAFFIC

Supreme Leader

The most powerful decision maker in Iran, the Supreme Leader has broad direct and indirect legislative and policy-setting powers over Internet communications. The Supreme Leader appoints directors of key military, security and governmental posts, which also serve as members of bodies involved in shaping and implementing Internet censorship in Iran.

Supreme Council on Cyberspace (SCC)

The top policy-making body for cyber activities in Iran, formed by the Supreme Leader in April 2012 to develop the state's domestic and international cyber policies in response to the "soft war" with the west.

Committee Charged With Determining Offensive Content (CCDOC)

The "filtering committee" is responsible for identifying web content to be filtered and blocked. The CCDOC creates lists of illegal websites and online content that violates public morals, contradicts Islam, threatens national security, criticizes public officials or organizations, or promotes cyber crimes or the use of circumvention tools. The SCC and the CCDOC share seven common members. This shows the lack of a coherent division of powers and responsibilities between officials in charge of making policies and those responsible for implementing censorship decisions.

Filtering List

The Prosecutor General's Office, as head of the filtering committee, issues the filtering list to the Telecommunications Company of Iran (TCI), the state-controlled company responsible for Internet and communications services in Iran. The Data Communications Company of Iran (DCI), a subsidiary of TCI that manages Iran's public data network, implements some filtering orders and transmits the remaining list for filtering by ISPs.

Iranian Cyber Army (ICA)

The Iranian Cyber Army is an underground network of pro-government cyber activists, hackers and bloggers who monitor the Internet and launch cyber attacks on opposition and anti-Islamic websites. It operates under the Intelligence Unit of the Revolutionary Guard.

Cyber Police (FATA)

A division within Iran's police department established in January 2011 to combat Internet crimes and online social networks that spread anti-Islamic activities.

Telecommunications Company of Iran (TCI)

TCI manages Iran's ITC and telecommunications infrastructure, including mobile and Internet communications, directly or through its subsidiaries. TCI is owned by the Iranian government and Etamad-e-Mobin Company, a private consortium with reported ties to the Revolutionary Guard.

Data Communications Company of Iran (DCI)

DCI, a subsidiary of TCI, maintains Iran's data network infrastructure, and is responsible for implementing filtering and blocking orders from the CCDOC. All Internet Service Providers (ISPs) are required to purchase bandwidth from the DCI.

Internet Service Providers (ISPs)

ISPs must comply with the CCDOC's filtering and blocking orders, and are also required to filter any materials that contradict Islam, the Constitution, insult the Supreme Leader or other religious figures, or any content that "undermines the independence of the country," disrupts national unity, stirs "pessimism and hopelessness in people against the legitimacy and efficacy of the Islamic government," or promotes "illegal groups and parties."

Content-control software

ISPs are required to install content-control software that automatically inspects, filters, blocks web content and monitors IP traffic and Internet-user activities. These programs are configured to identify and filter websites based on keywords that are customized by Iranian ISPs and network administrators.

Deep-packet inspection (DPI)

Technology capable of monitoring and inspecting network traffic data in "real time" and determining whether content can pass through the network or be redirected, flagged, blocked, or reported to network administrators. China's ZTE Corp in 2010 sold TCI a DPI-based surveillance system capable of monitoring landline, mobile and Internet communications. It is unclear how extensively the DPI system is being used in Iran, beyond interfering with anti-filtering tools.

Circumvention

Iranian authorities estimate that 20 to 30 percent of the country's Internet users rely on circumvention tools to bypass state censorship, although such technologies are illegal. These tools vary in technological sophistication and in their capacities to allow users to browse the web undetected.

