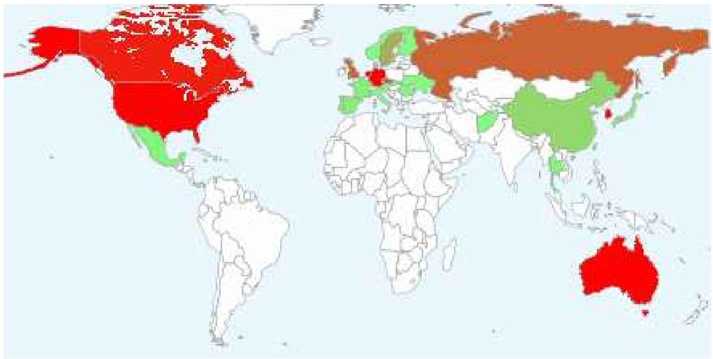
At-Large Summit Workgroup 5
DNS Security Issues within ICANN's Remit
Lawful access restrictions using DNS modifications

The Internet is not an unregulated space. Local and international law applies as usual. The everlasting new problem is, that the Internet is international in nature and designed to flatten every traditional hierarchy out there. That's why, several assumptions about lawful behavior need to be reconsidered.

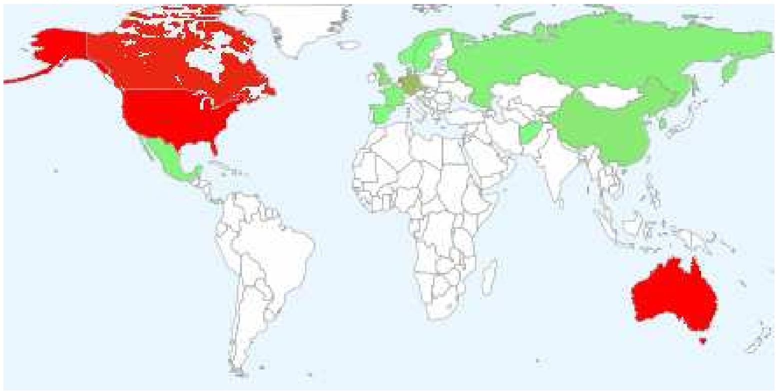
Criminal organisations do use every possibility to do their dirty activities. Of course they use the Internet. Law enforcement agencies had mastered the various communication channels in order to track the illegial activies and to bring those criminals into jail. That's the good news.



Several of the serious crimes which are perpetrated using the Internet deal with pictures. Politicans regulary come up with nauseous examples and rush into acting for the sake of acting. Unfortunly the law enforcement agencies are required to present something to "stop the crime".

Instead of fighting the criminals directly, most "solutions" simply aim to hide the crime from the innocent Internet user. The truth is as simple: Hiding is exactly what the criminals want to achieve. Serious crime does not depend on meetings by chance.

The righthand picture shows the geographical distribution of webservers containing illegal content. Almost all systems are located in lawful countries, where the police is able to catch the evil persons. Instead of follow the flow of money, investigate the felons who agonize innocent childs, and bring them together with their paying buyers into jail, all money and time is spent to prevent access to pictures, nobody would ever try to see. Because all parties know, that blocking access is not possible without taking the offering site down, they talk about lawful access restrictions and claim that 80% are enough.



The most common techniques to block accidental access are, transparent proxies, IP address blocking, and DNS manipulation. Expert reports show, that transparent proxies are costly, hard to set up, and a non-acceptable privacy intervention. IP address blocking is ineffective due to Fast Flux hosting and too broad, criminals try to misuse IP adresses of hosters which provide well known web sites. DNS manipulation seems to be smart: Only the required domains are blocked or redirected, the traffic is low, central resolvers can be modified by an preliminary injunction, it's hard to detect as long as DNSSEC is not deployed, and the criminals have no problem in using other domains or IP adresses.

In the consequence law enforcement agencies are required to act symbolic instead of catching the real criminals. Therefore a lot of illegal content stays on the same place for longer times. The lefthand graphic shows the geographical distribution of the same set of web sites a year after their first detection. All the missing sites were taken down, closed, or moved during this year.

Experience show that DNS manipulation is misused to block obnoxious, political inopportune, or unwanted web sites. Leaked lists contains 99% legal URLs, only about 1% of the entries point to real crime. The music industry as well as the patent guild is ready to add their claims, too.