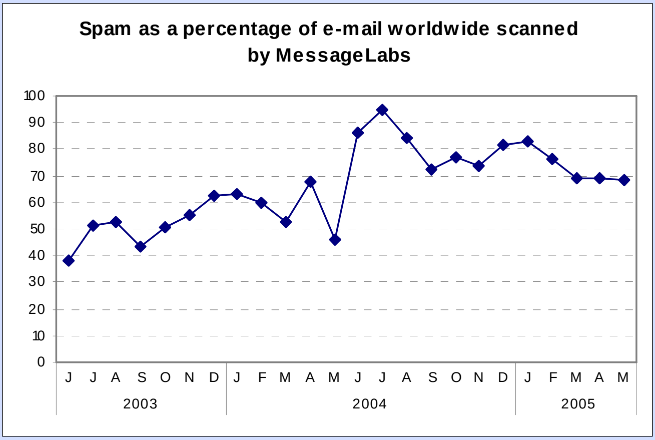
# 10 FIGHTING SPAM

Over the last decade, the unbridled growth of spam has gained increasing attention, not only due to its inconvenience and cost, but perhaps even more importantly, because spam often carries viruses and worms or poses other network security issues, or is used a vehicle for fraudulent behaviour. Today, there is general agreement about spam's core characteristics, including that it consists of unsolicited electronic messages sent in bulk. Spam messages tend to be identical and are sent indiscriminately to selected recipients. Most experts involved in the fight against spam counsel in favour of a multi-pronged approach, including technical solutions, legal and regulatory actions, end-user education and international cooperation.

**Figure 1.9 – Spam as Percentage of Emails Worldwide, 2003-05**

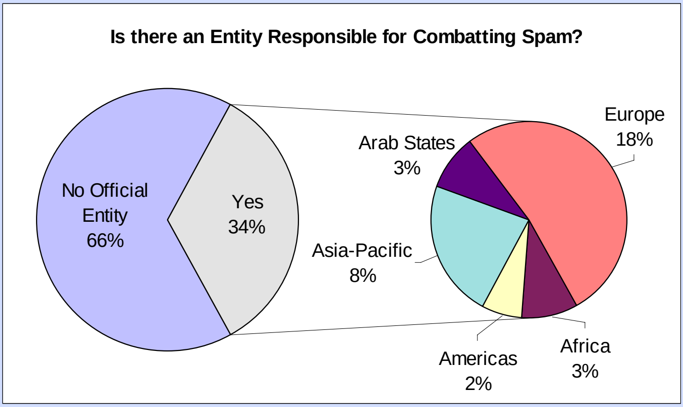


*Source*: MessageLabs.

According to some analysts, spam accounted for around 70 per cent of all e-mail traffic by mid-2005 (see Figure 1.9). The costs associated with spam are difficult to determine, although it is logical to assume that it puts pressure on ISPs in terms of reduced bandwidth and increased storage costs – not to mention the burden of dealing with customer complaints. In marked contrast, the costs of startup and operation for spammers are extremely low, and the architecture, based on Simple Mail Transfer Protocol (SMPT), allows them to work anonymously.

The success of legislating and making policies effective in countering spam has been limited thus far. In 66 per cent of all countries, there is no single, identifiable entity responsible for combating spam (see Figure 1.10). Only thirty-two countries have passed anti-spam legislation. As a region, Europe has the greatest focus on anti-spam measures, although international attempts at standardizing business practices – or at least harmonizing ISPs' approaches in countering spam – are growing.

**Figure 1.10 – Spam Regulation, 2005**



*Source*: ITU World Telecommunication Regulatory Database.

To date, anti-spam laws have focused mainly on tracking down and prosecuting spammers. Such anti-spam laws require considerable investigative and enforcement resources, the very resources that often are in short supply in developing countries. While anti-spam laws targeted at spammers remain an essential tool in the anti-spam arsenal, their use by developing countries may more likely be as the foundation for international cooperation. Anti-spam authorities with more experience and resources may seek to work with regulators in developing countries in tracking down and prosecuting spammers. Having an enforceable anti-spam law in place as part of a coordinated international effort will facilitate action against spammers acting (and hiding) across multiple jurisdictions.

But the time may also be ripe for anti-spam authorities to expand their efforts to include working with ISPs, who can be instrumental in fighting spam. Chapter 7 of this report therefore looks not only at the components of anti-spam laws targeted at spammers, but proposes the establishment of enforceable codes of conduct to be developed by ISPs, and then approved and enforced by regulators. Such a system of 'managed self-regulation' would require ISPs to prohibit their customers from using that ISP as a source for spamming and related bad acts, such as spoofing and phishing, and not to enter into peering arrangements with ISPs that do not uphold similar codes of conduct. Rather than continue to rely upon chasing individual spammers, regulators in the most resource-constrained countries in particular would be more likely to succeed by working with and through the ISPs that are closer to the source of the problem, to their customers, and to the technology in question. The regulator's job would be to ensure that ISPs within their jurisdiction adopt adequate codes of conduct and then to enforce adherence to those codes.

While some ISPs can be expected to resist even such light-handed regulation, the advantage is that it places all ISPs on a level playing field. Under current practices, responsible ISPs find themselves bearing the brunt of the costs of spam. This explains why some ISPs have begun suing spammers for damages, an option that may not be available in all jurisdictions. The goal of managed self-regulation is to reduce spam in a way that protects responsible ISPs. ISPs that implement responsible, effective anti-spam measures should be rewarded for their good behaviour. One means of rewarding those responsible ISPs is for regulators to hold their irresponsible competitors accountable. Regulators can also make consumers aware of the good works of the best ISPs, for example, by certifying ISPs that enforce their codes of conduct and allowing such ISPs to use the regulator certification in their advertising. As with many other telecommunication-related policy issue that is salient across national borders, the importance of consistency, shared strategic approaches and international cooperation is paramount.