Yes, voluntary codes of conduct can, and should, be used to encourage
ISPs, Users, and Government to better protect themselves. There are
ample benefits to engaging with a framework such as the Protected
Network, which can supply verified and formatted data to be used to
protect users on the Internet.

Awareness campaigns can be enhanced by being interfaced with the
Protected Network and essentially replacing bad links, with
educational information.

There are sources of botnet Command and Control server lists on the
Net. The golden aim of this function of the Protected Network is to
attempt to gain a list of ALL the Command and Control servers for a
Botnet, and then, but protecting users from those servers, rendering
an Botnet infection inert.

Botnets do cause a serious problem, but by and large, the infection is
started by users clicking on links that they shouldn't.

Public/Private Partnership is necessary to get this working, because
Government tend to get the information that is needed to fight these
threats, and have the seed funding to get it rolling.

Finding and Blocking access to Botnet Command and Control servers is
only the first step. Once they have been routed, those C&C servers
need to be repaired.

Users should be informed when they try and infect themselves. The
Protected Network handles this by preventing the infection in the
first place, and alerting users to the need for Anti-Virus software.

-- James :) Collins
The Protected Network
P.O. Box 1073,
Capalaba, Qld, 4157
http://www.protectednetwork.org/