Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

07-May-2012

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

## Working Party on Information Security and Privacy

# PROACTIVE POLICY MEASURES BY INTERNET SERVICE PROVIDERS AGAINST BOTNETS

JT03321193



DSTI/ICCP/REG(2011)11/FINAL Unclassified
English - Or. English

## FOREWORD

This report arises out of a proposal introduced by Australia on the role of Internet Service Providers (ISPs) in improving cybersecurity. It builds on prior work by the Working Party on Information Security and Privacy (WPISP) on malware, ISPs and botnets, as well as work by the Committee for Information, Computer and Communications Policy (ICCP) on Internet intermediaries.

It has been prepared for the WPISP by Aaron Martin, consultant to the OECD. It was declassified by the ICCP Committee in March 2012.

It is published under the responsibility of the Secretary-General of the OECD.

**TABLE OF CONTENTS**

## MAIN POINTS

Botnets are a threat to security and trust in online environments and their expansion would do considerable damage to online commerce, electronic government and other Internet-based services. Internet Service Providers (ISPs), by virtue of their ownership of the physical networks and customer-facing position, are well placed to respond proactively to botnets by communicating relevant information to users, working with customers to disinfect compromised machines and leading awareness-raising and educational campaigns.

This report analyses current proactive initiatives to mitigate botnets in Australia, Germany, Ireland, Japan, Korea, the Netherlands, the United Kingdom and the United States through which end-users are notified by ISPs when their computer is identified as being compromised by malicious software and encouraged to take action to mitigate the problem. The purpose of the report is to review the core dimensions of these programmes in order to identify the main challenges and provide high-level guidance on future policy development.

These initiatives are primarily private sector-led schemes and public-private partnerships. Anti-botnet measures are financially supported through government subsidies and industry funding. Funding covers programme start-up costs, the costs of investing in new preventive measures and the operating costs of notifying customers of infections and assisting them with disinfection. An outstanding policy challenge is sustaining funding for current and future anti-botnet initiatives.

Once an ISP has identified or been informed of an infected computer, it may take a number of different actions to resolve the problem, including forcing account password resets, disconnecting or quarantining an Internet connection, restricting certain forms of online communication, informing users about where to find tools to remove malware, directly providing users with these tools and offering support services for advanced problems or general queries.

These different activities embody varying degrees of intervention. They also differ in terms of costs and effectiveness. Deciding which practices to adopt requires a balancing of these different considerations. Policy responses to botnets must carefully consider the privacy of users whose machines may be infected and their right of access to the Internet, how to effectively communicate botnet-related notices to customers, the merits and challenges of cross-border co-operation and the need for robust metrics, among other policy challenges.

In addressing the botnet problem, OECD members should give consideration to implementing proactive initiatives like those described in this report. Although these iniatives are still in their infancy, some elements can already be identified as likely to contribute to their success. They have been brought together in a guidance section at the consclusion of the report and are summarised below in Box 1.

**Box 1. Summary of guidance on implementing proactive policy measures against botnets**

- **Work closely with industry and other stakeholders to develop and implement a policy.** There is a growing consensus that solutions to the problem of botnets involve internationally co-ordinated policy efforts that engage all stakeholders. As the owners and operators of the networks used by botnets, ISPs are well-positioned to understand the issues and to act on the botnet threat. ISPs, their users, and other stakeholders should be engaged from the outset in any policy development process.

- **Minimise unfunded mandates**, **share costs for policy development and implementation and seek ways of sustaining funding.** To maximise the effectiveness of anti-botnet policies, government agencies should contribute both to start-up and initial operational costs wherever possible and work with ISPs to find sustainable ways of covering the long-term operational costs.

- **Promote participation and transparency.** Where voluntary codes of practice are adopted to combat botnets, ISPs should be encouraged to publicly promote their participation in the programme. They should also be encouraged to demonstrate *how* they are achieving compliance with the code.

- **Establish minimum requirements but encourage extra effort.** At a minimum a code of conduct should include: *a)* a registration component, *b)* an awareness-raising component, *c)* guidance on network management; *d)* high-level advice on how to respond to threats and *e)* a reporting component.

- **Embed privacy protections into policies for botnet responses.** Anti-botnet measures may potentially infringe a person's privacy, depending on the applicable legal framework and factors such as how infected machines are identified. These risks can be reduced through the privacy-sensitive design of systems and organisational processes as well as appropriate supervision.

- **Devise mechanisms for trustworthy and verifiable communications during notification.** Policy makers and ISPs should consider how best to implement authentication mechanisms that facilitate trustworthy communications between ISPs, consumers and other actors.

- **Consider multi-channel notification measures, recognising the cost implications.** It is advisable to rely on multiple channels of communication to notify users about the presence of bots.

- **Design success and effectiveness metrics into policies.** The incorporation of good metrics into systems and enabling the reporting of measures to relevant authorities would be a useful step. Metrics should be internationally comparable to help participants identify best practices across borders and encourage other countries to promote such initiatives.

- **Focus on prevention – not just responding to infections *ex post facto*.** Working to educate users about how to protect themselves from installing malware and accidentally turning their computers into bots is a key element of a comprehensive approach.

- **Aim for global interoperability.** International co-operation amongst national governments, technical bodies and legislative institutions is crucial if the botnet threat is to be thwarted.

## Introduction

Botnets are networks of compromised computers that are remotely controlled by malicious agents (OECD, 2008a). They are used to send massive quantities of spam e-mail messages, co-ordinate distributed denial-of-service (DDOS) attacks and facilitate financial and identity fraud, among other economically and socially harmful activities. They therefore represent a major problem for security and trust in online environments. Their growth and increased severity would do considerable damage to online commerce, electronic government services and other Internet-based services, as consumers and citizens would become more reluctant to interact and transact online.

The 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Security Guidelines) advise that all participants in the networked economy share the responsibility of securing information systems and networks and are accountable in a manner appropriate to their individual role. Policy makers have since affirmed the importance of stakeholders taking shared responsibility. For example, the 2008 Seoul Declaration for the Future of the Internet Economy called for policies that reduce malicious activity online and reinforced national and international co-operation among all stakeholder communities, the 2008 OECD Recommendation on the Protection of Critical Information Infrastructures stressed the need for governments to work in partnership with the private sector and, more recently, the 2011 OECD Council Recommendation on Principles for Internet Policy Making encourages cross-stakeholder co-operation to promote Internet security. The recent Deauville G8 Declaration reiterated that the security of networks and online services is a multi-stakeholder issue requiring co-ordination amongst governments, regional and international organisations, the private sector, and civil society. In particular, the Declaration advised that "special attention must be paid to all forms of attacks against the integrity of infrastructure, networks and services, *including attacks caused by the proliferation of malware and the activities of botnets through the Internet*" (G8 2011, p. 6, emphasis added).

The problem of effectively responding to botnets has thus reached the global policy agenda. Moreover, the technological environment in which botnets are operating is changing fast. The continued widespread adoption of Internet-enabled devices, including mobile devices that are connected to the Internet, means that the already sizable security challenges facing network providers will only grow more complex in the future.

As with many pressing Internet policy issues, there is a growing consensus that solutions to this problem involve internationally co-ordinated policy efforts that engage all stakeholders. It is in this context that this study was proposed and carried out. In particular, this report focuses on the current and potential future activities of one kind of Internet intermediary, Internet Service Providers (ISPs), in proactively responding to botnets. In its recent work on the topic, the OECD defined Internet intermediaries as actors that "bring together or facilitate transactions between third parties on the Internet" (OECD, 2011b, p. 20). In exploring proactive measures against botnets, the current study distinguishes between ISPs and other intermediaries, such as online portals, search engines, hosting providers, and other web-based service providers. In this study ISPs are understood as the "Internet access providers that provide subscribers with a data connection allowing access to the Internet through physical transport infrastructure" (OECD, 2011b, p. 20). This encompasses more traditional service providers, as well as the mobile communications operators that are offering wireless Internet access.

The fact that the main focus of this report is the roles and responsibilities of these ISPs does not mean that other Internet intermediaries do not have important parts to play in this policy area. For example, search engines can help to raise consumer awareness about malware and botnets by displaying notices to users whose machines they suspect are infected.[1] However, studies have shown that ISPs have a unique

1. Google has recently begun to take this step. (BBC, 2011)

role to play in addressing and determining malicious activities and, if necessary, acting to eradicate threats (Van Eeten, *et al.*, 2010).

There are good reasons for ISPs to want to co-operate in botnet policy initiatives. A proactive approach to mitigating botnets can benefit ISPs in several ways, including allowing them to provide more secure services to customers, reducing costs associated with technical support and customer service, improving network performance through the management and reduction of compromised Internet connections and strengthening user confidence in ISPs that operate in an "enhanced security culture" (APEC, 2011).

This report therefore examines the proactive measures that ISPs in certain OECD member countries are taking, or may adopt in the future, to pre-empt and mitigate botnets. It also explores how governments can co-ordinate, support and enable these efforts. Key elements of these programmes often include: *i)* the identification of compromised computers; *ii)* the notification of end-users to help enable mitigation of the problems, *iii)* general awareness-raising and education; and, less frequently, *iv)* reporting. The analysis is based on a review of the current initiatives in Australia, Germany, Ireland, Japan, Korea, the Netherlands, the United Kingdom and the United States. The purpose of the report is to review the core dimensions of these current programmes in order to identify the main challenges and provide high-level guidance on future policy development.

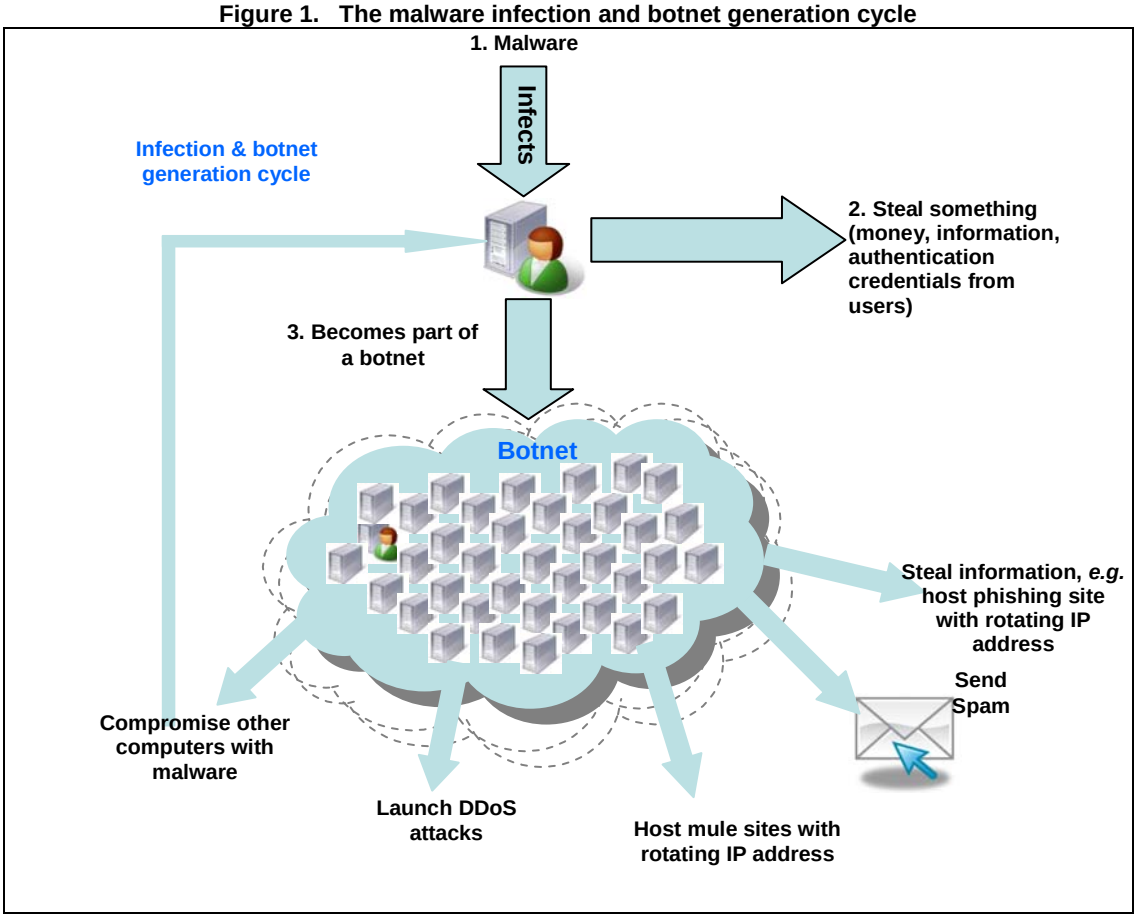
The analysis spans four main sections. It begins with background information on botnets, how they work, and their negative economic consequences. The next section analyses the major dimensions of anti-botnet initiatives. It is followed by a section that reviews the policy challenges that regulators face in developing frameworks for effective ISP intervention in botnets. The final section provides some guidance for policy making in this area that is derived from current approaches. Finally, brief profiles of each of the country initiatives under study are assembled in the Annex.

**Background information on botnets**

Botnets are networks of compromised computers ("bots", *i.e.* robots) connected through the Internet which are used for malicious purposes. These machines have been infected through a variety of techniques generally involving the installation of malicious software (known as malware[2]) that enable the orchestrator of the botnet ("bot master") to control them remotely. As mentioned above, botnets are created for different purposes, including propagating malware in order to grow the infected network, conducting Distributed Denial of Service (DDoS) attacks, distributing spam e-mail messages on massive scales and stealing personal and financial information from unsuspecting computer users. They have succeeded in propagating online due to the ease with which malicious agents can infect computers with malware. The development of botnets became common in the cybercrime underground because of the low costs involved in using them for committing attacks, the considerable profits that are gained by those operating these networks and the low probability that perpetrators will be severely sanctioned (ENISA, 2011, p. 5). There is even a market for buying, selling and renting botnets (OECD, 2008a, p. 23). Figure 1 depicts a typical botnet lifecycle.

2. "Malware is a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners." (OECD, 2009, p. 10)

**Figure 1. The malware infection and botnet generation cycle**




*Source:* OECD, 2008a, p. 23.

Botnets operate according to a command and control structure, with infected machines receiving orders from a remote bot master. To date, these architectures have typically resembled centralised models of control, with a botnet operator employing a main central server to send orders to networks of bots. Recently, however, peer-to-peer models have emerged. These more distributed networks make botnets more resilient to dismantling, as there is no longer a single node that can be taken out to disable the network. Botnet operators have also started masking their communications using web protocols to make their instructions to bots appear to be legitimate web traffic (OECD, 2008a, p. 24). These developments and other innovations have frustrated mitigation efforts.

A previous OECD analysis of malware spelled out the difficulties involved in quantifying the economic costs of malware and botnets but warned of erosion of trust and loss of confidence in the Internet economy if the botnet threat is not addressed (OECD, 2008a, p 7). The study also noted that existing responses and mitigation efforts are mainly reactive, and called for more structured and strategic co-ordination at both national and international levels to more adequately assess and mitigate risks. In particular, ISPs were identified as being well positioned to aid in this proactive strategy. First, their networks provide the conduit for much of the Internet's traffic. Second, due to their customer-facing position they are well-placed to provide information to users, raise awareness of information security issues and educate the public on how to better protect themselves online (*cf.* APEC, 2011, p. 2). Moreover, empirical studies have suggested that the networks of just 50 well-known established ISPs account for around half of all infected machines worldwide (van Eeten,*et al.*, 2010). Several countries have developed

strategies for botnet intervention and prevention. The next section reviews the main aspects of the initiatives in place in Australia, Germany, Ireland, Japan, Korea, the Netherlands, the United Kingdom and the United States.

**Analysing current approaches to tackling botnets**

The analysis is structured around important issues in the botnet policy space, rather than being presented on a country-by-country basis (country overviews can be found in the Annex). The focus in this section is on the similarities and differences in proactive anti-botnet policies and operations across the national policy contexts. The main dimensions of the analysis are the types of partnership in place, regulatory and participatory features, funding structures, response actions, legal implications, international co-operation, and measuring effectiveness.

***Types of partnership***

In theory, proactive policy measures against botnets could be classified as being primarily private sector initiated and organised (in which ISPs and industry groups lead the effort), government-led (with public sector bodies prescribing policy to providers), or a public-private blend. Only two types currently exist in practice: primarily private sector-led schemes and public-private partnerships.

For example, with the encouragement of the Dutch Telecom Regulatory Authority (OPTA), ISPs in the Netherlands have created a formal, private sector-managed alliance to address the country's botnet threat. Germany's anti-botnet effort is also led by the private sector, but with financial and technical support provided by the federal government.

The approaches taken by Australia, Ireland, Japan, and Korea all resemble a public-private blend, with government agencies working closely with ISPs to identify and mitigate botnets. Each of these countries has a dedicated department within the relevant government agency that co-ordinates efforts across ISPs.

In the United Kingdom, past efforts have been less formalised where ISPs have responded to botnets on an *ad hoc* basis. However, as noted in the Government's Cyber Security Strategy, published in November 2011, UK government departments, law enforcement and ISPs have laid the groundwork to form a public-private partnership in order to identify and mitigate botnet attacks, as well as identify the kinds of support that might be offered to Internet users.

The United States currently has a largely private sector-led response to botnets, in which ISPs combat bots and malware in the absence of government regulation. These efforts have included implementing notification systems for informing customers about infected machines (Comcast's 'Constant Guard' is one such example).[3] However, through a "Request for Information," the US government has recently expressed interest in advancing voluntary models for the detection, notification, prevention, and mitigation of botnets (U.S. DHS, *et al.*, 2011), recognising the seriousness of the threat from botnets.

***Forms of regulation and participation***

Across the countries analysed, strict top-down government regulations for ISP responses to botnets are absent. Incentives for responding to malware-infected computers and penalties for inaction are not codified in law. Instead, the regulatory forms that exist are codes of practice (typically written by

3. *http://security.comcast.net/constantguard/*

representatives from industry and trade bodies, often with support from relevant government agencies), self-regulatory covenants and best practice guidance.

In Australia and Germany, ISPs may sign a code of conduct pledging to participate in an initiative, although to do so is voluntary. In the Netherlands, participating ISPs sign a commitment to notify customers of compromised machines, isolate infected computers and share information with other providers, but no compliance mechanisms are in place. In the United Kingdom, the intention is for government, law enforcement and ISPs to co-design a series of guiding principles covering similar ground, to be adopted on a voluntary basis.

In the United States, the current policy guidance exists in the form of a 'best practice' document produced by the FCC-charted Communications Security, Reliability and Interoperability Council (CSRIC). Adoption of this guidance by ISPs is purely voluntary.

None of the countries analysed has yet mandated ISP participation in anti-botnet initiatives, although in most cases self-regulatory measures are widely adopted.

***Funding structures***

There are two main sources of funding for supporting botnet responses in the OECD countries with policies currently in place: government subsidies and industry funding. Funding covers different types of costs associated with anti-botnet measures, including start-up costs for setting up support centres, the costs of investing in new preventive measures (as malware techniques and botnets become more sophisticated) and the operating costs of notifying customers of infections and assisting them with disinfection.

In Germany, the Federal Ministry of the Interior currently pays for the technical support services provided to customers whose computers have been identified as infected. The Japanese government funds the Cyber Clean Center, which is the official organisation dedicated to assisting customers with infected machines. Likewise, Ireland's anti-botnet programme is funded by the government. There are no costs to ISPs that want to participate in Australia's *iCode* programme. The notification service is provided for free by the Australian Communications and Media Authority (ACMA), although providers will incur costs in communicating botnet-related information to their customers. The Korean government, through the Korea Communications Commission, provided funding to launch the country's programme.

As part of an industry-led programme, the ISPs that participate in the anti-botnet 'treaty' in the Netherlands are expected to fund their respective notification and disinfection activities. Likewise, under the current arrangements, US-based ISPs must cover the costs of their anti-botnet efforts.

One of the outstanding policy challenges is sustaining funding for current and future anti-botnet initiatives. Government funding allocated for initial start-up costs will ultimately dry up and there is a need to source funding for continuing anti-botnet efforts.

***Response actions: identification, notification, and mitigation***

A number of stakeholders are involved in anti-botnet initiatives and are responsible for different activities including detecting botnets, notifying customers about infected machines, and educating them about the risks of poor information security practices in order to prevent future incidents. ISPs feature centrally in all these activities.

*Identifying compromised computers* – Malware-infected machines or computers facilitating a botnet are detected in different ways across the world. Australian ISPs participating in the *iCode* initiative,

for example, largely rely on daily botnet reports from the Australian Internet Security Initiative, the sub-organisation within ACMA tasked with spotting botnets. ISPs in the Netherlands identify botnets using external detection systems and through data-sharing agreements with other providers in the country's anti-botnet alliance. Members of the German initiative use honeypots[4] and spam traps,[5] as well as information exchanged between ISPs. Japan's Cyber Clean Center and the KrCERT/CC in Korea also both use honeypots to detect botnets. Korea deploys additional techniques including DNS sinkholes,[6] malware analysis and an intruder detection system.

*Notification and mitigation* – Once the ISP has identified or been informed of an infected computer, it may take a number of different actions to resolve it. These different activities embody varying degrees of intervention. They also differ in terms of costs and effectiveness. Deciding which practices to adopt requires a balancing of these different considerations.

In Australia, providers may contact customers to inform them *a)* that their computer is compromised and the potential consequences of not addressing the situation; *b)* how to fix their machine (without directly providing them with the actual tools to do so); and *c)* how to prevent re-infection. Australian ISPs may reset a customer's password to force them to contact the helpdesk, where they may be informed of their malware problem. They are also allowed to temporarily quarantine an infected computer and/or restrict outbound e-mail messages (by blocking certain network ports).

Likewise, in the Netherlands ISPs have agreed to notify users about the problem and isolate their machines as necessary. The initiative in Germany involves notification and support through different channels, but does not permit blocking or quarantining users (a practice known as erecting a 'walled garden'). Disconnecting a user's Internet access, even temporarily, raises legal and commercial/cost-benefit challenges that will be addressed in the next section.

In Japan consumers are sent e-mails with information on their malware infection, including a URL directing them to a webpage with special cleansing tools. Japan's Cyber Clean Center programme also includes anti-virus software companies as participants, as does Korea's initiative, so that end-users are provided with tailored tools to effectively remove malware and other unwanted software from their computers. Korea also offers a 24-hour toll-free helpline for customers to call for technical support regarding an infection.

To summarise, the range of actions that ISPs may take to notify customers about an infection - with the aim of mitigating it – include:

- Contacting the user (through a variety of channels, including e-mail, phone, SMS, postal mail, or in a monthly billing statement)
- Password resets (to force a customer-initiated helpdesk call)

4 "A honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorised use of information systems." (OECD, 2008a, p. 59)

5 A spam trap is a honeypot used to collect spam. They are usually e-mail addresses created to lure spam (instead of for communication purposes).

6 A DNS (Domain Name System) sinkhole prevents infection by intercepting outbound DNS requests attempting to connect to known malicious domains, such as botnets, spyware and fake anti-virus software, instead returning a false IP address. (Bruneau, 2010)

- Disconnecting or quarantining an Internet connection, or restricting certain forms of communication (such as outbound e-mail)
- Informing users about where to find anti-virus software and other security tools online
- Directly providing users with the tools they need to disinfect their computers
- Offering support services for advanced problems or general queries regarding malware-infected machines.

*Consumer awareness and prevention*

Beyond these actions, botnet awareness-raising activities are a normal practice. All of the countries with current anti-botnet policy initiatives offer information (through websites) on the threats and risks of malware to their customers to raise awareness, with the overarching aim of stemming the spread of malware and preventing re-infection.

*Reporting*

Although not a common practice in the analysed countries, reporting on the effectiveness of specific anti-botnet measures represents an important dimension in current and future policy measures. Australia has a reporting mechanism in place for serious malware infections that present a risk to the critical national infrastructure or national security. Embedding reporting functions in anti-botnet policies and systems can assist ISPs and policy makers in better understanding what works and what does not.

**Policy challenges**

This section reviews the major policy challenges that ISPs and government policy makers are likely to face when developing proactive policies to address botnets. This list of challenges is not exhaustive, and might need to be updated on the basis of further experience with approaches that are still maturing and evolving. However, there are a number of issues that can already be identified as important success factors.

***Costs and funding***

The costs of designing, implementing and managing policies and systems for detecting and resolving botnets likely represent the biggest challenge to effective proactive measures. The more extensive the approach, the more costly it is likely to be. For example, deploying multiple communication channels for notifying end-users (*e.g.* e-mail, phone, postal mail) about an infected computer will impose additional costs on ISPs.

Where government bodies are able to cover these costs, anti-botnet policies may have a greater likelihood of success, but the reality of national budgetary constraints may mean that costs need to be at least partially assumed by ISPs. If ISPs are expected to fund these initiatives, then an additional challenge arises concerning the disparities in resources between large and small ISPs. Smaller ISPs that lack the financial means to pay for anti-botnet measures will be less likely to participate in voluntary programmes – a situation that may undermine an initiative's objectives.

Even where start-up funds are available to launch an anti-botnet initiative, finding sustainable funding sources remains a real concern. In Germany, for example, the anti-botnet programme was only provided with 18 months of initial government funding. It remains unclear where future funding for the

German scheme will come from. Such problems are likely to arise elsewhere as new programmes are launched and extended. Ireland's programme was able to minimise costs by building on the infrastructure that Germany already has in place. Rather than building a new system from scratch, Ireland contracted with Germany to provide an anti-botnet resource (including English language tools) targeted at Irish consumers on the pre-existing German platform.

***Regulatory implications***

There are important regulatory implications for anti-botnet initiatives that involve the interception of Internet traffic or processing of personal or identifiable information.

Similarly, collecting and sharing IP addresses of computers that are potentially operating in a botnet raises privacy and data protection concerns. In some countries, IP addresses are considered personal information and must be treated appropriately under privacy laws. Germany has recognised this concern and, as a result, obscures customers' IP addresses and other personal information as calls are processed in the Anti-Botnet Advisory Centre. Where multiple computers share the same IP address, additional information may be required to uniquely identify an infected device (such as a Media Access Control (MAC) address). Collecting and processing these identifiers increases the potential privacy risks of anti-botnet techniques.

Policy makers in the United States are currently considering what form of liability protections might be necessary for ISPs participating in a voluntary programme to address these types of concerns (Federal Register, 2011).

***Access rights***

ISPs may try to proactively block access to sites or services that are believed to be common vectors of botnet infection. If such blocking is not done transparently, the practice could be seen as censorship.

In order to avoid false positives, ISPs must understand how the use of privacy and anonymity services (*e.g.* Tor) may result in traffic patterns that are superficially similar to those of a botnet (EFF, 2011).

When it comes to ISPs disconnecting or quarantining infected computers, policy makers must consider the legal and ethical implications of removing Internet access, especially in light of recent statements from the United Nations linking Internet access to fundamental human rights (La Rue, 2011).

This situation becomes especially complicated when ISPs seek to act against repeat offenders. If a user repeatedly falls victim to malware, and his or her machine is recurrently participating in a botnet, providers may feel justified in severing their Internet connection. However, if the user is not disconnected in a careful and transparent manner then they may believe their access rights have been infringed upon and may seek legal redress.

***Trustworthy communications***

Another policy challenge involves fostering trustworthy channels to communicate with and assist users – especially those who are not technically savvy or are prone to naivety. Bad actors may try to take advantage of users by impersonating an ISP or support desk to deceive them into installing malicious software on otherwise 'normal' computers. For example, cold calls from individuals pretending to be an ISP, instructing customers to install malware disguised as anti-virus software, would be ruinous to anti-botnet measures. Likewise, cleverly disguised e-mails may lure customers into infecting their own

machines. The communication and notification components of anti-botnet policies therefore need to consider ways of authenticating calls, e-mails and other forms of communication from ISPs so that their claims can be verified and trusted.

***Consistency***

Along similar lines, policies should be designed to encourage consistent practices across ISPs within the same market. If ISPs do not employ similar methods for notifying users about an infection or cleaning a compromised machine, initiatives may prove less effective, as inconsistent practices may breed user confusion and/or distrust.

***Competition***

Policy makers who intend to devise or promote an anti-botnet initiative must also take into consideration how competition in the ISP market might complicate policy objectives. There are potential disincentives for ISPs to disconnect users whose computers are part of a botnet. ISPs may fear losing the customer's business to a competing provider. The disconnected user could simply change providers instead of going through the recommended (but potentially burdensome) steps for cleaning an infected machine. Related to this hypothetical scenario are questions about contract termination. If an ISP disconnects a user who has not responded to a notification regarding a botnet, is the user required to settle an outstanding bill?

***Policy coherence***

More broadly, policy makers should understand how anti-botnet policies potentially run counter to other Internet economy policies, such as those encouraging further broadband adoption and the uptake of electronic government services. This relates to the issue of access rights and the principle that citizens should be connected online and able to make use of public services.

***Cross-border co-operation***

Another major challenge involves the legal, organisational and technical barriers to facilitating cross-border co-operation on anti-botnet measures. First, botnets are rarely restricted to a single legal jurisdiction or market (as discussed above). As such, future national policies and initiatives will need to aspire to interoperate internationally. But such interoperability is by no means straightforward. For example, there will be legal issues (*i.e.* privacy concerns) that arise with the international transfer of IP addresses of machines suspected of being compromised by bots. Second, it is not obvious how botnet-related data will be transferred and by whom. Will national authorities be the main nodes for data transfers or will ISPs communicate directly with one another? These are issues that, to date, have not been settled by policy makers and private sector stakeholders. Third, reporting systems will probably need to be technically compatible if efficiencies are to be achieved and costs reduced. Ensuring this sort of technical interoperability will require considerable international co-operation on standards development.

***Measuring effectiveness***

It is difficult to discern the effectiveness of the anti-botnet initiatives that are already up and running. A better understanding of what works and what does not is needed. If ISP-level or national-level data do exist, then they should be shared with international partners so that lessons can be learned from these experiences.

It may be the case that these data are not readily available. There are certainly many challenges involved in measuring the effectiveness of policy interventions against botnets, but improved metrics would be very helpful in identifying best practices.

**Guidance for proactive policy measures by ISPs against botnets**

This section provides guidance in the formulation of policy responses involving ISPs to address the botnet problem. It is based on the findings from the analysis and reflections on these policy challenges, and draws on recent reports from the European Network and Information Security Agency (ENISA, 2011) and Asia-Pacific Economic Co-operation (APEC, 2011).

- **Work closely with industry and other stakeholders to develop and implement a policy.** As the owners and operators of networks, ISPs have an important role to play in addressing and deterring the botnet threat. Considering the nature of the botnet problem as well as the business environment, with ISPs owning and managing most of the physical networks through which attacks occur, it is understandable that heavily prescriptive, government-led responses have not emerged. ISPs should therefore be engaged from the outset in any policy development process, either directly or indirectly (through trade bodies and industry groups). Government bodies may need to lead the effort in certain circumstances or assume an active assisting role, but close collaboration with industry is essential. In markets in which a considerable number of small ISPs operate, it will be important to seek out their opinions to understand how the cost of complying with a proposal would impact on their business.

- **Minimise unfunded mandates**, **share costs for policy development and implementation and seek ways of sustaining funding.** To maximise the effectiveness of anti-botnet policies, government agencies should contribute both to start-up and initial operational costs wherever possible and work with ISPs to find sustainable ways of covering the long-term operational costs. Effective policies should result in lower rates of malware infection and botnets, which means that over time the costs for operating anti-botnet schemes should decrease.

- **Promote participation and transparency.** Where voluntary codes of practice are adopted to combat botnets, ISPs should be encouraged to publicly promote their participation in the programme. This can be done through the use of seals or trustmarks that identify which providers are participating (and, indirectly, who is not) and provide assurance that ISPs' commitments are met through appropriate audit mechanisms. Moreover, ISPs should be encouraged to demonstrate *how* they are achieving compliance with the code by being transparent regarding their detection, notification, mitigation and customer awareness practices.

- **Establish minimum requirements but encourage extra effort.** At a minimum a code of conduct should include: *a)* a registration component (in which ISPs formally commit to the programme); *b)* an awareness-raising component (so as to encourage the ISPs to be proactive and not simply reactive in their efforts); *c)* guidance on network management, *d)* high-level advice on how to respond to threats (*e.g.* whether and how to notify customers, remediation advice, etc.); and *e)* a reporting component (explaining what information ISPs should share with government agencies and the frequency of reporting).

- **Embed privacy protections into policies for botnet responses.** Anti-botnet measures may potentially infringe a person's privacy, depending on the applicable legal framework and factors such as how infected machines are identified (*e.g.*, through the use of 'deep packet inspection' technology) and with whom information such as a customer's IP address and account details is shared. Some of these privacy risks can be addressed through the privacy-sensitive design of systems and organisational processes as well as appropriate supervision.

- **Devise mechanisms for trustworthy and verifiable communications during notification.** The issue of how ISPs go about notifying consumers about potential bots is not trivial. Although most of the current evidence of fraudulent malware-related communications is anecdotal, there is a risk that malicious actors will abuse established consumer communication protocols. In order to prevent such abuse, policy makers and ISPs should consider how best to implement authentication mechanisms that facilitate trustworthy communications between ISPs, consumers and other actors. These mechanisms may leverage pre-established authentication and identity systems, where they exist, and should be privacy-sensitive.

- **Consider multi-channel notification measures, recognising the cost implications.** Notifying customers solely by e-mail that their computer is participating in a botnet may be inexpensive, but it may also result in high-levels of inaction, as these types of messages often go unread or may be treated as phishing attempts and thus viewed suspiciously. It is therefore advisable to rely on multiple channels of communication to notify users about the presence of bots. Using multiple channels to inform users will increase the likelihood that consumers are notified and that they subsequently act, but ISPs will likely incur additional costs in doing so.

- **Design success and effectiveness metrics into policies.** One of the major limitations of current anti-botnet initiatives is that little is understood about the success rates of interventions and the effectiveness of different ISP activities. There is a lack of evidence, for example, regarding what measures are most effective in terms of establishing contact with consumers, getting them to resolve the problem, and preventing re-infection. The incorporation of good metrics into systems and enabling the reporting of these measures to relevant authorities would be a useful step. Metrics should be internationally comparable to help participants identify best practices across borders and encourage other countries to promote such initiatives.

- **Focus on prevention – not just responding to infections *ex post facto*.** Working to educate users about how to protect themselves from installing malware and accidentally turning their computers into bots is a key element of a comprehensive approach. While most current initiatives have websites dedicated to explaining the risks of poor information security practices and providing users with tips on how to use their computers securely, much more can be done to promote consumer awareness.

- **Aim for global interoperability.** International co-operation amongst national governments, technical bodies and industry associations is crucial if the botnet threat is to be thwarted. Interoperability is needed at the policy level, where national policies should promote compatible anti-botnet measures and best practices. It is also needed at the technical level, to ensure that systems are capable of communicating and exchanging information with each other regarding incidents and identified threats, as well as means for maintaining the confidentiality of shared information as it is shared between national authorities and ISPs based in different jurisdictions.

## Conclusion

Proactive measures engaging ISPs, consumers and governments are a promising avenue to counter botnets. While the countries studied have encouraged ISP participation in co-ordinated responses to incidents, these initiatives are still in their infancy and there is a need for further experience in this area of policy development. For example, a key consideration is the assessment of the effectiveness of these initiatives which is essential for fine-tuning existing measures and for engaging other countries in similar approaches, especially as anti-botnet policies and programmes are now emerging in other countries (such as Spain and Sweden).

Further work is needed to better understand what policy framework can ensure that consumers' privacy and access rights are protected when infected machines are identified and disconnected. Finally, policy makers should explore how to address limitations of purely national approaches considering the global character of the botnet problem, including how to facilitate cross-border co-operation during botnet mitigation.

## BIBLIOGRAPHY

APEC (Asia-Pacific Economic Co-operation) (2011), APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice, APEC Telecommunications and Information Working Group, *http://publications.apec.org/publication-detail.php?pub_id=1269,* accessed 7 May 2012

BBC News (2011), "Google to warn PC virus victims via search site", British Broadcasting Corporation, *www.bbc.co.uk/news/technology-14232577,* accessed 4 November 2011.

Bruneau, G. (2010), *DNS Sinkhole,* SANS Institute.

EFF (2011), Comments of Electronic Frontier Foundation In the Matter of Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware, National Institute of Stanards and Technology, *http://www.nist.gov/itl/upload/EFF-Comments-to-BotNet-RFI_11-4-11.pdf,* accessed 22 January 2012.

ENISA (European Network and Information Security Agency) (2011), *Botnets: Measurement, Detection, Disinfection and Defence.*

G8 (Group of Eight) (2011), *Deauville G8 Declaration: Renewed Commitment for Freedom and Democracy,* Deauville, France.

Hustinx, P. (2011), *Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data*, European Data Protection Supervisor, Brussels.

ITU (International Telecommunication Union) (2008), *Study on the Financial Aspects of Network Security: Malware and Spam*, Geneva.

La Rue, F. (2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* United Nations Human Rights Council, New York.

OECD (2002), *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security,* OECD, Paris.

OECD (2008a), *Malicious Software (Malware): A Security Threat to the Internet Economy,* OECD, Paris.

OECD (2008b), *Recommendation of the Council on the Protection of Critical Information Infrastructures,* OECD, Paris.

OECD (2008c), *Seoul Declaration for the Future of the Internet Economy,* OECD, Paris.

OECD (2009), *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*, OECD, Paris.

OECD (2011a), *Recommendation of the Council on Principles for Internet Policy Making*, OECD, Paris.

OECD (2011b), *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, OECD, Paris.

PTS (2009), *Botnets: Hijacked Computers in Sweden*, National Post and Telecom Agency, Stockholm.

U.S. DHS (Department of Homeland Security), the National Institute of Standards and Technology, and the National Telecommunications and Information Administration (2011), "Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware", US Government, *www.federalregister.gov/articles/2011/09/21/2011-24180/models-to-advance-voluntary-corporate-notification-to-consumers-regarding-the-illicit-use-of* , accessed 4 November 2011.

Van Eeten, M. *et al.* (2010), "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data", OECD Science, Technology and Industry Working Papers, 2010/05, OECD Publishing. *http://dx.doi.org/10.1787/5km4k7m9n3vj-en.*

## ANNEX: COUNTRY PROFILES

This annex includes brief country profiles. Each profile provides an overview of the country's anti-botnet policy and includes a breakdown that captures: *a)* the main actors in the botnet response; *b)* the information flows in the network; *c)* what actions and decisions are typically taken and by whom; and *d)* any other relevant information.

### Australia

*Name of initiative*: Internet Industry Code of Practice (*iCode*).

*Type of partnership*: Voluntary code of practice with minimum standards for consumer education, botnet detection, and consumer notification and assistance.

*Main actors involved in the botnet policy design*: Australian Internet Industry Association (AIIA) in conjunction with the Broadband, Communications and the Digital Economy Department (DBCDE) and the Attorney General.

*Typical information sharing process in the botnet response*: Compromised computers may be identified by a number of different actors, including the Australian Internet Security Initiative (AISI) (which issues daily reports to ISPs detailing IP addresses on their networks that have been reported in the previous 24 hours, a timestamp and the type of suspected infection). ISPs may also identify compromised computers through their own network management practices, or based on information from trusted third parties such as CERT Australia.

*Typical actions taken to engage customers*: With this information, ISPs are expected to contact their customers to advise them that their computer appears to be infected, and to provide them with information to assist them in addressing the problem. ISPs may also intervene by temporarily quarantining the customer's service or restricting outbound e-mail.

### Germany

*Name of initiative*: German Anti-Botnet Initiative.

*Type of partnership*: Private sector initiative with support provided by the government.

*Main actors involved in the botnet policy design*: This initiative is led by *eco*, the association of the German Internet Industry, and is backed financially by the Germany's Ministry of the Interior (BMI). This funding mostly goes to operating the customer assistance service. The Federal Office for Information Security (BSI) provides technical support.

*Typical information sharing process in the botnet response*: Infected machines are identified through the use of spam traps and honeypots, which are operated by the respective ISPs. Providers also exchange information amongst one another about suspected botnets. Once an infected computer is identified, providers inform customers whose computers are responsible. These users are referred to a central help

service (the Anti-Botnet Advisory Centre), which provides information on personal computer security and offers software tools for removing malware.

*Typical actions taken to engage customers*: Customers who are unsuccessful using these tools to recover their computer may then contact their ISP for further assistance. Providers may then refer their customers to an inter-provider-operated call center specialising in malware removal. This referral is handled in a privacy-sensitive manner using pseudonyms and obscured IP address information. These calls can be escalated for additional assistance if customers continue to face problems.

Notably, ISPs participating in this initiative do not quarantine or disconnect the infected computers of end-users.

**Ireland**

*Name of initiative*: Irish Anti-Botnet Initiative.

*Type of partnership*: Government-led initiative, building on Germany's infrastructure, with close co-operation from ISPs.

*Main actors involved in the botnet policy design*: Department of Communications, Energy and Natural Resources in association with the Commission for Communications Regulation (ComReg), with technical assistance provided by the German Federal Office for Information Security (BSI).

*Typical information sharing process in the botnet response*: The Irish Reporting and Information Security Service (IRISS-CERT) identifies a computer infected with malware or participating in a botnet, after which it contacts the relevant ISP to act.

*Typical actions taken to engage customers*: Once notified by the CERT, ISPs contact end-users through a variety of channels to inform them of the compromised machine. Customers are directed to the Irish Anti-Botnet Initiative website to download cleansing tools. In the case of severe malware infection that is not easily resolved by the tools, users may request to be contacted (*i.e.* a call-back service) by the Irish Anti-Botnet Advisory Centre, which is based in the CERT.

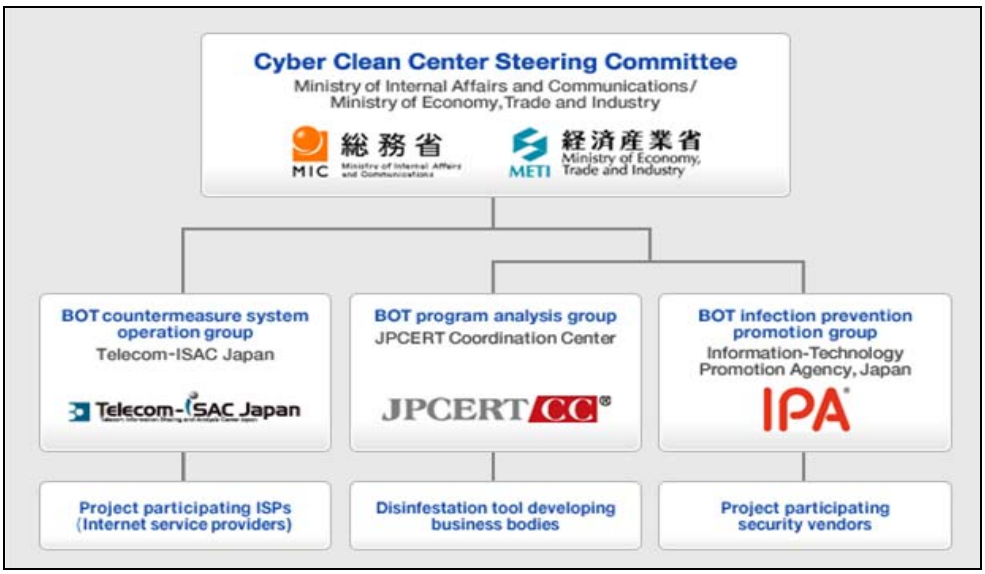
**Japan**

*Name of initiative*: Cyber Clean Center (CCC).

*Type of arrangement*: Government-led initiative with voluntary ISP participation, as well as the involvement of anti-virus and security software vendors.

*Main actors involved in the botnet policy design*: The Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade, and Industry (METI) formed a Steering Committee for the initiative, with three working parties providing technical support: Telcom ISAC (Information Sharing and Analysis Center), the Japanese Computer Emergency Response Team (JP-CERT) Co-ordination Center, and Information Technology Promotion Agency.

**Figure 2: CCC's organisational structure**

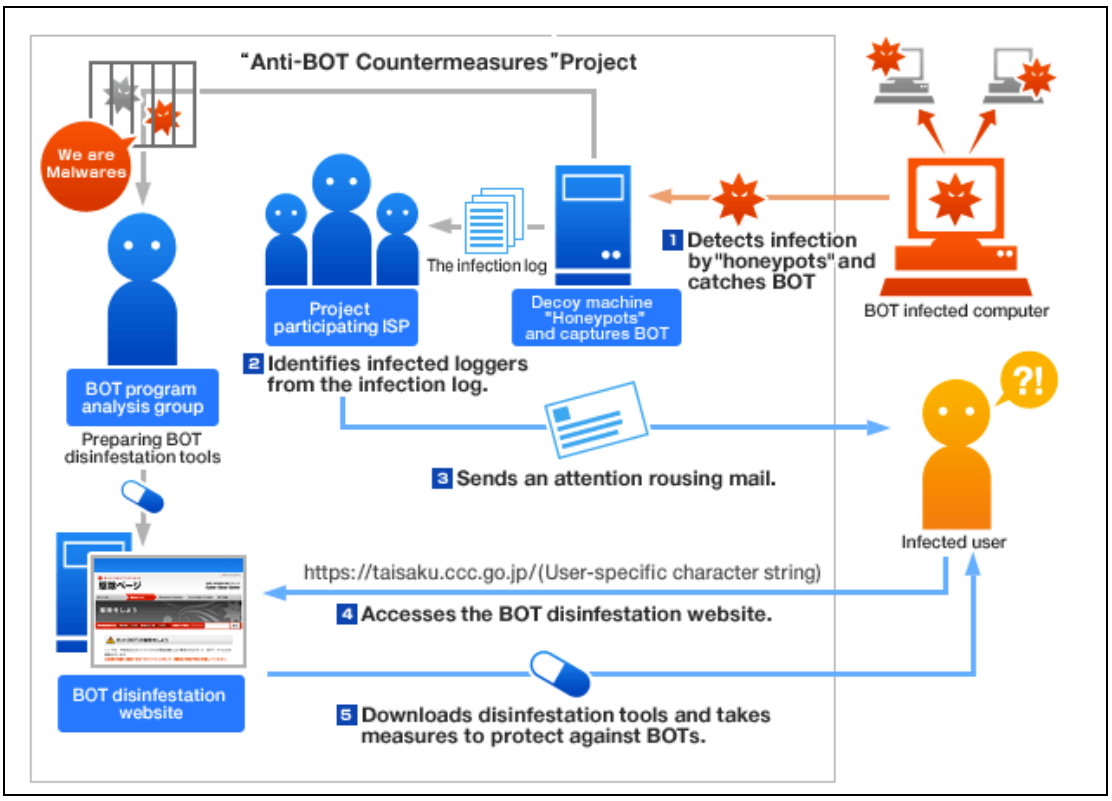



*Source:* Cyber Clean Center, *https://www.ccc.go.jp/en_activity/index.html*

*Typical information sharing process in the botnet response*: Botnets are typically detected through the use of honeypots, which the CCC then analyses to identify the source of the infection. The Center then communicates the IP address and timestamp of a compromised machine to the participating ISP.

*Typical actions taken to engage customers*: Based on this information, the ISP may identify the customer and contact them by e-mail, directing them to a CCC-sponsored webpage dedicated to botnet disinfection. Users may visit the site and download a tool to clean their computer. However, the initiative is set up such that the ISP may handle the disinfection process according to its own procedures. There are no strict rules specifying how ISPs should contact users and manage the process of eliminating bots.

**Figure 3: Japan's botnet response**




*Source:* Cyber Clean Center, *https://www.ccc.go.jp/en_activity/index.html*

**Korea**

*Name of initiative*: KrCERT/CC Anti-Botnet Initiative.

*Type of partnership*: Public-private initiative with co-operation from ISPs and anti-virus software vendors.

*Main actors involved in the botnet policy design*: Korean Internet Security Center, which is a part of the Korea Internet Security Agency (KISA).

*Typical information sharing process in the botnet response*: To detect botnets, KrCERT/CC (acting as a trusted clearinghouse for malware) sets up honeypots and analyses the logs of infected machines. Mitigation techniques include the use of DNS sinkholes. KrCERT/CC then informs ISPs of the IP addresses associated with affected computers.

*Typical actions taken to engage customers*: ISPs are expected to reach out to end-users to inform them of the malware on their computer and how to remove it. Anti-virus software companies provide free tools to assist in this effort. KISA also runs a toll-free, 24-hour response service ('118') with trained operators, who help customers repair compromised machines. KISA also allows users to forward spam to its team, which it then investigates.

**Netherlands**

*Name of initiative*: Dutch Anti-Botnet Initiative.

*Type of partnership*: Private sector-led alliance based on a regulatory covenant.

*Main actors involved in the botnet policy design*: The Dutch Telecom Regulatory Authority (OPTA) instigated the alliance, which is comprised of 15 ISPs that share over 90% of the market. The agreement expresses the participating ISPs' commitment to sharing information about infected systems, isolating infected machines, and notifying customers, although it does not prescribe *how* these aims should be achieved.

*Typical information sharing process in the botnet response*: This depends on the ISP.

*Typical actions taken to engage customers*: Again, this depends on the ISP.

**United States**

*Name of initiative*: No formal initiative exists at present, although the US government is currently seeking opinions on the establishment of a voluntarily, industry-wide initiative.

*Type of partnership*: Likely to be initiated by government but managed and operated by the private sector.

*Main actors involved in the botnet policy design*: Department of Commerce (including the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA)) and the Department of Homeland Security (DHS).

*Typical information sharing process in the botnet response*: Under consideration.

*Typical actions taken to engage customers*: Under consideration.

**United Kingdom**

*Name of initiative:* Not yet formally named but referred to as the Government-ISP partnership to co-design guiding principles.

*Type of partnership:* Partnership between relevant government departments, law enforcement and the five main ISPs in the United Kingdom to co-develop a series of guiding principles to be adopted and adhered to on a voluntary basis.

*Main actors involved in the botnet policy design*: Department for Business, Innovation, and Skills (BIS), Home Office, Serious Organised Crime Agency (SOCA), Cyber Security Operations Centre, Internet Service Providers Association (ISPA), and selected ISPs in the United Kingdom.

*Typical information sharing process in the botnet response*: Under consideration.

*Typical actions taken to engage customers*: Under consideration.