Internet Governance Forum

Best Practice Forum on the Regulation and Mitigation of Unsolicited Communications (2015)

Executive Summary

The 2015 Best Practice Forum (BPF) on the Regulation and Mitigation of Unsolicited Communications built on the work undertaken in 2014. For the purposes of this BPF, the terms unsolicited communications and spam are analogous, referring to all (written) unsolicited communications (that are carried on the Internet), including, and not limited to, messages that spread malware or have other nefarious purposes[1].

This year the BPF has focussed on two main, overarching streams:

1) Statistical and numerical data scaling the problem, and current examples of multi-stakeholder cooperation that attempt to resolve the problem and;

2) The future of unsolicited communications. The next billion coming online: Challenges for the developing world.

The 2015 BPF makes use of established practices providing examples of where they have been successful so that others are encouraged to consider what may work in their own environments.

Major Findings

This BPF found that despite unsolicited communications being a global issue, accurate quantification is a significant hurdle. No single data-set can measure the scope and scale of the problem, and the cost impact on economies for both industry and government. Statistics reflecting the impact of cybercrime were also difficult to source. In spite of these difficulties, this report presents the best statistical information available. Indeed, the statistics presented in this report show that there has been a recent downward trend in spam volumes. It is not yet known what the reasons for this are and whether the trend will continue. This BPF has a consensus view that more research is needed in order to develop more reliable and robust metrics.

This BPF has the view that the problems that are likely to be encountered by the next billion coming online are most likely very similar to those that have come before. Spam, infections, malware and cybercrime will invariably be prevalent, perhaps more so in developing nations, as measures that have been developed over time to address such issues may not be implemented prior to the broader deployment of broadband connectivity.

This BPF wanted to learn more about the needs and wants of those coming newly online and so solicited input from developing nations, working closely with IGF Africa. Capacity building and training have been flagged as a particular need. In order to give more focus to this issue the BPF organised a matchmaking session on “Day zero” of the IGF, an experiment that added to the work in a significant way. The session discussed many of the issues that have been highlighted in the BPF report and detected a willingness from many to collaborate in moving these issues forward. Some felt strongly that it is important for trainers to travel to the people who need training. Organisational and funding discussions could focus on how this can be put into practice.

[1] For this reason the addition “(e.g. “spam”)” is taken out of the title of this BPF.

This BPF has received several case studies, including visionary views, academic research, successful solutions, public-private and private-private partnerships. These case studies can be learned from and where appropriate replicated or adapted. They are contained in the annexes to this BPF's report. The case studies demonstrate that a shared idea, need or vision can lead to cooperation and solutions that make the Internet safer.

Suggestions for future work

This BPF considers its work completed and advises to stop work on, "unsolicited communications". In general, this work was found to be valuable and it was acknowledged that in order to facilitate the implementation of the recommendations, there would be a need for a regular 'check-in' or review.

As unsolicited communications are only one aspect of the many issues relating to the protection of infrastructure and citizens online, there would be more value for any future work within an expanded remit that encompasses broader cybersecurity and cyber safety issues.

The suggestions for future work relate to the IGF and include considerations for the immediate follow-up to this BPF as well as possible themes for the future work for the IGF. The report also includes more general recommendations addressed to the broader community.

1. Follow-up to this BPF

This BPF identified the need for future work in the broader cybersecurity and cyber safety areas. One way forward to continue work in a meaningful way could be to form a Dynamic Coalition. As there are overlapping issues concerning cybersecurity and network abuse with the work carried out by the BPF on CSIRTs, one option could be to involve experts who worked in both of these BPFs. Preliminary discussions focused on the theme "preventing network abuse". Questions that could be addressed include the following: how to reduce abuse; implement best practices and improve the overall security of the Internet.

2. Themes to be taken up by the IGF

In order to avoid duplication of efforts, any future work the IGF undertakes needs to take into consideration ongoing work in other organizations and fora, such as FIRST, M^{3}AAWG, and the ITU. The IGF can add value by linking up stakeholder communities and foster discussion and cooperation with a view to implementing outcomes. The themes proposed for future work could be taken up as workshops, main sessions, new BPFs, dynamic coalitions or other new initiatives.

The following themes are offered to the broader IGF community for consideration:

a. The implementation of Internet standards and best practices

Cyber security is achieved through a combination of factors: the implementation of standards and (maintenance of) best practices; end users' use of cyber sanitation measures; governmental interventions, for example, awareness programs; safer ICT products (throughout the whole production chain); etc. No single actor can influence a safer Internet environment on his own as there is a strong interdependency. By focusing work on the need of implementation of standards and best practices, different stakeholder groups can be brought together and discuss the hurdles that prevent the implementation of Internet standards and best practices.

b. Developing reliable metrics

There is a need for further work to pin down a set of reliable metrics that relate not only to spam, but broader cybersecurity issues.

c. Cybercrime and cyber security incidents reporting and statistics

This BPF has shown that it is not common for citizens to report cybercrimes or cyber security incidents. In addition, when cybercrimes are reported they may not be categorised as such, making reporting and developing strategies for dealing with systemic issues difficult. Experts consider that it is important that reporting becomes the norm in order to classify, measure and start preventive as well as investigative actions. A next step could be to bring the involved stakeholders together and discuss potential ways forward so that priorities can be set and scaled.

d. Basic cyber security training in developing countries

There was a consensus on the need for basic cyber security capacity building within an expanded remit that encompasses broader cybersecurity and cyber safety issues for network and anti-abuse administrators in developing countries. Experience shows that it is best to bring the trainers to the places where the potential trainees are. This report identifies the first steps, including willing actors, towards these capacity building efforts. The IGF could assist by bringing the right people together and thus facilitate the organisation and funding of cyber security workshops in developing countries.

General recommendations

The general recommendations cover many topics including, but not limited to, training, education, the value of botnet mitigation centres, cybercrime reporting, the desirability of further region-specific surveys and the benefits of multistakeholder arrangements both public-private and private-private (examples of which, as mentioned above, are annexed to the BPF's report). The recommendations were, generally speaking, well received and many have been nuanced in response to the productive and candid discussions that resulted.

Recommendation 1: That newly connected economies consider multistakeholder anti-botnet efforts (botnet mitigation centers) as they have a role in reducing the number of infections on end users' devices.

Recommendation 2: That effort be taken by law enforcement to categorise crimes undertaken using the Internet.

Recommendation 3: That governments and law enforcement take proactive steps to encourage the reporting of cybercrime by all users: citizens and industry.

Recommendation 4: That further attention ought to be given to surveying the needs of African nations (and other developing nations), not only in dealing with the problem of spam, but the broader issues of cybersecurity and cyber safety.

Recommendation 5: That there is a need for basic cybersecurity training, including in relation to the mitigation of unsolicited communications, in the African region and perhaps other regions of the globe. Active participation from other regions is recommended. An example could be to organise workshops at the African Internet Summit.

Recommendation 6: That there is a need for education of citizens, including children, on matters relating to cybersecurity in economies coming newly online.

Recommendation 7: That industries affected by spam, phishing, etcetera must continue to evolve in order to protect their own reputations and to ensure that their own customers do not become victims; including the provision of funding for education programs.

Recommendation 8: That further consideration ought to be given to producing simple lists of low or no cost initiatives that can assist newly-connected economies to protect their infrastructure.

Recommendation 9: That consideration ought to be given by newly connected economies to a wide variety of multi-stakeholder arrangements, including public-private and private-private initiatives in combating unsolicited communications.

Report

Background

In 2014 this BPF carried out extensive work that identified 16 challenges and 11 recommendations[2] for future work, that were presented in the Internet Governance Forum's secretariat's report, published on its website in 2014[3]. In 2015, the Multistakeholder Advisory Group (MAG) decided that the Best Practice Forum on 'Regulation and mitigation of unsolicited communications (e.g. "spam")' was to continue its work based on the identified challenges and recommendations. This has led to two main, overarching streams from which recommendations have emerged.

1) Statistical and numerical data scaling the problem, and current examples of multi-stakeholder cooperation that attempt to resolve the problem and;

2) The future of unsolicited communications. The next billion coming on line: Challenges for the developing world.

For the purposes of this report, the terms unsolicited communications and spam are analogous. In this context unsolicited communications is a broad term that encompasses all (written[4]) unsolicited communications (that are carried on the Internet), including, and not limited to, messages that spread malware or have other nefarious purposes.

It is not the intention of this BPF to provide a new set of best practices that must be followed. Rather this BPF aims, mainly through the collection of case studies, to provide examples of where best practices have been successful so that others are encouraged to consider what may work in their own environments.

The BPF would like to take this opportunity to thank the many individuals who dedicated their time and knowledge by providing case studies to be included in this report. It should be noted that the case studies are contributions made by individuals and are not to be considered as representations of the opinions of the BPF group or its experts.

Defining the Problem: Spam is a Global Issue

What do the statistics say?

Despite spam being a global issue, accurate quantification is a significant hurdle. No single data-set can measure the scope and scale of the problem, and the cost impact on economies for both industry and government. Statistical data about spam has several shortcomings. This is especially so as the volume and type of spam received by a given network will differ significantly. For example, a commercial freemail provider such as Hotmail receives vastly more spam per user, and of an entirely different type than a corporate, an educational or government email system.

Further while volume is undeniably a good metric, a spear-phish spam campaign (defined below), for example, of tiny volume may have a more significant impact on an organization than a voluminous spam campaign with a replica brand goods payload. This therefore makes it difficult for the uninitiated to recognize and treat appropriately all the risks that are present.

[2] See Annex 1 for an overview of the recommendations of 2014

[3] http://www.intgovforum.org/cms/documents/best-practice-forums/regulation-and-mitigation-of-unwanted-communications/411-bpf-2014-outcome-document-regulation-and-mitigation-of-unsolicited-communications-spam/file

[4] For the purpose of this report, unsolicited voice communications are excluded. This is because, although this is an emerging issue, some of the treatments and symptoms are quite distinct.

The BPF has been able to obtain some reasonably current high level statistics about Internet abuse, that were presented at the Microsoft Digital Crimes Consortium conference in February 2015 by the EUROPOL Deputy Director of Operations. That is, there are:

- 116 billion emails sent each day;
- More than 90% of those emails are spam, totalling 103, 500, 000, 000 spam emails per day;
- 7 billion devices online;
- Estimated to be 24 billion devices connected by 2012 (12 billion mobile devices);
- 123 million unique malicious objects identified online;
- 307 new unique cyber threats coming online every minute;
- Estimated $445 billion USD cost of spam per annum, accounting for 1% of the global BBP.

While the majority of unsolicited commercial messaging is sent by way of botnets[5], the majority of spam that arrives in user in-boxes - at least in Internet mature economies - is not botnet generated. This is because stakeholders in those economies have taken steps to block the spam before it gets to users[6]. Up until 2012 or thereabouts, most botnet activity took place on individual and home-users' computers. However, in part, due to multilateral anti-botnet efforts in the United States (ABCs for ISPs), Germany (Botfrei), Japan and elsewhere, this vector has been remediated to a certain degree. However, significant botnet activity has subsequently emerged from commercial hosting companies, providing miscreants with better reliability and connectivity, usually through compromised user accounts and CMS (content management systems) compromises.

However as of the publication date of this report, levels of spam are down significantly over the last two quarters and certain botnets appear not to be operating or are sending spam at much lower levels. Experts are unable to determine the reason for this and this may well be a temporary respite[7].

It is true, the vast majority of the bots have disappeared and hence the incredibly high volume/low return per instance spam has declined. Some of these are undoubtedly due to the bot masters (owners) getting identified and in some cases investigated and prosecuted.

Some of this is due to the low-end users (who rent the botnets aka script kiddies) moving to more lucrative, less risky stuff like executive spoofing, Pump & Dump (stock-price kiting), extortion and outright data theft both in bulk and individually.

[5] The M^{3}AAWG report 'Bot Metrics Report, Report #1' (2014) gives the following description of a bot and botnets: *"While definitions of bots can differ from country to country, the metrics below report on malware, or malicious code, discovered by a network operator while processing a subscriber's email or other Internet activities. Bots are installed directly on end-users' systems, often without their knowledge. Once deployed, the "botted" machine can be controlled by commands from a "bot master," a person who uses infected machines as a network to send spam or carry out fraudulent activities. The malicious code is often designed to run in background mode, so subscribers are usually unaware their systems are infected".*

[6] https://www.signal-spam.fr/sites/default/files/BAROMETRE_7_signal_spam.pdf. Spambot related spam reported to Signal Spam represents in average 7% of cybercrime related spam which itself represents 27.15% of the total spam reports. This is confirmed when analysing which networks are at the origin of emails, mostly hosting providers, way ahead of Internet access providers. This certainly means that most botnet related spam is filtered inside ISP networks before arriving in mailboxes, but this example shows an issue of point of view when measuring spam.

[7] http://www.cbc.ca/news/technology/spam-email-down-below-50-1st-time-in-a-decade-1.3156850

We also do know that massive volume bots (for example, Kelihos[8] *and Cutwail) are still lurking around and make themselves known frequently enough at far lower volumes than we know their capabilities are. Kelihos still has close to a million bots (infected nodes) in total. Lethic is still present too.*

As such, the CBL/Spamhaus infectivity graphs are more important than ever, but the importance has shifted a bit more towards criminality other than just spam. I'd caution against anyone to think, "it's over" just because it's died down. We've seen dips like this before. The capabilities/resources still exist, we need only an incentive for a few actors to raise volumes higher than we've ever seen before.

- Chris Lewis, Chief Scientist, Spamhaus Technology

Statistics relating to phishing, or spear-phishing, where senders attempt to fool email recipients into handing over their credentials because they believe the email came from a genuine source (for example, a bank) shed insight on the nature of the problem. A report of a U.S. based research institution[9] claims that phishing attacks cost an average U.S. company up to $ 3.7 million per year. The Anti-Phishing Working Group (APWG) publishes a quarterly report on phishing. It describes phishing as: *"A criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials"*[10]. The most recent report at the time of writing is from the fourth quarter of 2014. It provides the following data[11]:

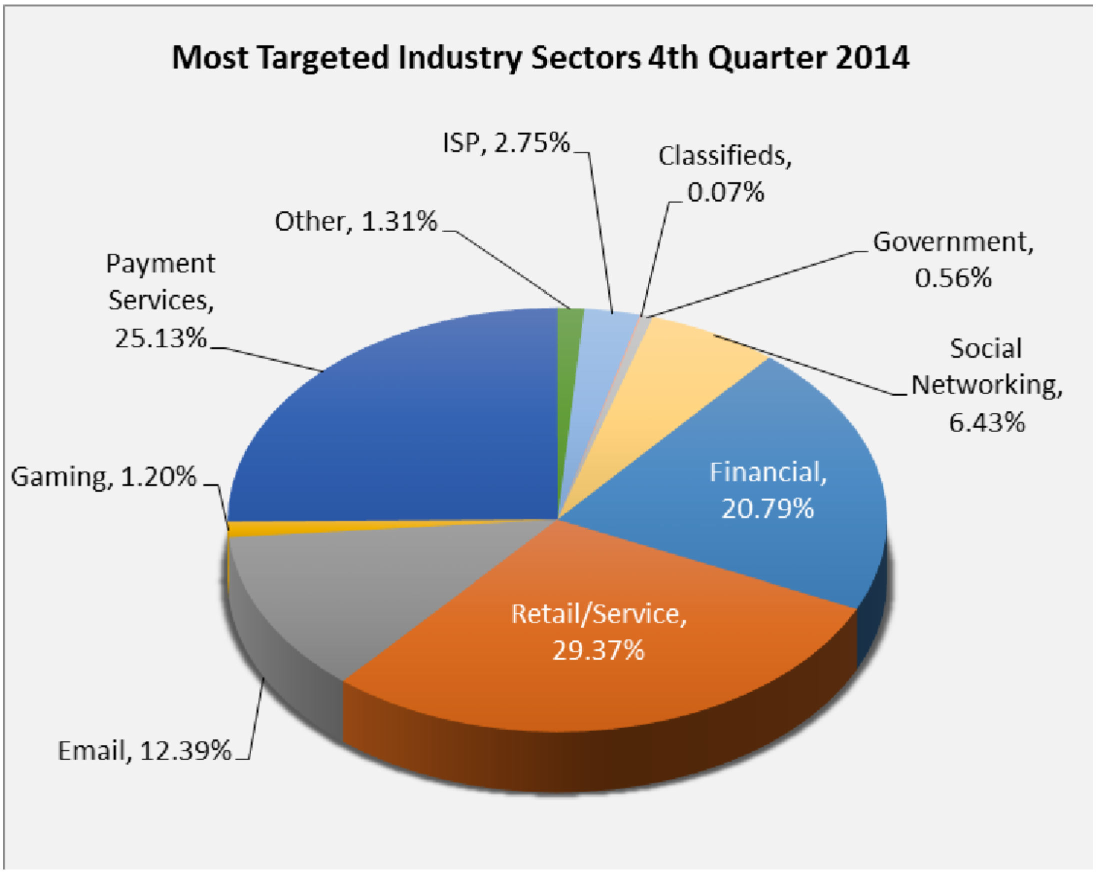
- During the 4th quarter of 2014, a record number of malware variants were detected – an average of 255,000 new threats each day;
- The number of unique phishing reports submitted to APWG during Q4 was 197,252. This was an increase of 18 percent from the 163,333 received in Q3 of 2014;
- The total number of phish observed in Q4 was 46,824;
- A total of 437 brands were targeted by phishers in Q4;
- The United States continued to be the top country hosting phishing sites;
- The United States remained the top country hosting phishing-based Trojans and downloaders during the three month period.

[8] Keliho, Cutwail and Lethic are the names given to a botnet

[9] The Cost of Phishing & Value of Employee Training, Ponemon Institute (2015)

[10] APWG. 'Unifying the Global Response To Cybercrime. October – December 2014', Published April 29, 2015

[11] Ibidem



Graph 1. Most targeted industry sectors, 4th quarter 2014, source: APWG[12]

Spam Levels

Composite BlockList (CBL)

The CBL[13] maintains massive spamtrap[14] networks and provides blocking services (both free and commercial) for botnet-sent spam. The CBL was founded in 2003. The next two graphs represent total email flow into one of the CBL's larger spamtraps, and give a reasonably representative indication of overall spam flow.

The Y axis is emails per second. "5.0k" means 5,000 emails/second. Thus, for each 1,000 emails/second, the daily total is 86MM emails in 24 hours. The X axis is the date/time in GMT.

No attempt is made to distinguish spam from non-spam email hitting the trap. The total flow numbers will include "backscatter"[15]. The CBL does not list IP addresses for this reason, but other DNSBLs do.

One of the most important things to note is the highly cyclic volume of spam being sent. In particular, it is noteworthy, as is already mentioned, that spam is down significantly at the time of the writing of

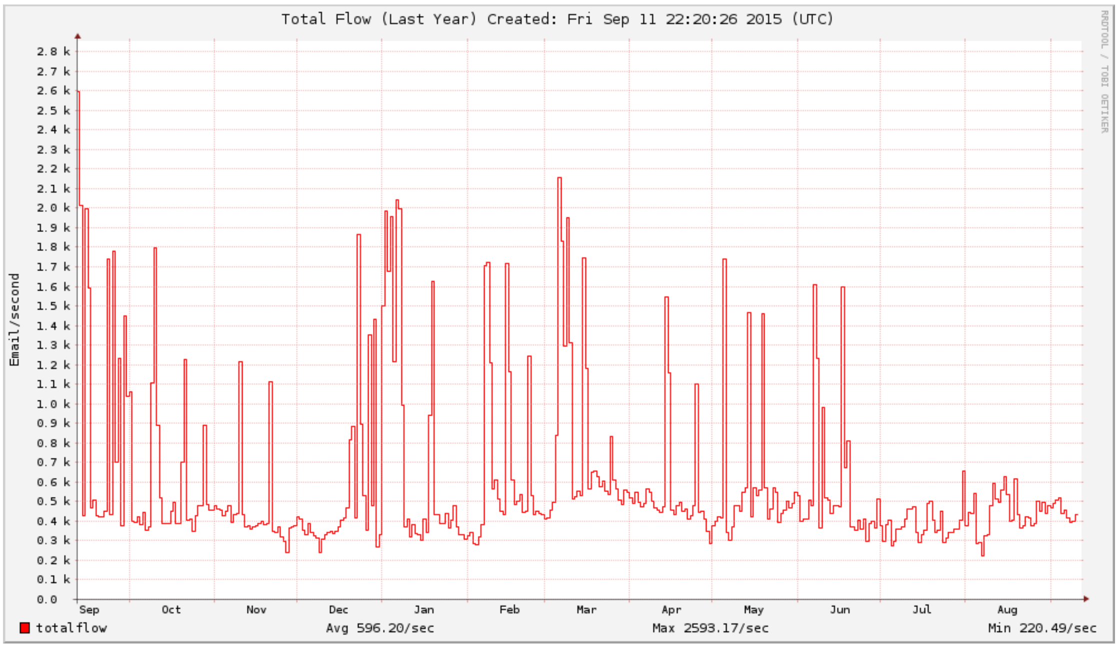
[12] Idem

[13] *http://cbl.abuseat.org/nas.html*

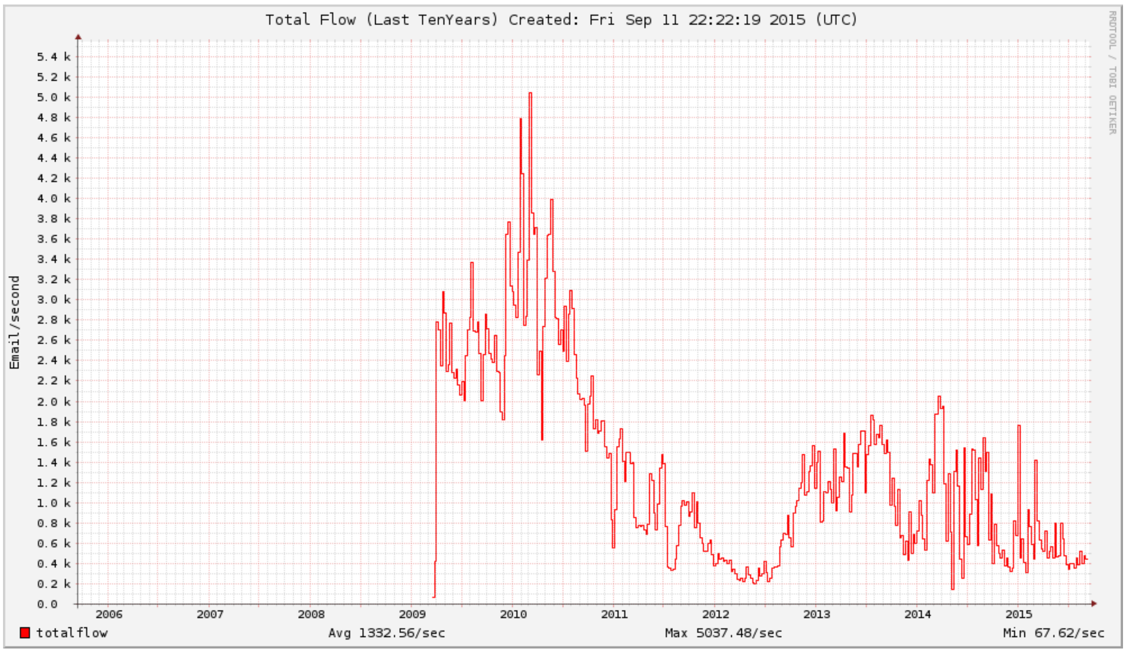
[14]Spamtraps are email addresses which do not belong to real users. A spamtrap either never belonged to a real user, or did but was closed and rejected email for a significant period before being repurposed". http://www.spamhaus.org/faq/section/Glossary#169 (Accessed 25-09-2015)

[15] Backscatter is where spam is created with a forged sender address, and is sent to a mail server that rejects the email by a bounce - to the forged address.

this report. Experts are extremely reluctant to attribute any reasoning to this - to do so would be conjecture - nor to indicate that this is anything but a temporary anomaly.



Graph 2. Flow to a single spamtrap, one year, source CBL (see Annex 3)

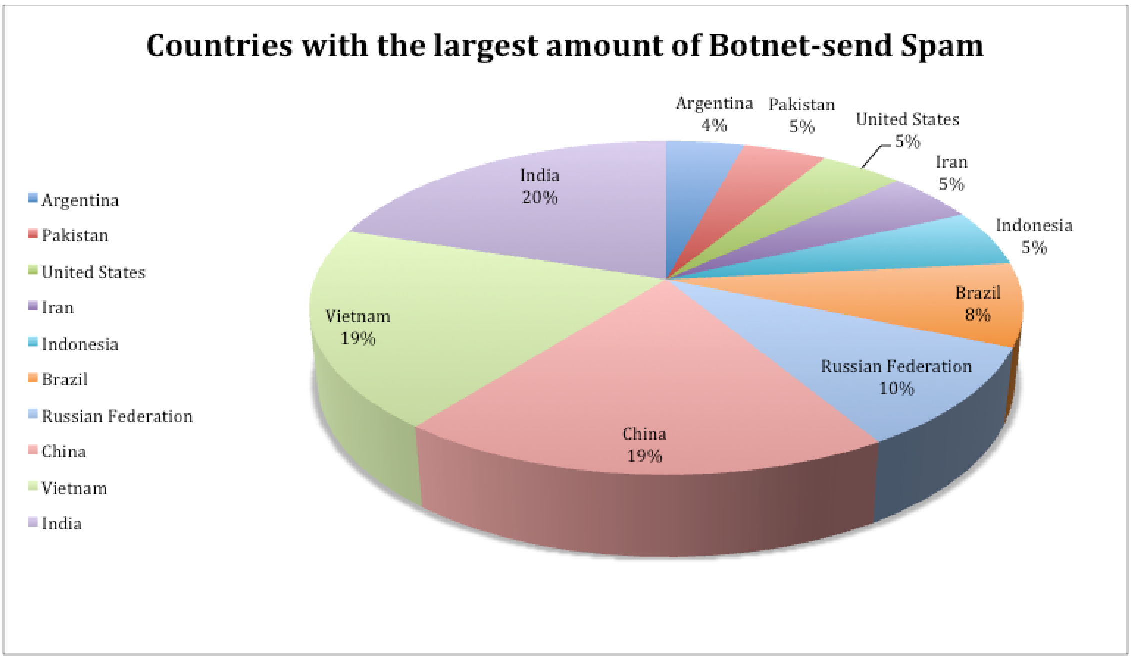


Graph 3. Flow to a single spamtrap, decade, source CBL

The Spamhaus Project

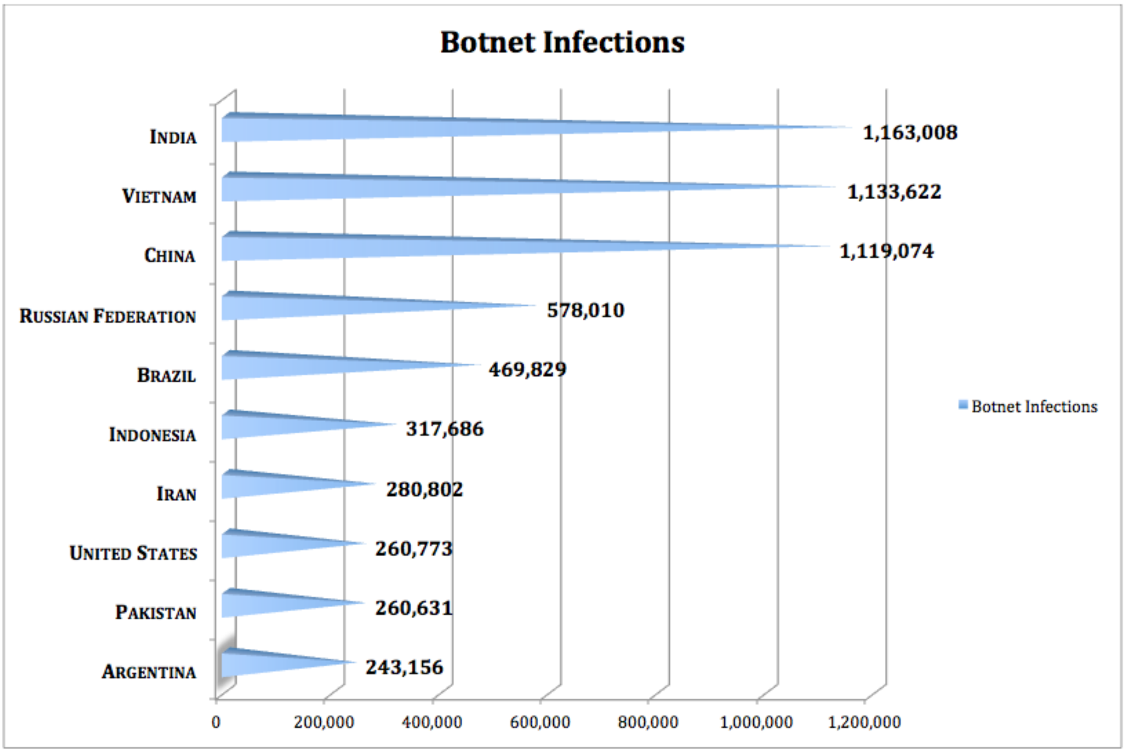
The Spamhaus Project[16] is an international nonprofit organization whose mission is to track the Internet's spam operations and sources, to provide dependable realtime anti-spam protection for Internet networks, to work with Law Enforcement Agencies to identify and pursue spam and malware gangs worldwide, and to lobby governments for effective anti-spam legislation.

Founded in 1998, Spamhaus is based in Geneva, Switzerland and London, UK and is run by a dedicated staff of 38 investigators, forensics specialists and network engineers located in 10 countries.



Graph 4. Countries with the largest amount of botnet-sent spam, source Spamhaus

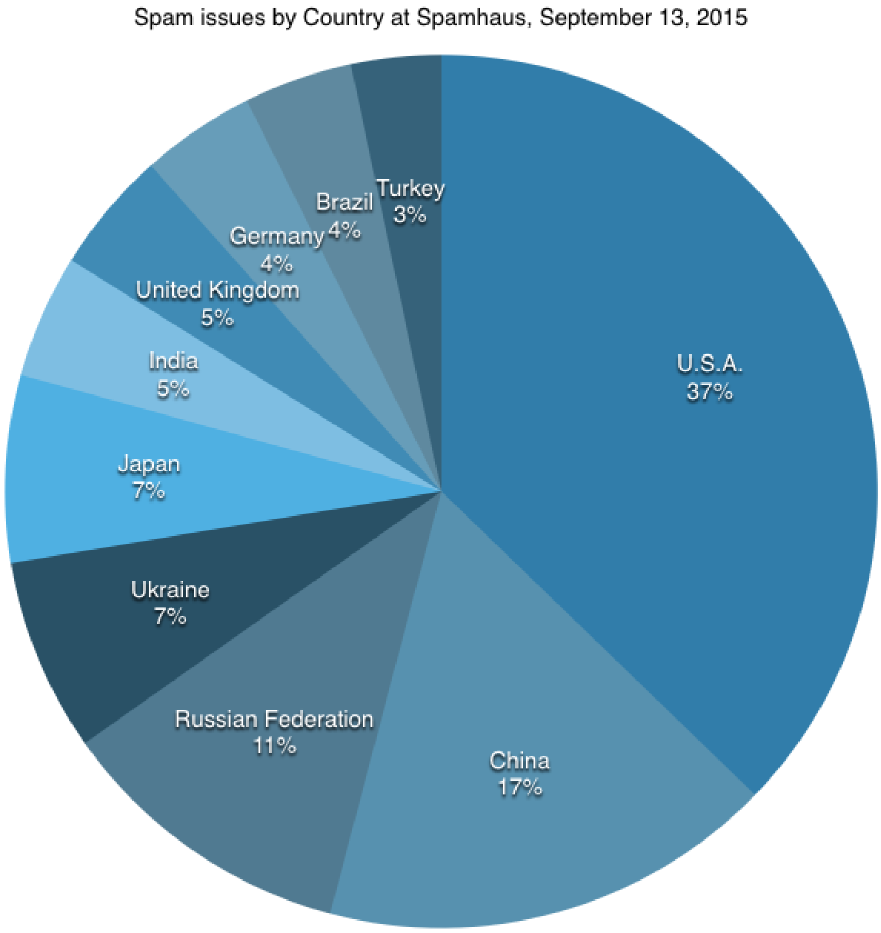
[16] http://www.spamhaus.org/statistics/networks/



Graph 5. Botnet infections, source Spamhaus

As can be clearly noted, those countries that undertook an anti-bot initiative in the early part of the decade no longer appear in the top 10 infected countries.

The following chart indicates the level of listings (botnet, hosting, DNS services provided, etcetera) per country at Spamhaus as of the date indicated.



Graph 6. Spam issues by country, September, 13 2015, source Spamhaus

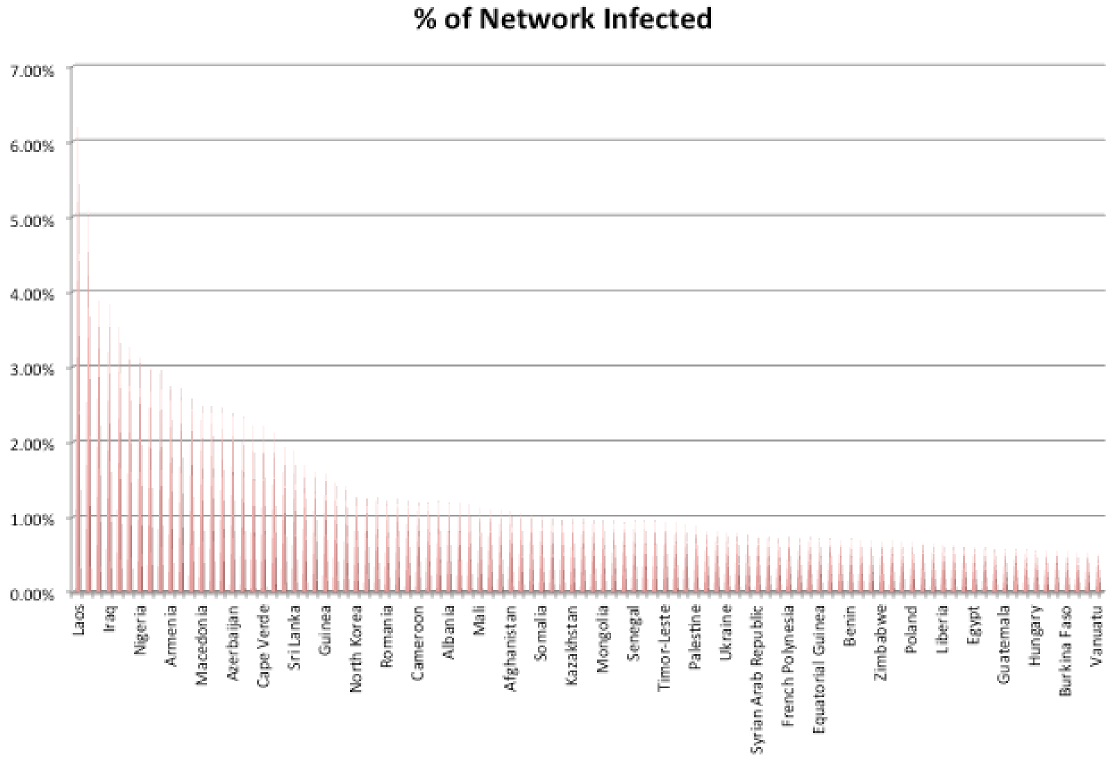
Botnet Infections, when viewed per-capita provide an entirely different picture; developing nations are significantly more at risk when this is taken into account.

#	Country	% Rate per capita
1	Dominica	8.36%
2	Côte d'Ivoire	2.18%
3	Algeria	1.70%
5	Macedonia	1.54%
6	Armenia	1.52%
9	Timor-Leste	1.18%

10	Belarus	1.17%
11	Mauritius	0.98%
12	Pakistan	0.91%
16	Libya	0.85%
18	Taiwan	0.80%
19	Tunisia	0.80%
20	Kazakhstan	0.77%

Stat 1. Botnet infections per capita, source Spamhaus

When we look at the percentage of infections in relation to network size, again, we see that Internet developing nations are more infected are at a higher risk of elevated botnet activity (see Annex 3 for a complete chart).

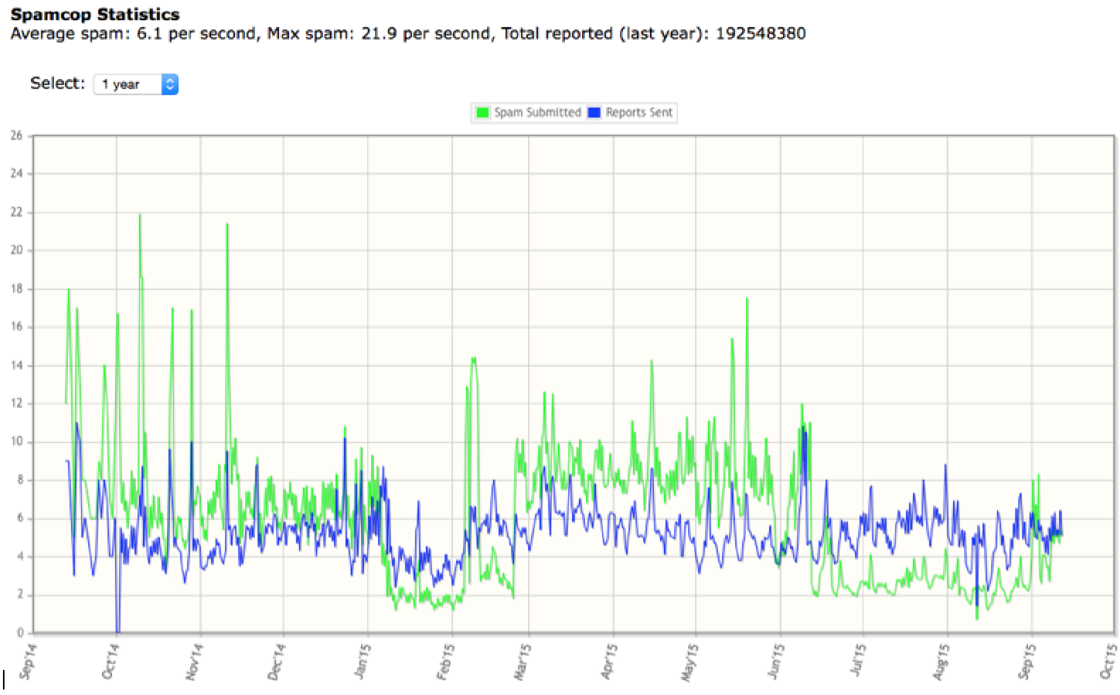


Graph 8. % of network infected per country, source Spamhaus

Spamcop

SpamCop[17] is a web-based service for reporting and blocking spam, founded in 1998. SpamCop processes millions of spam complaints a day and is supported by hundreds of thousands of users, a knowledgeable volunteer community, and a professional staff. SpamCop is now a wholly-owned subsidiary of Cisco Systems, Inc.

Spamcop's statistics are consistent with those presented above, noting a significant reduction in spam at time of writing.



Spamcop Statistics
Average spam: 6.1 per second, Max spam: 21.9 per second, Total reported (last year): 192548380

Select: 1 year

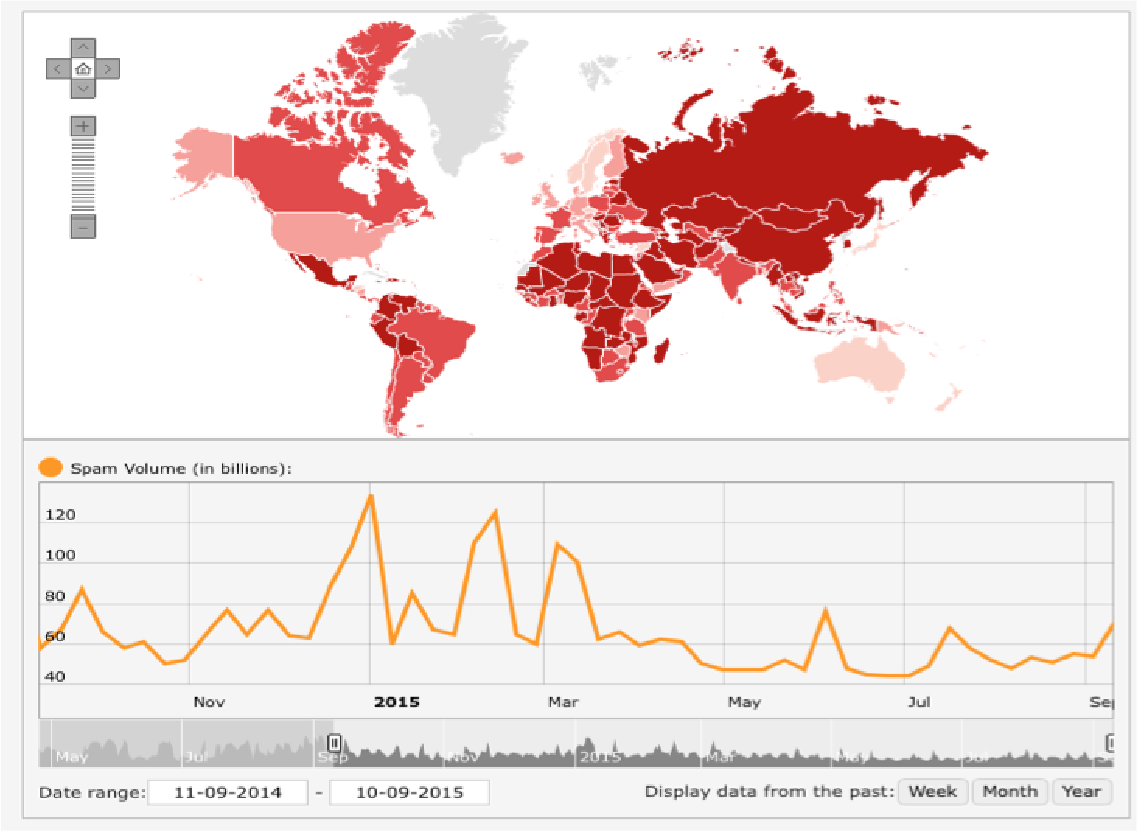
Graph 9. Average spam message per second, source Spamcop

Trendmicro

Trend Micro Inc. is a global security software company founded in Los Angeles, California with global headquarters in Tokyo, Japan, and regional headquarters in Asia, Europe and the Americas.

In the following map[18], darker colours indicate more activity. Again, a dip in spam levels is notable.

[17] https://www.spamcop.net/spamstats.shtml
[18] http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-spam-map/



Date range: 11-09-2014 - 10-09-2015

Graph 10. Spam activity per country, source Trend Micro

A list of other spam reference sources is at Annex 4.

Other 'statistical' information

This BPF has also considered whether statistics relating to cybercrime could help scope the spam problem. EuroJust, the European Union's Judicial Cooperation Unit[19], describes cybercrime as follows: "The term cybercrime is conventionally used to describe a criminal activity in which a computer or a network plays an essential role; however, cybercrime is also used to include other traditional crimes in which computers or networks make the illicit activity possible"[20]. It encompasses a range of activities, that are summed up in a EuroJust newsletter, as follows:

- A tool of the criminal activity (e.g. spamming, copyright crime);
- A target of the crime (e.g. unauthorized access, malicious code);
- The place of the criminal activity (e.g. telecommunications fraud);

[19] Eurojust stimulates and improves the coordination of investigations and prosecutions between the competent authorities in the Member States (of the EU) and improves the cooperation between the competent authorities of the Member States, in particular by facilitating the execution of international mutual legal assistance and the implementation of extradition requests. http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx

[20] http://www.eurojust.europa.eu/doclibrary/corporate/newsletter/Eurojust%20News%20Issue%207%20%28Nov%202012%29%20on%20the%20fight%20against%20cybercrime/EurojustNews_Issue7_2012-11-EN.pdf

- Facilitates cybercrime (e.g. Nigerian fraud, hacking, phishing, child pornography, identity theft)[21].

It is worth considering how cybercrime is reflected in the reporting of crime to governmental and law enforcement authorities, and their respective abilities to aggregate and publicly report on such figures. Team Cymru[22] notes that for the United Kingdom, no statistics on cybercrime could be found[23]. It was able, however, to provide figures on botnet controllers, infrastructure geo-located in the following countries that has the potential to cause harm globally[24].

U.K.	137
U.S.	422
Russian Federation	130

Stat 2. Number of botnet C&C per country, source Team Cymru

Team Cymru notes that the victims of the resultant botnet infections do not report being infected or hacked. It argues that reporting is important because: “*It helps us benchmark where we are today, drives investment and allocation of resources to meet demand. As with all organisations, governments will only make an investment where there is a clear demand and risks that cannot be mitigated by other means. Also with cyber crime as there has been no clear measurement to hold up against other types of crimes that Police Forces are measured against, it therefore falls down the priority list.* ...*“What gets measured gets done!*’””[25].

This is reiterated by Mark Goodman in his book *Future Crimes*[26]. “*This silence is at the very heart [of] our cybersecurity problems*”. The result being that: “*these incidents cannot be aggregated and studied, common defences are not developed, and perpetrators roam free to attack another day*”[27]. Goodman advocates that admitting a cyber problem is the first step towards getting better.

Dr. Christian Nordlohne of the University of Gelsenkirchen studied malware prevalence. He devised a new way to measure the value of a botnet against different measure points. To measure the prevalence of botnets is to identify the relevant factors and scale and to determine the ranking. There are two major steps:

- the bigger the botnet is the more it is prevalent;
- to assign numbers to the different malware families and botnets specifically in order to create a ranking[28].

All Botnets are hosted somewhere. Dr. Michel van Eeten at the Delft University of Technology “benchmark(s) the performance of hosting providers in terms of security reputation metrics (…) These

[21] Ibidem

[22] Team Cymru is a U.S. based organization that is “a group of technologists passionate about making the Internet more secure and dedicated to that goal. We work closely with and within Internet security communities, as well as with all manner of other organizations”. http://www.team-cymru.org/about-us.html

[23] Measurement of Cyber Crime. https://blog.team-cymru.org/2015/06/measurement-of-cyber-crime-royal-holloway-university-london/

[24] Ibidem

[25] Idem

[26] Future Crimes. Mark Goodman, New York (2015)

[27] Ibidem, pp 374-375

[28] Measuring Botnet Prevalence: Malice Value. Christian Nordlohne, Gelsenkirchen (2015)

metrics measure the degree to which servers of the provider are abused by criminals, as well as the speed with which providers remediate the situation"[29].

The Microsoft Security Intelligence Report (SIR) focuses on software vulnerabilities, software vulnerability exploits, malware, and unwanted software[30]. In the latest report three main conclusions are drawn on trends in malware[31]. One shows that criminals have found new weaknesses in the online world such as the targeting of vulnerabilities in Android apps. The report presents statistics on computers reporting in to Microsoft's systems on malware encounters and malware infections: "On average, about 19.2 percent of reporting computers worldwide encountered malware over the past four quarters[32]. At the same time, the MSRT (Malicious Software Removal Tool) removed malware from about 9.1 out of every 1,000 computers, or 0.91 percent"[33]. This figure seems fairly consistent for the whole of 2014.

At the core of this paper is a consideration of the 'Next Billion coming online.' To this end, a report published in 2014 in Kenya provided some insight into the scope of the malware problem in that jurisdiction, as follows[34].

Year	PBX attack[35]	Malware	Botnet	Proxy[36]	Trojan[37]
2012	450,000	1,000,000	900,000	50,000	200,000
2013	780,000	1,750,000	1,800,000	290,000	580,000
% increase	73%	75%	100%	480%	290%

Stat 3. The scope of malware in Kenya, source Kenya cybersecurity Report

The following graph, taken from the Kenyan report, shows that threat numbers can grow more rapidly than Internet connections.

[29] http://blog.check-and-secure.com/300615-security-reputation-metrics-hosting-providers/ (accessed, 2-7-2015)

[30] Microsoft Security Intelligence Report. Volume 18, June through December 2014, p V.

[31] All quotes come from Ibidem, p VI.

[32] Of 2014

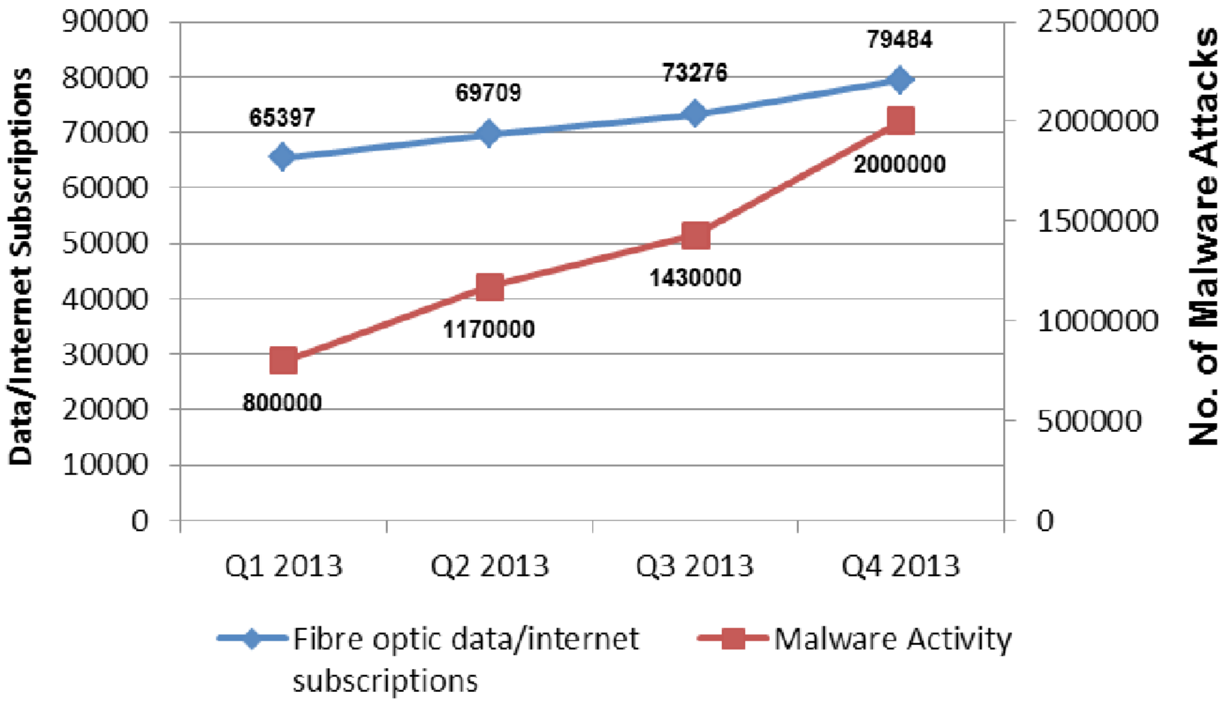
[33] Microsoft Security Intelligence Report. Volume 18, June through December 2014, p 39

[34] Kenya cyber-security Report 2014. Rethinking cyber-security – "An Integrated Approach: Processes, Intelligence and Monitoring.", page 13. Tespoc (2014)

[35] A private branch exchange, or in-company telephony exchange. A PBX attack makes illegal telephone calls that get billed to that company.

[36] *"Anonymous proxy servers refer to computer systems that allow users to access the Internet without leaving a footprint*", Kenya cyber-security report', page 12

[37] *"A trojan horse is a malicious software program that hides inside other programs. It enters a computer hidden inside a legitimate program, such as a screensaver. Then it puts code into the operating system that enables a hacker to access the infected computer. Trojan horses do not usually spread by themselves. They are spread by viruses, worms, or downloaded software*". https://support.microsoft.com/en-us/kb/129972.



Graph 11: Threat activity vs. Internet usage in 2013[38]

In summary, this BPF has brought together statistics from different sources that are respected in different communities and reflect the current situation about spam volumes. It is noted that there has been a recent downward trend in spam volumes, but it is not yet known what the reasons for this are and whether the trend will continue. At this point the BPF has consensus that more research is needed in order to measure the scope, to scale the problem and its cost on economies – both industry and government.

The next billion coming on line: What do the next billion want and what lessons can be learnt?

The BPF has the view that the problems that are likely to be encountered by the next billion are most likely very similar to those that have come before. Spam, infections, malware and cybercrime will invariably be prevalent, perhaps more so in developing nations, as measures that have been developed over time to address such issues may not be implemented prior to the broader deployment of broadband connectivity. However, the BPF also acknowledges that the next billion may require some alternate solutions directly applicable to their circumstance. For example, it is likely that connectivity by end-users will be predominantly through mobile devices and will be IPv6-based, thus making the implementation of traditional approaches more difficult (many anti-spam blocklists are only now coming out with IPv6 blocking capabilities, for example). While connectivity will inevitably bring a wealth of information and accessibility, it will also bring risks. This BPF has therefore considered the likely challenges for the next billion to come online, drawing on the experience and expertise of those who are already online and, in some cases, have learned some difficult lessons, while balancing this with the opinions of those coming online.

Survey of IGF Africa

As the IGF acknowledged in 2015, there are many challenges for the first (of several) billion who will be coming online in the coming 5 to 10 years. This BPF wanted to learn about the current situation

[38] Idem, page 14

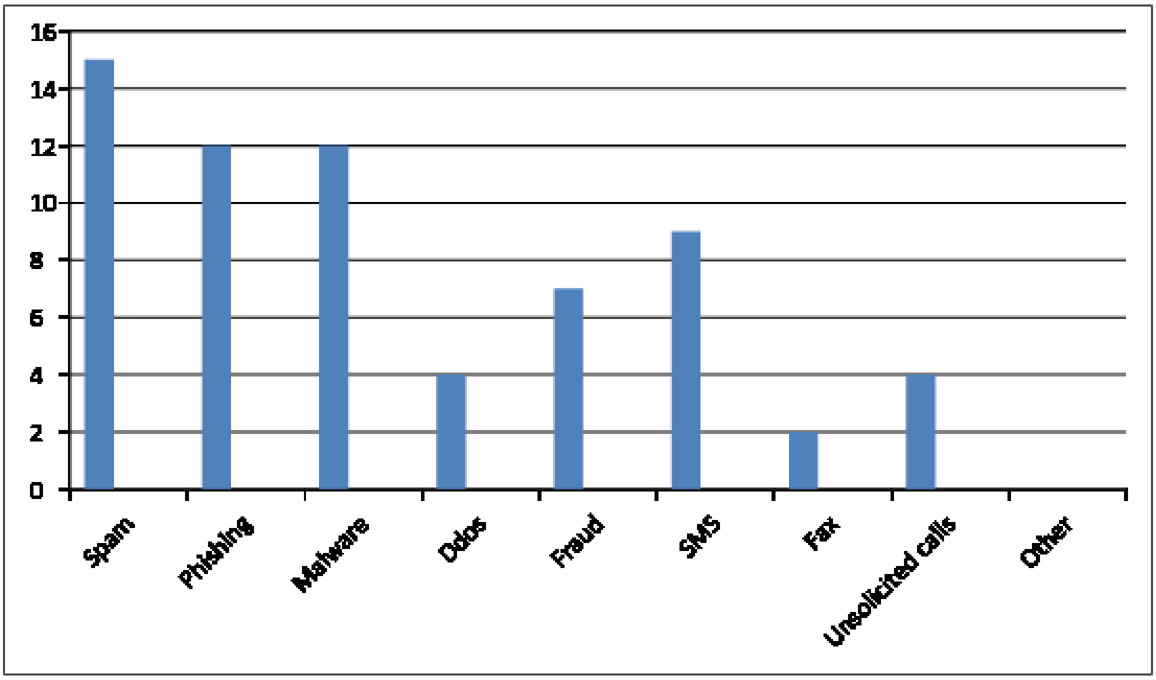
from first-hand experience and so solicited input from developing nations, working closely with IGF Africa[39].

In order to receive first-hand accounts of the situation in developing nations, a survey was created and sent out to the members of IGF Africa (see Annex 5). A total of 15 responses were received[40]. While with such a small number of respondents it is not possible to claim that the results of the survey are representative, the qualitative data indicates that respondents consider that there are issues relating to unsolicited communications that ought to be addressed. In summary all participants felt a need for change, saw a need for training and sensed an urgent need for action.

Responses to the survey were received from representatives residing in the following countries[41]: Senegal; Burundi; Kenya; Liberia; Niger; Benin; Togo; Cameroon and Nigeria. The backgrounds of respondents varied; including from governments, NGOs, IGOs and academia.

None of the countries represented have anti-spam legislation in place although one indicated that a law was in the process of being made. Five respondents indicated, however, that there is a cybercrime law in their home jurisdiction, while a further four indicated that such a law is planned. The results do not show if the existing or planned cybercrime laws cover unsolicited communications.

Fourteen respondents indicated that ISPs in their respective jurisdictions have not implemented best practices to prevent unsolicited communications. Respondents highlighted that spam, malware and phishing were all prevalent (see following graph).



Graph 12: Spam categories as reported by respondents

Awareness campaigns relating to cybersecurity were available in the jurisdictions of 7 respondents. 7 Respondents also indicated that cybersafety was a topic of the curricula at schools and/or

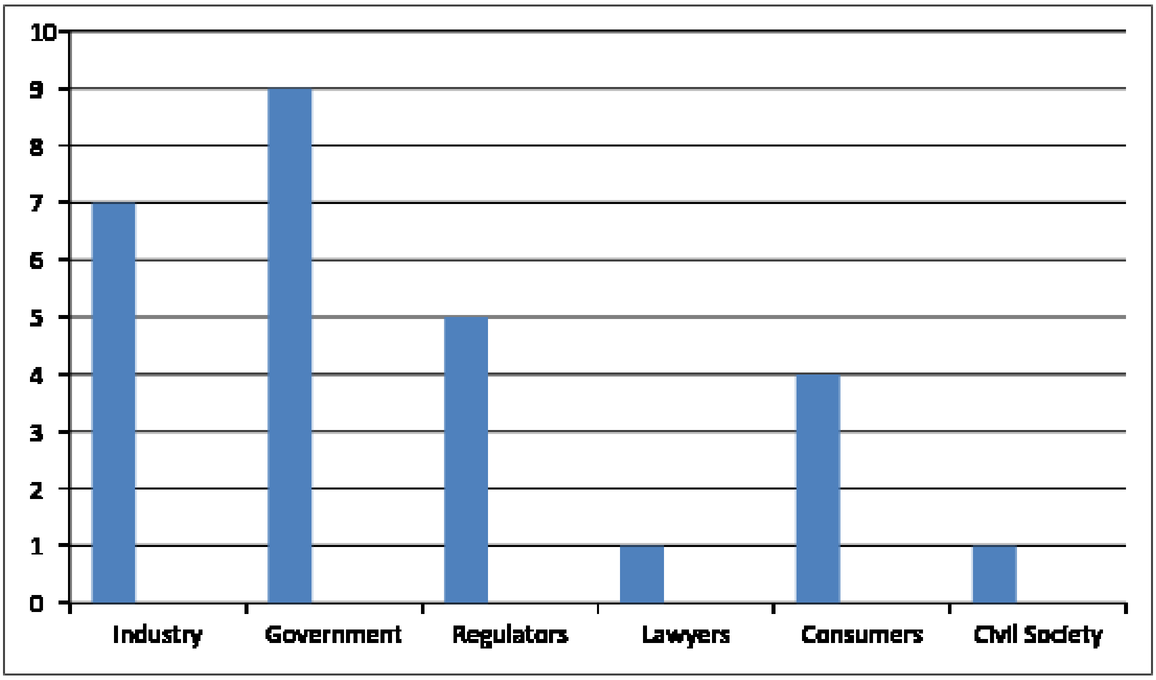
[39] This BPF thanks Mr. Makane Faye for his kind cooperation.

[40] IGF Africa used the outcome of this survey in its anti-spam program before and during its regional meeting in September 2015.

[41] Not all the home jurisdictions of respondents could be identified.

universities. Seven respondents mentioned that there was either a national (5) or regional (2) multi-stakeholder initiative[42] that deals with unsolicited communications or cybersecurity.

The second half of the survey considered plans for the future. Respondents were able to provide free text responses to questions. Responses indicated that training was considered a necessity for policymakers, industry, civil society, lawyers and end users (see following graph).



Graph 14: If training were to be made available, who needs this training?

When asked about topics for training, a range of responses were received including the following:

- The need for awareness programs so that citizens can distinguish between spam and genuine messages;
- Internships and exchange programs;
- Balancing privacy protections with the right to open access; and
- Technical skills.

Two examples were provided by respondents of mitigation strategies relating to unsolicited communications that had been tried, including: (i) carrier restriction on outgoing SMS to three per day in Nigeria; and (ii) measures in the Senegalese mobile market by the regulator. In addition, two respondents flagged a desire for the closure of port 25 by Internet Service Providers (as is the case in other jurisdictions).

While the number of respondents to the survey is small, the results clearly indicate a desire for leadership to resolve the problem of unsolicited communications. Training has been flagged as a particular need and, as will be seen, is a key recommendation of this BPF. Other recommendations

[42] The following initiatives were mentioned: www.kigf.or.ke; www.kictanet.or.ke; West-Africa IGF, local CSIRT; http://www.cybersecuritynigeria.org.ng/; the national IGF

which will be presented at the end of this document are equally relevant to African and other developing nations who are newly online.

It should be noted that this BPF has received feedback from the IGF Africa meeting where the participants "found the results reflecting the real situation in Africa"[43]. This statement seems to endorse the survey conducted by this BPF and may indicate that there is merit in distributing similar surveys to other developing regions in the future. Further, this BPF has been advised that the IGF Africa made recommendations in relation to cybersecurity issues, including spam (see below). This again highlights the importance being placed on these issues in African economies.

Addressing cybersecurity issues, including spam

Panellists put emphasis on the need for an African Safety mechanism for African e-consumers with an emphasis on Pan-African collaboration and cooperation in the prevention, investigation and prosecution of Cyber Crimes including issues related to effectively countering and combating spam. The following specific recommendations were made:

1. *Encourage government, the private sector and non-governmental organizations to work together to raise public awareness on the risks of spam and of cybercrime and of what can be done to combat it;*

2. *Enhance capacity building in cybersecurity, including spam for law enforcement personnel, prosecutors, magistrates and judges;*

3. *Encourage African government to ratify the African Union Convention on cybersecurity and Personal Data Protection and to transpose their cybersecurity laws in the framework of the Convention in such a way as to facilitate international cooperation in preventing and combating these illicit activities;*

4. *Encourage all African government to update their criminal laws as soon as possible, in order to address the particular nature of cybercrime. In determining the strength of new legislation, States should be encouraged to be inspired by the provisions of the African Union Convention on cybersecurity and Personal Data Protection;*

5. *Build regional and international cooperation in cybersecurity to enhance public protection and to promote more effective information sharing to address cyber crimes issues (effective regulation adoption, anti-spam technology development, and training/awareness raising of users and providers);*

6. *Disseminate anti-spam best practices for service providers to enable them take the most appropriate measures to combat spam*[44]*.*

This BPF has consensus on the need for training and capacity building in the African region and concludes that this BPF's African survey outcomes reflects the current situation in Africa.

Some international lessons

While this stream makes recommendations on how developing economies can prepare themselves for the future, threats delivered using unsolicited communications are constantly evolving. This is not only as a consequence of technology advances (particularly in relation to the number, availability and type of Internet-enabled devices, the "Internet of Things") but because online threats, particularly those delivered by way of unsolicited communications, have become increasingly sophisticated.

The Australian Communications and Media Authority noted at the launch of a new portal for its Australian Internet Security Initiative (AISI) in 2014: ""*I urge you to think back to how you used the*

[43] E-mail M. Faye to W. de Natris, 8 September 2015
[44] E-mail M. Faye to W. de Natris, 18 September 2015

Internet in 2005. How many computers did you have at home compared to now? Certainly, you were unlikely to be using a smartphone or a tablet or a refrigerator, television and other household appliances were unlikely to have Internet connectivity. All of this has changed in recent years and it has meant for Internet users, and for schemes such as the AISI, that finding the actual device that is infected on a particular Internet service can be complex. And it is likely, with the emergence of smart homes that many, many more home appliances will be Internet-connectable and that this complexity will be a continuing theme into the future". The ACMA went on: "*With threats constantly evolving it's a bit like gazing into a crystal ball when contemplating the future, suffice to say that we will not be resting on our laurels. Having said this, there are already some fundamentals we can build on. Educating consumers and businesses to take action to minimize their risk is critical; and ensuring that programs which involve public-private partnerships, such as the AISI, and its latest innovation the AISI portal, identify problems when they do arise, will help keep the Internet clean. Indeed, we at the ACMA will continue to fight malware on two fronts*"[45].

As mentioned earlier in this report, central to the spam problem is the issue of malware that permits the spread of unsolicited communication via botnets. The Delft University of Technology has in recent publications focussed on the effectiveness of botnet mitigation centers. While there are limitations to the scope of this work, it was acknowledged that (participation in a) botnet mitigation centre seems to nudge ISPs in a certain direction, but does not dictate their actions. What has been noted, is what seems to be a shift of infections from members of AbuseHUB[46] to non-members[47]. If this trend is substantiated in follow up research, the conclusions of this evaluation may change over time.

In Finland the combination of the Telecommunications Act making disinfection mandatory, a regulator with the power to regulate and ISPs that adhere to the law, results in the lowest botnet infection figures for years on end[48].

Researcher of the University of Tilburg, Karine e Silva, assisted the BPF by providing a case study (at Annex 6) detailing current anti-spam and botnet research, highlighting the value of public-private cooperative efforts and international cooperation.

This BPF also received input on territoriality from prof. Dan Jerker Svantesson of the Bond University in Australia in which he states that "*The issue of jurisdiction over online activities has been controversial since the earliest days of large scale Internet usage*" and that "*the time has come to abandon territoriality as the core principle of jurisdiction*". His full contribution is found in Annex 7 to this draft report.

On the basis of the provided input, this and last year, from academic researchers as well as in the above mentioned recommendations made to African states, it is the consensus view of this BPF that cross border cooperation must evolve.

Existing examples of best practice documentation

It is not the role of this BPF to reinvent the wheel. Indeed, there have been many best practice documents on the handling of spam and abuse; they vary in both quality and continued relevancy due to depreciation as they age and the threat landscape continues to evolve. The following is a discussion

[45] http://www.acma.gov.au/theACMA/live

[46] See annex 11 for an extensive introduction of AbuseHUB.

[47] Evaluating the impact of AbuseHUB on botnet mitigation. Interim deliverable 1.0. Giovane C. M. Moura, Qasim Lone, Hadi Asghari, and Michel J.G. van Eeten (2015)

[48] http://www.intgovforum.org/cms/component/content/article/116-workshop-proposals/1023-igf-2012-workshop-proposal--no-87-cross-border-cooperation-in-incidents-involving-Internet-critical-infrastructure

of the recently-published revision of an omnibus best practices document: Operation Safety-Net: Best Practices to Address Online, Mobile, and Telephony Threats[49].

The Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG[50]) founded in 2003, is an international non-profit, industry-led organization founded to fight online abuse such as botnets, phishing, fraud, spam, viruses and denial-of service attacks that can cause great harm to both individuals and national economies. M^{3}AAWG draws upon technical experts, researchers[51] and policy specialists from a broad base of Internet service providers and network operators[52] representing over one billion mailboxes, and from key technology providers, academia and volume sender organizations[53].

M^{3}AAWG has published dozens of best practices documents[54] dealing with all aspects of Internet messaging abuse.

In October of 2011, members from the anti-spam civil law enforcement association the London Action Plan (LAP)[55] and M^{3}AAWG made a presentation to the Organisation for Economic Cooperation and Development (OECD) Committee on Consumer Policy (CCP) regarding the current prospect for the OECD's anti-spam recommendations to address future online threats.

In June 2012, members of LAP and M^{3}AAWG and experts from the community-at-large began the process of developing the report which was published in October of that year[56]. Operation Safety-Net, the Global Best Practices report provides readers with a plain-language description of the threats facing businesses, network providers and consumers in the online and mobile threat environment, divided into four key sections: Malware and Botnets; IPs and DNS; Phishing and Social Engineering; and Mobile Threats. Furthermore, the report includes a rich set of reference materials for those charged with resource allocation and implementation of the policies, protocols, and technical measures modern anti-abuse activities demand.

The initial report served as the basis for numerous global training initiatives and was evangelized to all levels of government and industry. Three years later, 100 leading experts from academia, industry, law enforcement, government, and end-user advocacy NGOs began work to update the materials, to reflect the changing online landscape, and to ensure the document remained accurate and relevant. The second version of the report, published in June 2015[57], included updates to the four original sections, and covers new areas including Voice over Internet Protocol (VoIP) and Voice Telephony fraud, Caller ID Spoofing, abuse issues for Hosting and Cloud Services, and online harassment.

Ultimately, the document arrives at several key conclusions:

This report provides best practice recommendations for consumers, industry and governments to address online and mobile threats. These include recommendations for consumers to be more proactive in securing their own devices; for service providers to implement recommended security technologies and practices without delay; for governments to ensure modern regulatory and legislative environments are in place and enforced, and to work with international organizations to champion collaborative efforts.

[49] https://www.M3AAWG.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf
[50] https://www.M3AAWG.org/
[51] https://www.M3AAWG.org/senior-technical-advisors
[52] https://www.M3AAWG.org/about/roster
[53] https://www.M3AAWG.org/our-partners
[54] https://www.M3AAWG.org/published-documents
[55] http://londonactionplan.org/
[56] http://www.cauce.org/2012/10/best-practices-report.html
[57] Operation Safety-Net. Best Practices to Address Online, Mobile, and Telephony Threats. MAAWG/LAP (2015)

These recommendations are a set of tools to manage online, mobile and voice threats. However, the threats described in this report are just a snapshot of the threat environment today. As online activities change, the use of mobile computing grows, and Internet users and businesses change their responses and defences to existing threats, these threats will shift and adapt to exploit new vulnerabilities and pursue new targets. Putting these recommendations into practice will take a concerted multilateral approach. To that end, the authors of this report strongly encourage the OECD and other international organizations to join with M^{3}AAWG and the LAP and engage with the organizations that govern and administer Internet infrastructures. In addition, in order to stay in front of the changing threat environment, all organizations concerned should begin to more proactively collaborate in monitoring threats and implementing new measures as needed to address them[58].

Further, M^{3}AAWG supports the notion of training for the developing world that is broader than simply education on the perils of spam. Its contribution in Annex 8 expands upon this.

This BPF concludes that many economies do not have a proficient technical knowledge to address complex abuse problems. Moreover, there is often a lack of awareness of existing community partnerships and a need for ongoing work to address these issues. Many of the economies with new or expanding Internet infrastructure participating in the ITU discussion have requested assistance in implementing practices and technologies that protect their developing networks from spam and other threats. This view, again, is substantiated by the IGF Africa survey and the recommendations made to African governments. This BPF is close to consensus on the need for training at the network level and will come back to potential ways forward below.

Legislative solutions

It was mentioned earlier in this report that none of the respondents to our IGF Africa survey came from countries that have anti-spam laws. Many western countries have found legislation to be an effective way to tackle the problem of spam[59]. A case study from Peter Merrigan of the New Zealand Department of Internal Affairs at Annex 9, details the experience in New Zealand.

Multi-layered strategies for fighting spam

Many jurisdictions have realised that it is simply not possible to fight spam with a single approach. Rather, they have decided to tackle the problem using a number of different complementary approaches that create a multi-stakeholder framework to deal with the problem. The case study at Annex 10 from Cristine Hoepers of Cert.br explains the Brazilian experience.

Multi-stakeholder initiatives involving industry

A number of jurisdictions have adopted malware mitigation strategies that are, in essence, multi-stakeholder initiatives. The case study at Annex 11 from Machiel Bolhuis, Chairman of the Abuse Information Exchange, explains the Abuse Information Exchange in the Netherlands.

Other examples of security initiatives that impact unsolicited communication

As mentioned in the introduction of this report, the BPF has benefited from contributions made by a number of individuals in the form of case studies. There are, however, a number of initiatives that have not already been mentioned that have shown to be effective in minimising spam. It is worth noting, however, that this BPF acknowledges that many of these initiatives (as well as some mentioned earlier) are not entirely dedicated to the prevention of unsolicited communication. Rather, they are cybersecurity initiatives that have a broader goal. These are detailed at Annex 12.

This BPF concludes that there are several successful public - private and public - public partnerships in operation, cooperating in the mitigation of (some form of) unsolicited communication. The BPF has

[58] Ibidem, p 63

[59] Spam laws and their backgrounds have been discussed extensively in last year's BPF report.

consensus that this form of cooperation is an important way forward, deserving further study, with the aim of implementation in other jurisdictions.

Public-Private Partnerships

As part of this BPF, a list of public-private partnerships has been started. These are at Annex 13.

Lessons learned from this BPF and recommendations

The following are some key observations and recommendations that have emerged through the BPF. Each of the recommendations, that were derived from the online BPF process, were tested at the BPF session at João Pessoa through idea rating sheets that were distributed in the room. The results are reflected in the text below.

Scope

In collating this report, it became abundantly clear that it has been difficult for the group to stay on topic – that is dealing with best practices for dealing with unsolicited communications. Spam has, for many years, been a symptom of poor cybersecurity practices. As the Internet has evolved, Internet speeds have got faster and cybercriminals have got smarter, spam has become only one of a range of problems that might arise for those who are coming newly online. As this report shows, often solutions that help the spam problem are designed to deal with other security issues. While this BPF does not consider that spam is a problem to be ignored, the BPF has demonstrated that our thinking has broadened and that in future, it would be better for BPFs to focus on broader cybersecurity issues. This recommendation has been generally supported, however, it was noted by some that future work will need to be focussed in order to be meaningful.

Recommendation 1: That if the IGF decides to continue this work, there would be more value in identifying a specific topic (for example, capacity building) within an expanded remit that encompasses broader cybersecurity and cybersafety issues, as unsolicited communications are only one aspect of the many issues relating to the protection of infrastructure and citizens online.

Statistics

As stated toward the beginning of this report, this BPF held high hopes of finding a single dataset that described the scale of the spam problem. The BPF was unable to find such a dataset. This report, however, has provided numerous facts and figures about spam, malware and botnets that we consider provides some guidance on the scale of the problem. However, the BPF considers that further work could be done to pin down a set of reliable metrics that relate not only to spam but broader cybersecurity issues and sees a role for academia here. Broadly speaking, there was agreement with this recommendation in João Pessoa. One participant noted that: "*We need to encourage companies affected by the problem to talk about it more openly.*"

Recommendation 2: That further work could be done to pin down a set of reliable metrics that relate not only to spam, but broader cybersecurity issues.

Botnet mitigation

This BPF has learned that although researchers remain cautious, the first statistical research into the effects of botnet mitigation centres has shown that these centres have a positive effect in dealing with botnets. It is noted that the success of such programs rely on the action taken by participating ISPs on infections in their respective networks.

This recommendation had strong unanimous support at the BPF session in João Pessoa.

Recommendation 3: That all, including newly connected economies consider multistakeholder anti-botnet efforts (botnet mitigation centres) as they have a role in reducing the number of infections on end users' devices.

Reporting of cybercrime

As detailed earlier in this report, it seems likely that citizens vastly under report cybercrime and that, when they do, it may not be classified as such. As researchers have indicated, this has meant that the scale of the problem cannot be reliably scoped. This BPF considers that processes should be amended to properly categorise crime that is undertaken using the Internet. Further, this BPF considers that citizens should feel free to and comfortable about reporting cybercrime.

While those in João Pessoa were mainly supportive of recommendations 4 and 5, a small number voiced concern that focussing on statistics could delay the resolution of criminal issues. It was also noted that many crimes being conducted using the Internet are the same crimes that have always been perpetrated.

Recommendation 4: That effort be taken by law enforcement to categorise crimes undertaken using the Internet.

Recommendation 5: That governments and law enforcement take proactive steps to encourage the reporting of cybercrime by all users: citizens and industry.

African IGF Survey

The results of the African IGF survey have been a major output of this BPF. As detailed in the relevant section of this report, although only 15 responses were received, the reach of the survey was broad and some key themes came through, such as the recognition of the need for training. It is clear to this BPF that there is significant interest in Africa on this topic and a need to be heard. Indeed, the BPF was approached asking if the survey could be extended as the IGF Africa identified others who are interested in participating, and, as is covered in the relevant section of this report the IGF Africa recognises the need to take action in relation to cybersecurity matters and specifically mentions spam. It is therefore a key recommendation of this group, as was suggested earlier in this report, that further attention ought to be given to surveying the needs of African (and other developing nations), not only in dealing with the problem of spam, but the broader issues of cybersecurity and cybersafety.

There was broad support for this recommendation at the IGF. However, there was one participant who did not agree and it was noted that infrastructure is needed first.

Recommendation 6: That further attention ought to be given to surveying the needs of African nations (and other developing nations), not only in dealing with the problem of spam, but the broader issues of cybersecurity and cybersafety.

Training

This BPF recognised the need for basic cybersecurity training, including spam mitigation, in the African region and presumes that this may be the same in other regions around the globe. The implementation of basic spam security measures and best practices heightens the security of end users and organisations in the region immediately and prevents high numbers of unsolicited communications from reaching other regions as well.

Training tools, such as the M^{3}AAWG/LAP Best Practice document, already exist and training has and is being deployed to those who are newly online as the M^{3}AAWG training case study outlines. The BPF has discussed and acknowledges that there are difficulties in tailoring training for audiences for a range of reasons including:

- cultural issues – for example, an inclination not to ask questions at the time of training in some countries as it may be viewed as being discourteous to the trainer;
- language issues – most training materials have not been translated into local languages and experts rarely have the requisite language skills to present in native tongues;

- lack of technical skills; and
- financial issues.

However, this BPF considers there is value in moving this forward, even if it is incrementally. To facilitate a first step, this BPF conducted a separate workshop on the issue in João Pessoa. In particular, capacity-building for developing nations coming online in the form of technical, consumer, regulatory and other learning needs were identified at that session; as was the need for industry to help fund such initiatives. Early signs suggest a willingness from many to collaborate in moving these issues forward.

There was unanimous agreement with this recommendation in João Pessoa.

Recommendation 7: That there is a need for basic cybersecurity training, including in relation to spam mitigation, in the African region and perhaps other regions of the globe. Active participation from other regions is recommended. An example could be to organise workshops at the African Internet Summit.

Consumer Education

It was noted during the comments period that miscreants will always find a way to send unsolicited communications and that people would be better protected if they were educated. In particular, it was suggested that effort should be put towards helping end users understand the characteristics of scam and phishing emails. Further it was suggested that affected industries, such as the banking industry, develop widely understood practices such as agreeing to only contact their customers through online portals such as online banking and not contacting via email. This BPF supports these notions. In particular, the BPF considers that education of citizens is something that must start with children as experience has shown that in technical matters, it is the children that tend to educate their parents rather than the other way around. Further, the BPF considers that affected industries must adapt to not only protect their own reputations but to ensure that their own customers do not become victims.

There was unanimous and strong agreement with recommendation 8 in João Pessoa. Particular comment was made of the need for Internet matters to be incorporated into school curricula as one of the basics, along with reading, writing and arithmetic. There was also unanimous strong agreement with recommendation 9, and it was specifically discussed that industry ought to contribute to the cost of education referred to in recommendation 8.

Recommendation 8: That there is a need for education of citizens, including children, on matters relating to cybersecurity in economies coming newly online.

Recommendation 9: That industries affected by spam, phishing, etcetera must continue to evolve in order to protect their own reputations and to ensure that their own customers do not become victims; including the provision of funding for education programs.

Quick wins

As part of this BPF group members were asked to create lists of low or no cost solutions that could assist in dealing with the spam problem. While it was hoped that more complete lists could be compiled, the following are the quick wins that were identified for regulators:

- Education of industry through blogs and social media outlining obligations;
- Snappy consumer slogans; for example - Ignore it! Report it! Delete it!;
- Looking for speaking opportunities at e-commerce forums (speakers often attend the conference free of charge);

- Joining industry coalitions such as M^{3}AAWG.org or the London Action Plan where ideas and investigation information can be shared;
- Regular engagement with Industry, including ISPs, MNOs, Marketing authorities, relevant to work/patterns/trends;
- Attendance at Internet related and cybersecurity related conferences is very beneficial;
- Issue press/media releases on important and significant milestones/prosecutions;
- There are numerous websites that provide relevant educational materials and resources.

A technical list of low and no-cost initiatives has also been started:

- Set up a reporting center using open source tools for example, using databases built by other jurisdictions and offered freely or building a phishing reporting centre using a webform that emails reports to a ticket system;
- Deploy authentication at important senders: banks, government. This helps to prevent some types of phish. (SPF/DKIM/DMARC);
- Process DMARC records (free tools are available);
- Use publicly available feeds and parse them for bot-infections in country (clean these up with the assistance of an ISP if doable);
- Make sure operators understand how to identify responsible parties/abuse contacts for Internet resources (training).

These lists are by no means complete. So the BPF recommends that further consideration be given to producing lists of low or no cost initiatives that can help newly connected jurisdictions to take quick, cheap and achievable steps to assist in protecting their infrastructure from unsolicited communication.

Recommendation 10 had unanimous support in João Pessoa.

Recommendation 10: That further consideration ought to be given to producing simple lists of low or no cost initiatives that can assist newly-connected economies to protect their infrastructure.

The role of multi-stakeholder initiatives

This BPF spent considerable time considering multi-stakeholder initiatives that deal with the problem of unsolicited communications. A number of case-studies have been included in this report and some other examples have been referred to the annex section. It has been clear through this BPF that while it is always beneficial for government to have a role in the management of unsolicited communication, it does not need to tackle the problem on its own. Indeed, some of the examples cited in this report do not involve government. Having said this, governments can and should play a key role in ensuring a safe online culture within their own jurisdictions; including through the promotion of education, legal avenues, supporting technical solutions and (where necessary or helpful) facilitating or supporting public - private and private - private initiatives.

There was unanimous strong agreement with recommendation 11.

Recommendation 11: That consideration ought to be given by all, but especially newly connected economies to a wide variety of multi-stakeholder arrangements, including public-private and private-private initiatives in combating unsolicited communications.

Conclusion

In conclusion this BPF has taken significant steps to outline the scale and scope of the unsolicited communication problem, taking into account the limitations of such an exercise. The BPF has engaged directly with those who are newly online in Africa and has formed a view that although cybersecurity is constantly evolving that the assistance that is sought by those directly affected, generally matches with the expectations of those who can assist.

The BPF has outlined in some detail the experience of others, through case studies, and hopes that these experiences also provide a guide for those who are newly coming online. It remains, however, for those with funds and in positions of power, including governments, to consider their roles in protecting the connectivity of their respective jurisdictions and educating citizens on safe online practices.

Annex 1 Recommendations for future work in the 2014 report

a. Common understanding of the problem. The more aligned stakeholders are with regard to the issues, their severity and the priority of their resolution, the more focused the dialogue is, and the more coherent various efforts aimed at mitigating unsolicited communications will be.

b. Common understanding of solutions. The challenge here is that there is a whole array of possible solutions (technical, policy, economic, financial, social) and each of them solves only part, or one set of the problems at a particular point in time. It is important to understand that there is no “silver bullet”, but rather, evolving building blocks that can be used in constructing many solutions.

c. Understanding of the differences between common and individual costs versus common and individual benefits when taking appropriate measures. The technology, policy, economic and social building blocks vary in the costs and the benefits they bring individually, for example to a company, institution, user etc., and to the common good of the global Internet and users in general. There are signs these are misbalanced. Understanding these factors and how they are (not) aligned with the needs of governments, Internet users, the business objectives of network operators and other stakeholders and how to share the costs and benefits between them fairly and equitably is crucial for sustained improvements in addressing unsolicited communications.

d. Ability to assess risks. The ability to properly assess risks, including risks to the whole Internet ecosystem, can assist in determining the tools and approaches needed. This requires agreement on metrics and factual data and trends associated with them. This data is also important for the measurement of the effect of such tools once they are deployed and to monitor the changing dynamics of the environment.

e. Identifying good practices. An overview of good or common practices within communities involved in combatting spam seems absent or at least is unfamiliar between communities. Identifying and/or making an inventory of these practices and share them with other stakeholders who have a need for this is useful in developing multi-stakeholder approaches. These future overviews or lists could also be of added value to those starting work to address spam in developing countries.

f. The difference between the developing and developed world. It is important to understand that there is a difference in the challenges they face. The developing world still has to find its way in mitigating spam at its most basic level. The developed world faces the challenge of dealing with professional, mostly malicious spammers that are active from or (ab)using resources in multiple jurisdictions. How can existing, successful anti-spam measures be used as models to follow or implement?

g. Clarification on consumer education, regulation, enforcement and rules. There is a need to define and make an inventory of resentment against governmental involvement concerning the fight against spam, as well as the reasons behind the call for more regulation and the effect of both stances.

h. Understanding of new spamming techniques. New techniques could be presented and explained to governments and agencies on a regular basis, so that they can focus on solutions and educational processes.

i. Understanding of the business case of spammers. Most measures discussed here focus on reactive prevention in one way or another. Could a better understanding of the business case lead to forms of offensive actions against (the tools and finances of) spammers and make a difference? If so, which stakeholders need to be(come) involved in this sort of actions?

j. There is a need for a better understanding of data protection and privacy regulation

in the face of fighting spam and botnets. A major challenge is the exchange of privacy sensitive

data in general and especially between public and private entities, in the fight against (one of the main

causes of) spam. It is of utmost importance to be able to share relevant privacy-sensitive data, like IP addresses, between involved actors. However, there are still important questions and safeguards that need answering, respectively solving, before involved parties on the public and private side can cooperate in the fight against spam and botnets.

k. The balance between fighting spam, freedom of speech, privacy, innovation and doing business. There are thin lines between these elements. Can the different stakeholders find ways in which all can act according to their respective roles, while at the same time strengthen each other's resolve.

Annex 2

Presentation to ISOC CERT & Network Operators' Panel @ AfricaCERT by Neil Schwartzman, Executive Director CAUCE.org on behalf of the M^{3}AAF Foundation
http://www.m3aaf.org

http://cauce.typepad.com/files/isoc-tunis-tunisia-redact.pdf

Annex 3

Full data-set related to botnet infections, chart pp. 12; courtesy of the Composite Blocklist (CBL) / Spamhaus Technology as of September 19, 2015.

Country	Population	Internet Population Percent	Infection Count	Bot Traffic Count	Network Size	% Infected
Laos	6,894,098	14.26%	4,147	29,004	65,536	6.33%
Yemen	24,968,508	22.55%	4,222	1	80,912	5.22%
Vietnam	90,730,000	48.31%	1,176,140	23,834,435	29,189,352	4.03%
Iraq	34,278,364	11.30%	33,938	18,041	845,568	4.01%
Cote d'Ivoire	20,804,774	14.60%	15,015	8,831	403,456	3.72%
Myanmar	53,718,958	2.10%	3,036	45,962	87,808	3.46%
Nigeria	178,516,904	42.68%	30,082	67,170	894,720	3.36%
Kyrgyzstan	5,834,200	28.30%	11,524	854,401	357,120	3.23%
Mauritania	3,984,457	10.70%	801	654	25,088	3.19%
Armenia	2,983,990	46.30%	24,213	663,569	819,200	2.96%
Libya	6,253,452	17.76%	14,899	152,670	514,816	2.89%
Togo	6,993,244	5.70%	139	6,205	5,120	2.71%
Macedonia	2,108,434	68.06%	29,059	208,022	1,118,464	2.60%
Serbia	7,129,428	53.50%	34,251	163,869	1,333,376	2.57%
India	1,267,401,849	18%	1,141,565	6,396,766	45,472,484	2.51%
Azerbaijan	9,537,823	61%	19,063	519,210	786,176	2.42%
Comoros	752,438	6.98%	97	0	4,096	2.37%

Bosnia and Herzegovina	3,824,746	60.80%	16,286	6,578	728,576	2.24%
Cape Verde	503,637	40.26%	386	205	17,408	2.22%
Congo	69,360,118	3%	566	512	26,112	2.17%
Belarus	9,470,000	59.02%	68,277	1,757,521	3,465,472	1.97%
Sri Lanka	20,639,000	25.80%	27,654	10,644	1,425,152	1.94%
Niger	18,534,802	1.95%	420	30	24,064	1.75%
Nepal	28,120,740	15.44%	14,328	4,703	841,984	1.70%
Guinea	12,043,898	1.72%	277	143	16,640	1.66%
Sao Tome and Principe	197,882	24.41%	4	0	256	1.56%
Pakistan	185,132,926	13.80%	259,456	302,704	17,243,438	1.50%
North Korea	25,026,588	%	14	0	1,024	1.37%
Iran	78,470,222	39.35%	292,379	5,479,021	21,684,296	1.35%
Turks and Caicos Islands	33,736	%	148	1,455	11,008	1.34%
Romania	19,910,995	54.08%	118,118	1,532,274	9,063,676	1.30%
Indonesia	252,812,245	17.14%	369,024	1,205,680	28,580,960	1.29%
Cambodia	15,408,270	9%	9,988	166,384	786,253	1.27%
Cameroon	22,818,632	11%	5,047	7,052	409,088	1.23%
Croatia	4,236,400	68.57%	31,283	30,462	2,551,680	1.23%
Palau	21,097	26.97%	47	0	3,840	1.22%

Albania	2,894,475	60.10%	3,178	341,157	263,936	1.20%
Ethiopia	96,506,031	2.90%	3,229	16,239	269,312	1.20%
Algeria	39,928,947	18.09%	115,273	372,050	9,664,256	1.19%
Mali	15,768,227	7%	1,055	1,363	92,672	1.14%
Virgin Islands	104,170	50.07%	368	5,536	32,448	1.13%
Thailand	67,222,972	34.89%	217,031	332,376	19,185,953	1.13%
Afghanistan	31,280,518	6.39%	1,314	2,474	116,480	1.13%
South Sudan	11,738,718	15.90%	116	0	10,496	1.11%
Venezuela	30,851,343	57%	80,310	97,320	7,363,328	1.09%
Somalia	10,805,651	1.63%	154	3,529	14,336	1.07%
Philippines	100,096,496	39.69%	99,171	711,768	9,296,192	1.07%
Morocco	33,492,909	56.80%	105,074	261,022	10,035,712	1.05%
Kazakhstan	17,289,111	54.89%	83,967	3,264,073	8,040,192	1.04%
Bhutan	765,552	34.37%	326	2,005	31,232	1.04%
Uzbekistan	30,742,500	43.55%	6,173	30,382	609,280	1.01%
Mongolia	2,881,415	27%	5,025	165,692	497,920	1.01%
Aruba	103,431	83.78%	548	19,115	56,064	0.98%
Argentina	41,803,125	64.70%	241,591	1,599,308	24,837,520	0.97%
Senegal	14,548,171	17.70%	6,613	12,077	681,728	0.97%
Peru	30,769,077	40.20%	78,280	2,048,778	8,091,136	0.97%

Oman	3,926,492	70.22%	9,346	464	988,416	0.95%
Timor-Leste	1,212,107	1.14%	208	122	22,016	0.94%
Suriname	543,925	40.08%	729	1,174	77,312	0.94%
Lebanon	4,510,301	74.70%	10,442	61,980	1,127,424	0.93%
Palestine	4,294,682	53.67%	10,461	25,109	1,170,944	0.89%
Swaziland	1,267,704	27.10%	374	95	43,520	0.86%
Ghana	26,442,178	18.90%	7,886	10,847	918,784	0.86%
Ukraine	45,362,900	43.40%	146,812	6,409,502	17,483,558	0.84%
Russian Federation	143,819,569	70.52%	577,197	11,205,492	68,918,169	0.84%
Montenegro	621,800	61%	340	841	40,960	0.83%
Syrian Arab Republic	23,300,738	28.09%	7,793	1	966,912	0.81%
Turkmenistan	5,307,171	12.20%	214	2,833	26,880	0.80%
Jordan	6,607,000	44%	9,515	12,664	1,236,992	0.77%
French Polynesia	279,835	60.68%	431	3	56,064	0.77%
Haiti	10,461,409	11.40%	2,352	6,083	306,688	0.77%
Chad	13,211,146	2.50%	47	36	6,144	0.76%
Equatorial Guinea	778,061	18.86%	171	107	22,784	0.75%
Bangladesh	158,512,570	9.60%	16,341	96,266	2,219,532	0.74%
Cocos (Keeling)		%	652	8,024	90,624	0.72%

Islands						
Benin	10,599,510	5.30%	408	14,155	56,832	0.72%
Bolivia	10,847,664	39.02%	12,264	226,914	1,735,424	0.71%
Madagascar	23,571,962	3.70%	1,219	742	173,824	0.70%
Zimbabwe	14,599,325	19.89%	882	1,599	126,208	0.70%
Dominican Republic	10,528,954	49.58%	19,862	20,573	2,847,232	0.70%
Uruguay	3,418,694	61.46%	33,870	70,689	4,876,544	0.69%
Poland	37,995,529	66.60%	159,808	860,339	23,243,688	0.69%
Congo	4,558,594	7.11%	364	887	53,104	0.69%
Gambia	1,908,954	15.56%	417	156	61,952	0.67%
Liberia	4,396,873	5.41%	339	10,277	50,688	0.67%
Saudi Arabia	29,369,428	63.70%	92,897	369,862	13,945,856	0.67%
Tajikistan	8,408,947	17.49%	120	1,100	18,432	0.65%
Egypt	83,386,739	31.70%	168,877	58,879	26,252,288	0.64%
Jamaica	2,721,252	40.50%	1,807	12,209	284,928	0.63%
Central African Republic	4,709,203	4.03%	31	25	5,120	0.61%
Guatemala	15,859,714	23.40%	18,290	31,235	3,023,104	0.61%
Greece	10,957,740	63.21%	44,298	271,130	7,350,473	0.60%
British Indian Ocean		%	18	9	3,072	0.59%

Territory						
Hungary	9,861,673	76.13%	34,243	134,425	6,049,626	0.57%
Malaysia	30,187,896	67.50%	84,693	216,588	15,031,648	0.56%
Bahrain	1,344,111	91.00%	5,610	19,752	1,001,749	0.56%
Burkina Faso	17,419,615	9.40%	788	155	141,824	0.56%
Chile	17,772,871	72.35%	72,458	288,057	13,267,968	0.55%
Malawi	16,829,144	5.83%	695	75	130,304	0.53%
Vanuatu	258,301	18.80%	71	27	13,312	0.53%
Fiji	887,027	41.80%	376	58	73,216	0.51%
Mexico	123,799,215	44.39%	191,715	1,209,029	37,646,752	0.51%
Bahamas	382,571	76.92%	722	18,691	143,360	0.50%
El Salvador	6,383,752	29.70%	1,322	15,195	267,776	0.49%
Angola	22,137,261	21.26%	6,169	5,781	1,251,328	0.49%
Guinea-Bissau	1,745,798	3.32%	5	0	1,024	0.49%
Mayotte		%	5	18	1,024	0.49%
Dominica	72,341	62.86%	4,667	46,574	963,584	0.48%
Moldova	3,556,400	46.60%	9,612	134,609	1,984,595	0.48%
Djibouti	886,313	10.71%	352	48	74,496	0.47%
Sudan	38,764,090	24.64%	10,801	42,894	2,327,048	0.46%
Honduras	8,260,749	19.08%	2,357	9,357	509,184	0.46%

Italy	61,336,387	61.96%	252,054	1,678,910	54,580,059	0.46%
Samoa	191,831	21.20%	229	181	50,432	0.45%
Brunei Darussalam	423,205	68.77%	831	4,885	189,440	0.44%
Mozambique	26,472,977	5.94%	2,362	20,298	558,080	0.42%
Saint Vincent and the Grenadines	109,371	56.48%	31	226	7,680	0.40%
Gabon	1,711,294	9.81%	1,836	1,802	471,552	0.39%
Spain	46,404,602	76.19%	144,279	932,057	37,095,808	0.39%
Uganda	38,844,624	17.71%	1,273	808	336,128	0.38%
Colombia	48,929,706	52.57%	75,797	1,270,182	20,754,408	0.37%
Brazil	202,033,670	57.60%	477,840	2,669,049	134,704,752	0.35%
Namibia	2,347,988	14.84%	1,954	1,332	556,544	0.35%
American Samoa	55,320	%	114	1,046	32,512	0.35%
United Arab Emirates	9,445,624	90.40%	28,207	206,471	8,102,216	0.35%
Macao	575,481	69.78%	1,469	7,066	422,912	0.35%
Tonga	105,782	40%	22	14	6,400	0.34%
Maldives	351,572	49.28%	854	1,035	253,696	0.34%
Qatar	2,267,916	91.49%	5,328	44,842	1,584,137	0.34%
Taiwan	23,359,928	80%	176,312	979,490	53,624,096	0.33%

San Marino	31,637	49.60%	103	1,030	33,536	0.31%
Georgia	4,504,100	48.90%	4,417	106,392	1,441,024	0.31%
Turkey	75,837,020	51.04%	103,756	2,331,958	33,937,488	0.31%
Wallis and Futuna		%	8	0	2,816	0.28%
Lithuania	2,929,323	72.13%	11,127	402,370	3,970,596	0.28%
Puerto Rico	3,548,397	78.78%	2,370	10,588	901,632	0.26%
Andorra	80,153	95.90%	127	248	48,384	0.26%
Ecuador	15,982,551	43%	13,643	243,653	5,226,816	0.26%
Tunisia	10,996,600	46.16%	39,493	288,246	15,511,552	0.25%
Bulgaria	7,226,291	55.49%	29,439	1,385,605	11,686,157	0.25%
Bermuda	65,181	96.80%	628	8,355	254,736	0.25%
Marshall Islands	52,772	16.80%	10	5	4,352	0.23%
Papua New Guinea	7,476,108	9.38%	156	4,069	70,912	0.22%
Tanzania	50,757,459	4.86%	3,806	6,078	1,739,008	0.22%
Greenland	56,295	66.70%	49	0	22,528	0.22%
Austria	8,534,492	81%	50,678	1,160,152	23,376,896	0.22%
Portugal	10,397,393	64.59%	15,947	250,141	7,476,992	0.21%
Israel	8,215,300	71.45%	28,070	843,539	13,177,118	0.21%
Luxembourg	556,074	94.67%	1,568	28,815	744,205	0.21%

Slovakia	5,418,506	79.98%	5,509	125,070	2,628,897	0.21%
Belize	339,758	38.70%	290	748	142,081	0.20%
Cyprus	1,153,058	69.33%	4,046	24,172	1,996,576	0.20%
Saint Martin (French part)	31,530	%	2	50	1,024	0.20%
Lesotho	2,097,511	11%	228	257	118,528	0.19%
Mauritius	1,260,934	41.44%	5,317	15,743	2,797,056	0.19%
Cayman Islands	59,226	74.10%	166	264	87,552	0.19%
Kuwait	3,479,371	78.70%	8,616	107,022	4,813,314	0.18%
China	1,364,270,000	49.30%	1,104,660	2,783,648	624,256,496	0.18%
Kenya	45,545,980	43.40%	8,577	22,206	4,884,480	0.18%
Australia	23,490,736	84.56%	109,330	88,152	62,428,984	0.18%
Ireland	4,612,719	79.69%	9,069	44,867	5,279,896	0.17%
Micronesia	103,903	29.65%	24	0	14,336	0.17%
Germany	80,889,505	86.19%	205,839	790,045	123,761,663	0.17%
Guyana	803,677	37.35%	95	1,809	58,112	0.16%
Jersey		%	269	32,706	165,888	0.16%
Saint Kitts and Nevis	54,789	65.40%	33	2,753	20,736	0.16%
Solomon Islands	572,865	9%	54	4	34,304	0.16%
Grenada	106,303	37.38%	23	844	15,104	0.15%

United Kingdom	64,510,376	91.61%	132,222	665,604	87,831,239	0.15%
Botswana	2,038,587	18.50%	382	3,672	263,168	0.15%
Cook Islands		%	23	1	15,872	0.14%
Sierra Leone	6,205,382	2.10%	57	35	41,472	0.14%
Paraguay	6,917,579	43%	3,749	7,814	2,789,376	0.13%
Trinidad and Tobago	1,344,235	65.10%	980	25,007	739,328	0.13%
Bonaire		%	9	87	6,912	0.13%
Singapore	5,469,700	82%	14,320	155,279	11,487,904	0.12%
Panama	3,926,017	44.92%	4,608	68,396	3,748,672	0.12%
Rwanda	12,100,049	10.60%	570	2,462	477,440	0.12%
Nauru		%	21	1	17,664	0.12%
Slovenia	2,062,218	71.59%	3,138	37,803	2,656,546	0.12%
Estonia	1,313,645	84.24%	1,901	21,896	1,631,761	0.12%
Burundi	10,482,752	1.38%	66	123	56,832	0.12%
Anguilla		%	7	151	6,144	0.11%
Czech Republic	10,510,566	79.71%	11,343	285,030	10,042,508	0.11%
Cuba	11,258,597	30%	281	86	256,256	0.11%
Faroe Islands	49,460	94.66%	67	1,115	62,464	0.11%
New Zealand	4,509,700	85.50%	9,149	11,014	8,572,820	0.11%

Hong Kong	7,241,700	74.56%	27,084	135,590	25,524,354	0.11%
Costa Rica	4,937,755	49.41%	3,685	18,189	3,499,712	0.11%
Nicaragua	6,169,269	17.60%	518	1,767	493,824	0.10%
New Caledonia	266,000	70%	232	2,190	227,072	0.10%
South Africa	54,001,953	49%	48,442	119,252	49,019,709	0.10%
CuraÃ§ao	155,872	%	86	1,905	87,808	0.10%
Guam	167,546	69.27%	212	9,052	241,664	0.09%
Japan	127,131,800	90.58%	231,699	143,538	271,723,601	0.09%
Belgium	11,225,207	85%	12,720	92,332	15,645,496	0.08%
Guadeloupe		%	6	847	7,680	0.08%
Norfolk Island		%	1	0	1,280	0.08%
Latvia	1,990,351	75.83%	2,734	102,819	3,850,253	0.07%
Seychelles	91,526	54.26%	128	391	180,480	0.07%
Malta	427,404	73.17%	620	766	883,200	0.07%
France	66,201,365	83.75%	49,911	326,195	76,140,539	0.07%
French Guiana		%	2	0	3,072	0.07%
RÃ©union		%	36	218	57,344	0.06%
Zambia	15,021,002	17.34%	784	32,715	1,276,928	0.06%
Barbados	286,066	76.67%	4	0	6,656	0.06%
Isle of Man	86,475	%	3	463	5,120	0.06%

Monaco	38,066	92.40%	57	2,111	97,280	0.06%
Sweden	9,689,555	92.52%	13,334	863,640	23,583,569	0.06%
South Korea	50,423,955	84.33%	76,501	1,177,808	138,731,246	0.06%
Saint Pierre and Miquelon		%	2	0	4,096	0.05%
Virgin Islands		%	23	0	57,345	0.04%
Holy See (Vatican City State)		%	1	0	2,560	0.04%
Netherlands	16,854,183	93.17%	11,789	62,235	32,792,987	0.04%
Gibraltar		%	58	66	165,376	0.04%
Switzerland	8,190,229	87%	4,758	169,337	13,806,277	0.03%
Iceland	327,589	98.16%	303	17,727	946,688	0.03%
Canada	35,540,419	87.12%	26,133	312,985	92,987,044	0.03%
European Union	508,308,718	78.10%	12,566	212,011	55,949,914	0.02%
Antigua and Barbuda	90,903	64%	9	23	40,960	0.02%
Norway	5,136,475	96.30%	2,023	699,430	10,480,428	0.02%
Niue		%	31	2	178,560	0.02%
Liechtenstein	37,194	95.21%	53	2,079	306,946	0.02%
Denmark	5,639,565	95.99%	2,277	203,736	14,622,752	0.02%
United States	318,857,056	87.36%	263,171	12,088,485	2,021,114,820	0.01%

Finland	5,463,596	92.38	579	34,224	11,469,440	0.01%

Annex 4

Other Reference Sources of Spam Data

Spamrankings

Spamrankings[60] recaps botnet data from several sources in graph form by monthly measure, highlighting problem areas such as by country and RIR.

Cloudmark Threat Research

Email and SMS filtering company Cloudmark provide a rich source of reference and statistical data[61]. (Sign-up required).

Kaspersky Lab

Kaspersky Lab[62] is an international software security group operating in almost 200 countries and territories worldwide. The company is headquartered in Moscow, Russia, with its holding company registered in the United Kingdom.

Signal Spam

Signal Spam[63] is a not for profit organisation processing spam reports from individual users (mostly in France) and automatically addressing abuse reports to member ISPs, email service providers and partner organisations in other countries (The Netherlands, Switzerland, Japan, Canada, United States, Luxembourg). Members and partners take action according to their activity (ISPs identify botnets, hosting providers identify abusive or abused servers and ESPs unregister victim emails and/or take action against customers abusing their platforms).

Signal Spam publishes a quarterly report on the information received from its users: these reports are based on spam received in users' mailboxes and which they deem unsolicited (commercial, abusive or illegal). Over T2 2015, 72.85% was classified automatically as commercial spam, the remaining being cybercrime related (phishing, scams, malware, etc.)[64].

[60] http://www.spamrankings.net/rankv2/2015/07/01/monthly/countries/volume/cbl/all/regular/

[61] http://www.cloudmark.com/en/s/threat-research and http://www.cloudmark.com/en/s/threat-research/threat-reports

[62] https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015/

[63] https://www.signal-spam.fr/

[64] https://www.signal-spam.fr/sites/default/files/BAROMETRE_7_signal_spam.pdf

Annex 5

Questions in the African IGF survey

The following questions were presented to the IGF Africa members.

Are unsolicited communications a problem in your country/institution?

Does your country have an anti-spam law in place?

Does your country have a computer crime law in place?

Do Internet Service Providers implement best practices to prevent unsolicited communications from reaching end users?

Are ISPs nationally owned or subsidiaries of larger, international corporations?

Are there any public awareness campaigns in your country concerning cybersecurity?

What would you prefer to change first in your country where cybersecurity is concerned?

What does your country need foremost concerning cybersecurity?

If training were to be made available, who need this training?

What should in your opinion be part of this training program?

Are there multi-stakeholder cooperation initiatives in your country or regionally that deal with the mitigation of cybersecurity and/or unsolicited communications?

Are there cyber education tracks in schools or universities in your country or specific digital training courses available?

Do you have one or more cases that could be presented as an example to the world where mitigation of unsolicited communication succeeded, failed or never started while it was intended to do so? Please provide details in the form of a limited sized case study.

Are there reports or statistics concerning unsolicited communications available from your country, e.g. from academia, industry, government, etc.?

Annex 6

Contribution by Karine e Silva of the University of Tilburg

1. Botnets and Spam

Botnets are networks of compromised machines remotely controlled by so-called botmasters[65]. Botnets serve various criminal purposes: DDoS attacks, click fraud, keylogging, spam[66], among others[67]. Spamming practices, in particular, have occupied a prominent place in botnet activities[68]. As noted by experts from Microsoft and UC Berkeley, spam is a driving force in the economics of botnets, serving as a monetization strategy[69]. Botmasters profit from using their network to send spam email (for the purpose of advertising, phishing, malware distribution, etc.) as well as by selling and/or renting their compromised machines to spammers. In a recent study, researchers from UC Santa Barbara and Aachen University defend botnets are essential elements to the success of spam campaigns[70], highlighting the fundamental connection between the two malicious behaviors and the underground transactions conducted by spammers and botmasters. To illustrate this relationship, it is worth to remember the Rustock botnet, an infrastructure once responsible for 1/3 of world's total spam[71]. In short, a holistic approach to fighting against spam must encompass a strategy to mitigate botnets.

2. Fighting Against Botnets: different angles

Mitigation against botnets includes prevention, detection, disruption, and disinfection. Prevention of botnets may refer to increasing the costs of criminality as well as enabling better industry security standards. Detection and disruption depend on the development and deployment of fine-tuned techniques, adapted to the evolving dynamics of mass infections. Finally, disinfection should enable infection removal and vulnerability patching, preventing the re-exploiting of the machine by the same bot family. Clearly, there are several hurdles to achieving each of these mitigation steps and concrete results must combine perspectives from the technical, legal, and policy angles.

2.1 Legal Perspective

[65] A more technical definition calls botnet a large collection of computing systems that is infected with the same piece of malware (bot) and is remotely controlled by one or more attackers (botmasters), using a specific C&C infrastructure, with the purpose of performing malicious actions. See Nuno Rodrigues et al. Characterization and Modeling of Top Spam Botnets. Network Protocols and Algorithms, December 2012, Vol. 4, No. 4. Available at http://www.macrothink.org/journal/index.php/npa/article/view/2058/2400

[66] A standard definition of spam is any unsolicited email sent in bulk. According to Spamhaus, an electronic message is "spam" if (A) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND (B) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent. See https://www.spamhaus.org/consumer/definition/

[67] See https://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets; https://www.honeynet.org/node/52; https://www.fbi.gov/news/news_blog/botnets-101/botnets-101-what-they-are-and-how-to-avoid-them

[68] See http://www.microsoft.com/security/sir/story/default.aspx#!botnetsection_spam

[69] Li Zhuang et al. Characterizing Botnets from Email Spam Records. Proceedings of First USENIX Workshop on Large Scale Exploits and Emergent Threats, April 2008. Available at http://www.eecs.berkeley.edu/~tygar/papers/Botnets.pdf

[70] Gianluca Stringhini et al. The Harvester, the Botmaster, and the Spammer: On the Relations Between the Different Actors in the Spam Landscape. ASIACCS'14, June 2-3, 2014, Kyoto, Japan. Available at http://www0.cs.ucl.ac.uk/staff/G.Stringhini/papers/harvesters-asiaccs2014.pdf

[71] See http://krebsonsecurity.com/2012/02/whos-behind-the-worlds-largest-spam-botnet/; http://www.cnet.com/news/report-spam-down-33-percent-after-rustock-takedown/

Massive botnet takedowns in recent years have three common characteristics: one, close collaboration between public and private sector; two, cooperation between foreign law enforcement officers; and they are temporary measures, and in most cases the botnet has come back up. The disruptions of Gameover Zeus[72], ZeroAccess[73], BeeBone[74], Ramnit[75], and others, demonstrate the paramount influence of these two elements, further discussed below.

2.1.1 Public-private collaboration.

As noted by Germano[76], while industry has expert insight and knowledge for combatting threats, public authorities hold prerogatives for investigation and prosecution of crimes, and for providing statutory protection in the context of information sharing. Ideally, a combination of both skills and mandates would support further results in fighting against botnets than isolated efforts can yield. Despite its advantages, in most countries public-private collaborations are yet to substantiate their legitimacy, effectiveness, and accountability. In other words, it is often unclear whether public-private collaborative efforts conform to the rule of law, whether they concretely translate into better results, and whether actors are held accountable for misuse of power or fundamental rights violations. Solutions to these barriers may include the adoption of clear frameworks to promote transparency, trust, and accountability of public-private collaborations in face of citizens and/or specialized multi-stakeholder committees. Finally, there is a great need for empirical research on the effectiveness and efficiency of public-private collaborative efforts, which can help demonstrate the added value of such initiatives and encourage government, society, and industry support.

2.1.2 International cooperation in criminal matters.

Contrary to law enforcement powers, online activities are characterized by the fluidity and thinning of geographical borders. In cyberspace, communication is ubiquitous and malicious users take advantage of this flexibility to target victims in various parts of the world, while subjecting themselves to minimum risk. In this context, international cooperation is key, as it enables actors to bring together pieces of the puzzle that would be otherwise out of reach. In mass-scale contaminations, it is very common for evidence to be spread over different countries, and in the possession of various companies and law enforcement agencies. By combining efforts, law enforcement agents are able to join their powers and compensate for the limits of territorial jurisdiction. While the exchange between EUROPOL and the FBI has strengthened international cooperation involving EU Member States and the U.S., a systematic framework for cooperation in cybercrime is still lacking. The Council of Europe Convention on Cybercrime is a landmark on international cooperation against cybercrime, but limited to an array of mostly European countries. There is thus a need for an international instrument representative of the demands of different countries, capable of facilitating the investigation and prosecution of cybercrime at a global level, while ensuring balance with human rights.

[72] https://www.europol.europa.eu/content/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

[73] https://news.microsoft.com/2013/12/05/microsoft-the-fbi-europol-and-industry-partners-disrupt-the-notorious-zeroaccess-botnet/

[74] https://www.europol.europa.eu/content/international-police-operation-targets-polymorphic-beebone-botnet

[75] https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation

[76] Germano, Judith. Cybersecurity Partnerships : a new era of public-private collaboration. The Center on Law and Security, New York University, 2014

Annex 7

Contribution of Prof. D. Svantesson

Fighting unsolicited communications and territoriality[77]

Dan Jerker B. Svantesson (2015) has provided the following excerpt as a case study for the BPF that considers the issue of territoriality.

Internet jurisdiction – overcoming the problems by abandoning territoriality

The issue of jurisdiction over online activities has been controversial since the earliest days of large scale Internet usage. Here I will put forward a proposal that hopefully can represent a step towards a solution.

The territoriality principle – the idea that a State has the exclusive right to regulate all that occurs in its territory for the simple reason that it occurs in its territory – dominates our contemporary thinking about jurisdiction. However, it is poorly equipped for today's modern society characterised by constant, fluid and substantial cross-border interaction, not least via the Internet.

Despite its long history, the time has come to abandon territoriality as the core principle of jurisdiction. Applied to the Internet, it quite simply does not work. After all, it is not always possible to point to where events occur online. Only by legal fictions, stretching reality beyond recognition, can we say that a person was defamed online at a specific place, that copyright was violated at a particular location online, that the cybercrime activity takes place at a particular place and so on.

Elsewhere, I have advocated that we should replace our focus on territoriality with three principles – principles that can represent the jurisprudential core of jurisdiction both online and off-line:

In the absence of an obligation under international law to exercise jurisdiction, a State may only exercise jurisdiction where:

(1) there is a substantial connection between the matter and the State seeking to exercise jurisdiction;

(2) the State seeking to exercise jurisdiction has a legitimate interest in the matter; and

(3) the exercise of jurisdiction is reasonable given the balance between the State's legitimate interests and other interests.

Despite its highly theoretical aim, the proposed paradigm shift provides benefits also on the practical level. Done carefully and diligently, this development would see no practical change in non-controversial areas of jurisdiction. The absolute majority of cases, both offline and online, will involve a similarly natural connection between territoriality, on the one hand, and substantial connection and a legitimate interest, on the other hand.

At the same time, the proposed paradigm shift would see us being much better equipped to address what are now controversial areas. It will allow us to think more creatively rather than just mechanically binary. It would, for example, free us from the thinking that State A always must have a possible jurisdictional claim over all aspects of data that happened to be located on a server located in State A; we would be looking for connections and interests rather than engaging in sterile searches for 'where' events occur online.

[77] For an introduction: Do we need new laws for the age of cloud computing? Dan Jerker B. Svantesson (2015) https://agenda.weforum.org/2015/02/do-we-need-new-laws-for-the-age-of-cloud-computing/ Accessed 29-08-2015

So how can we achieve this paradigm shift from territoriality to the three core principles advocated here? The reality is that international law develops, at least in part, in mysterious ways, and the first step required is that we all stop taking for granted that territoriality necessarily must be the central pillar in our thinking about jurisdiction. Everyone, from academics to businesses, from judges to bloggers, can play a role in this[78].

Professor Dan Jerker B. Svantesson Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council.

[78] For those wanting to learn more see also https://www.asil.org/blogs/introduction-symposium-rethinking-state-jurisdiction-Internet-era

Annex 8

To Champion a Safe and Secure "Next Generation" Internet

The "bandwidth revolution" in emerging online countries is providing high-powered global Internet access to millions of users for the first time and vastly changing the anatomy of the connected world. Unfortunately, we also know that when a new region brings significant bandwidth online, an onslaught of criminals follows, rushing to establish their abusive and illegal practices in new unprotected territory. While broadband access brings the promise of both economic and personal growth to these regions, it also opens the door to spammers and cybercriminals looking to set up new cyber-breeding grounds and expand their illicit operations around the world.

This raises an important question for the rest of the world: Will these rapidly evolving countries come online with all of the advantages from the industry's decades of hard-won expertise in protecting end-users or will they unwittingly go through the same mundane struggles and ordeals, starting from scratch in learning about spam, malware, bots, DDoS attacks and other threats?

This is an educational and technology issue with global economic repercussions. As we all know, the Internet is a borderless entity and along with the communications and monetary exchange it enables, there also is an endless stream of spam, malware and fraudulent messaging surreptitiously flowing from country to country. Spam generated in one country very often targets users on the other side of the world.

For everyone involved, it is vital to prevent the establishment of new spam and cybercrime havens. Without the necessary understanding to protect their end-users, these developing countries will never fully recognize the benefits of the global online economy. If spammers and cybercriminals are allowed to subsist in these regions, users in countries with existing robust Internet economies will also be severely harmed.

Recognizing the hazards, many developing countries have asked for assistance with training, best practices and technical support to combat spam and abuse on their networks.

Training Goals

We should advocate safe and effective Internet access for users in all countries with all the benefits of participating in the online community, including economic growth and improved wellbeing. To this end, we should promote the voluntary implementation of known anti-abuse best practices for network and hosting operations to fight online abuse such as spam, bots and malware, and the continual updating of these practices with new techniques and technologies. This encourages reliable, safe and sustainable access to the global Internet community for business, governments and users.

The goals are:

1. Help emerging online countries become functional and safely-engaged participants in the global community by training industry ecosystem producers - such as ISPs and network operators, email service providers, technically-focused government agencies and NGOs — to avoid spreading unwanted traffic and other threats to the Internet community. This includes training to reduce the distribution of abusive messaging on all platforms and to abate related threats like bandwidth hijacking;

2. Provide training to help emerging online countries protect their own citizens from Internet abuses, such as spam, phishing, malware, bots and other threats.

How to Achieve These Goals?

1. Provide experts to speak on best practices and topical work that already exists within M^3AAWG and other respected anti-abuse organizations.

2. Develop programs and curriculum for basic "101 courses" since many best practices assume certain technical and operational knowledge, that take network administrators and anti-abuse personnel to the next level by teaching how to operate and manage safe networks.

3. Train the trainers on anti-abuse best practices so that the instruction lives on and is not "one shot work."

4. Provide training at hosted training venues such as the ISOC Combating Spam Project workshops or M^{3}AAF[79] organized workshop/training meetings.

5. Develop partnerships with other organizations in related work to expand the M^{3}AAF outreach effort.

6. Develop relationships with "champions on the ground' in each region as a channel for sharing future M^{3}AAWG and other organizations' best practices.

Why Now?

While countries around the world are looking to join the global online economy, a number of public policy and governance events are underway that could have a profound effect on the technical community. Currently, there are major International Telecommunications Union (ITU) initiatives under consideration focusing on spam and Internet governance that also address the roles of the ITU and the Internet community.

[79] http://www.m3aaf.org

Annex 9

Case Study: Implementation of New Zealand legislation[80]

In May 2004, the Ministry of Economic Development (now the Ministry of Business, Innovation and Employment) released a discussion paper entitled "Legislating Against Spam"[81]. This document was the first step in the Government's proposal to address the specific problem of spam through legislation[82]. The discussion paper provided a background on spam, the relevant New Zealand legal framework – namely the Privacy Act 1993 and Harassment Act 1997, and detailed legislative issues for anti-spam legislation. The issues that were detailed included the legislative scope (what type of messages should be regulated), consent (for example, whether an opt-in or opt-out approach be adopted), transparency (the need for sender details or an unsubscribe facility), privacy (the use of address harvesting software and address harvested lists) and enforcement (for example, whether the legislation should be civil or criminal).

The Government wanted to benefit from widespread input prior to drafting the legislation. Therefore, the discussion paper posed several high-level questions, and sought consultation through submissions from those interested. These included the Direct Marketing Association, Email Service Providers, Internet Service Providers and Mobile Networks. There were a number of key outcomes from the submission stage, for example all of the respondents considered spam to be an important issue, and spam had markedly eroded people's confidence in the reliability of email. Furthermore, almost all respondents agreed that legislation was required. The submissions were taken under consideration; the legislation was drafted in June 2005[83].

The Unsolicited Electronic Messages Bill was formally 'introduced' into Parliament on 28 July 2005.

In order to properly frame the legislation, the Government had to formally scope the nature and magnitude of the problem and ascertain the need for action. They compiled the examination of the issue into a "regulatory impact and compliance cost statement"[84] which formed an integral part of the Bill. Considerations for the cost statement included:

- The Government's 2005 Digital Strategy[85].
- Metrics on the amount of spam relevant to total email traffic in New Zealand.
- The potential economic impact relevant to the loss of productivity (in a workplace), loss of confidence in dealing with business and other communications online, as well as the consumption of network and computing resources.
- New Zealand laws that might already have contained aspects of spam regulation.

[80] This case study outlines how the Unsolicited Electronic Messages Act 2007 developed in New Zealand and relevant considerations. It is not meant to be prescriptive, but rather a high-level overview. Inclusion in the Internet Governance Forum Best Practice Document can provide legislators in developing and developed economies with ideas, possible action points and suggestions should they want to implement their own legislation. The case study was provided by Peter Merrigan of the Department of Internal Affairs of New Zealand.

[81] MED Discussion Paper 2004, http://www.politechbot.com/docs/new.zealand.spam.051804.pdf

[82] Page 4 of the discussion paper noted the high-level extent of the problem as "Major problems caused by spam are breaches of privacy and a lowering of user confidence, deceptive practices, illegal or offensive content such as pornography and scams, threats to network integrity and security, desired email getting blocked by anti-spam technologies, and the financial costs imposed on ISPs and users".

[83] Unsolicited Electronic Messages Bill, Bill 281-1, www.parliament.nz/resource/en-NZ/00DBHOH_BILL6896_1/1dba471cd026848653fca0e312fd458372707de9

[84] IbIdem

[85] The Digital Strategy: Creating Our Digital Future, http://workspace.unpan.org/sites/Internet/Documents/UNPAN039463.pdf

- Self-regulation measures within the industry.
- Risks of not implementing an anti-spam law – for example, New Zealand becoming a safe haven for spammers.
- What other countries had implemented by way of anti-spam law.

Through the Unsolicited Electronic Messages Bill, the Government also created objectives in accordance with its Digital Strategy. This identified the individual benefits of implementing an anti-spam law (the benefits for Government, businesses, Internet Service Providers and society), and captured the results of the initial consultation via earlier submissions.

In 2005, the Ministry of Justice considered whether the Unsolicited Electronic Messages Bill was consistent with provisions of the New Zealand Bill of Rights Act 1990, such as the right to freedom of expression. It concluded that the Bill was consistent.

The Bill went through the required three 'readings' in Parliament - the first reading on 13 December 2005, the second reading on 5 December 2006, and the third reading on 27 February 2007. There were a number of amendments recommended and actioned through this process, prior to the third (and last) reading in 2007[86].

The Unsolicited Electronic Messages Bill became law on 5 March 2007 and came into force six months later.

While the Ministry of Business, Innovation and Employment administers the Unsolicited Electronic Messages Act 2007[87], the Department of Internal Affairs was selected as the enforcement department. The Electronic Messaging Compliance Unit (EMCU) was set up within Internal Affairs to regulate the Act.

The Act is a civil piece of legislation rather than criminal. It provides provisions for the sending of commercial electronic (email, SMS, fax and instant messaging) messages with a New Zealand link. While there is generally a high domestic compliance rate toward the Act , there remains the challenge of regulating unsolicited commercial electronic messages (spam) coming into New Zealand from offshore; spam that can be deceptive, harmful and fraudulent.

[86] Ministry of Justice, http://www.justice.govt.nz/policy/constitutional-law-and-human-rights/human-rights/bill-of-rights/unsolicited-electronic-messages-bill

[87] The Unsolicited Electronic Messages Act 2007, http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html?src=qs

Annex 10

The Spam fight in Brazil. Contribution by Cristine Hoepers, general manager Cert-Br[88]

Internet Governance Context

Fighting spam has been a topic debated on Internet Governance related forums in the past 15 years. The reasons for this topic being present on discussions for so long are as diverse as the ways we can research the topic. The efforts to stop spam can be approached from technological, legal, political and social aspects.

In Brazil the strategies to fight spam are the result of a coordination effort by the Brazilian Internet steering Committee (CGI.br) Anti-Spam Task Force (CT-Spam). This effort involved bringing into the discussion of possible solutions dozens of Telecommunications Companies, thousands of Internet Service Providers, Consumer Protection organizations, representatives from the Civil Society and the Academia, as well as the technical staff of NIC.br/CGI.br.

The success of this initiative points to the fact that a multi-stakeholder collaboration is the best strategy to effectively implement security policies, deal with cybersecurity related issues and establish trust on the Internet.

A Brief History

The CT-Spam was created in 2005, as one of the CGI.br initiatives, with the objective to deal with the obvious problems that spam was causing to the Internet in Brazil and abroad. This effort was proposed and Coordinated by the CGI.br Board Member Henrique Faulhaber.

Since its inception the CT-Spam is working with actors from different sectors to raise awareness about their roles and the importance of implementing anti-spam policies and technologies. At the same time it was working to provide awareness and education to end users about safety and security on the Internet.

Different Approaches to Different Problems

After several studies conducted by CERT.br it was clear that the major spam problem in Brazil was the abuse of the country's broadband infrastructure by international spammers, usually abusing open proxies or through botnets, both in end user infected computers.

The impacts of inaction were already being noticed by consumers and access providers, specially:

- the inclusion of whole broadband providers' IP ranges in blacklists and;
- in some cases the blacklisting of the whole country;
- raise in operational costs, invariably transferred to consumers;
- instability of the broadband connectivity, as the spammers were using all the available upload bandwidth;
- international effects, as the spam messages were both originated and destined to other countries.

Nevertheless, there were also other issues to be dealt with, especially:

- educating the end users on how to identify spams, especially those related to malware and phishing;

[88] See also http://antispam.br/en/

- raising awareness of the e-mail marketing sector about the importance of best practices, data protection and privacy issues related to e-mail marketing;
- studying a legal framework for Brazil.

As the result of the multi-stakeholder discussions the CT-Spam worked to implement different policies and technologies for the different aspects of the spam problem. Among these activities the main areas of work were:

A) Antispam.br Website

A Web Portal was created with information for end users, e-mail and connectivity providers. For end users the information is focused on explaining what is spam, the risks of malware and fraud and how to avoid these risks. This information is presented also in four videos. For the e-mail and connectivity providers the focus is on several anti-spam techniques, including DKIM, SPF, Greylisting and Port 25 Management.

B) Port 25 Management

To prevent broadband infected computers to perform direct delivery of spam our studies showed that the most effective countermeasure would be to implement Port 25 Management. This is the term used to refer to the policies and technologies implemented in residential or dynamic IP address spaces to enforce the separation between message submission and message transport.

This measure was formally recommended by CGI.br in its Resolution "CGI.br/RES/2009/02/P". This recommendation led to two other important documents: a formal statement from the Consumer Protection Department of the Ministry of Justice, analyzing the consequences do consumers and recommending its adoption; and the Cooperation Agreement, signed by CGI.br, Anatel, the Telecommunication Companies Union and the ISP Associations, with the details of the implementation process.

The implementation of this technique alone was responsible for taking Brazil out of almost all existing lists of "Top Countries" originating spam.

The port 25 management adoption process was characterized by an intense collaboration coordinated by the Brazilian Internet Steering Committee - CGI.br - among actors seeking to satisfy the public interest. The implementation of such a Brazilian multi-stakeholder and multi-participative Internet governance model left no doubts about its success. CGI.br Councilor Eduardo Levy, who is the President of the Telecommunication Companies Union, acknowledged this result in his interview to specialists documenting the project:

"Well, this is complex; yet it is beautiful from a democratic point of view and for the various forces that acted in it; and it’s better still because it was the whole society who benefited in the end. Nothing was strong enough to prevent society from gaining. To me, personally, and to the whole telecom sector, being part of this process and being able to publicize it, made us very proud."

C) Anti-Spam Legislation

Anti-Spam Legislation - CT-Spam promoted a legal study of all international anti-spam laws, as well as all the laws being proposed in the Brazilian Congress. At the end of this study a new text for a legislation was proposed, based on the opt-in principle. This text is the base of the current anti-spam bill being currently considered in the Congress.

D) E-mail Marketing Self-Regulation Code

This initiative arose from the perception that more than working on new legislation, there was a need to establish standards and best practices to guide email marketing companies. This Code details how to send e-mail marketing respecting opt-in principles, e-mail reputation best practices and data privacy and protection related to e-mail address lists.

Annex 11

The Abuse Information Exchange in the Netherlands

The Abuse Information Exchange is an association of Dutch Internet providers and other stakeholders, established as initiative from private parties to effectively share and use information on botnet infections and other Internet abuse by centrally collecting, analyzing and correlating information from various national and international sources. Therefore the Abuse Information Exchange can be defined as the National Abuse Report Clearing House. This initiative has been established in 2012 and was supported by the Dutch Ministry of Economic Affairs that provided a grant to start this initiative.

Botnet software usually causes few problems on the infected computer; often the infection is not detected at all. But botnets can cause great inconvenience and harm to others. According to research from the Technical University of Delft 5 to 10% of all computers in the Netherlands are infected with a botnet infection every year.. Current members of the Abuse Information Exchange are Internet service providers Tele2, KPN, Solcon, RoutIT, Zeelandnet, XS4ALL, Ziggo, and Surfnet and SIDN (Foundation for Internet Domain Registration in the Netherlands). Recently, the hosting providers association ISPConnect and the Dutch Hosting Providers Association (DHPA) have become members of the Abuse Information Exchange thereby extending the scope of the Abuse Information Exchange to almost all Internet access and hosting providers in the Netherlands. The association meets on a regular basis with the Dutch National cybersecurity Centre (NCSC) to give updates about the progress that has been made. The association also meets with other stakeholders such as academics and ministries to further improve Internet safety.

The central software of the association, called AbuseHub, receives information from a large number of reliable notifiers. It was specifically built to be able to analyze great amounts of data, in order to allow the member ISPs to act swiftly in case of a botnet infection on computers in their networks. Abusehub analyses the information from notifiers and forwards it to the specific member ISPs, who use the notifications to warn their customers about botnet infections on their machines. Anonymized statistical data on the received Abuse reports is available through the self-care environment. This combination of both a community and a system (Abusehub) provides a powerful and concrete mechanism to increase the maturity of the Internet safety and the general Abuse handling in the Netherlands.

A recent report of the Technical University of Delft has indicated that The Netherlands scores above average in terms of botnet control[89]. Also, the report indicates that Dutch ISPs perform above average compared to ISPs in other countries. Especially the Internet providers that are members of the Abuse Information Exchange have improved their performance. Their combined share in botnet infections has fallen from 80 % in 2010 to 63 % in 2014. The most infected non-members are smaller ISPs that have not (yet) joined AbuseHub and hosting providers. The fact that the hosting providers association ISPConnect and DHPA have recently joined the Abuse Information Exchange is an effective step to further increase the maturity of the Internet safety and the general abuse handling in the Netherlands.

[89] Evaluating the Impact of AbuseHUB on Botnet Mitigation Interim Deliverable 1.0 PUBLIC VERSION Giovane C. M. Moura, Qasim Lone, Hadi Asghari, and Michel J.G. van Eeten, Economics of CyberSecurity Group, Faculty of Technology, Policy, and Management, Delft University of Technology, March 24, 2015. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2015/04/10/evaluatie-the-impact-of-abusehub-on-botnet-mitigation/evaluatie-the-impact-of-abusehub-on-botnet-mitigation.pdf

Annex 12

Other examples of security initiatives that impact unsolicited communications

Advanced Cyber Defense Center (ACDC)

The ACDC program, which was mentioned in the 2014 BPF report, ended on 1 August this year. One of the goals of this EU program was to establish 8 botnet mitigation centres in Europe. At 1 August there were 12 botnet mitigation centers in Europe, although not all ACDC partners, including Finland and The Netherlands. Some of these centers are established within CSIRT, e.g. Croatia and Spain, others with a regulator, such as Finland and others are public – private initiatives, such as in Germany, France and the Netherlands.

Check and secure

Check and secure[90] is an online initiative "powered by" a German cybersecurity company called Cyscon, that, according to its website, cooperates with a host of partners including government, anti-virus companies, ISPs, mobile companies and with the anti-botnet initiatives ACDC and Botfrei.

Check and secure is an online tool that allows end users to check, for free, whether their IP address is sending unsolicited communications. If a positive response is received the end user is warned and pointed towards a mitigation tool. The tool also checks whether the most common software programs have the most recent updates installed. If not, it recommends that this be done straight away.

Internet.nl

Internet.nl[91] is an initiative of the Dutch Platform Internetstandaarden and was launched at the Global Conference on Cyber-Space in April 2015. A combination of different organizations representing the Internet industry, government, NGOs and Internet community joined to make the initiative a success. Its aim is to present end users the option to find out whether their Internet connection uses the latest Internet standards by testing the Internet connection and providing responses to the following questions:

- How secure is my email?
- Is IPv6 offered?
- Is DNSSEC used?

One of the features of Internet.nl is that "concerned" end users are encouraged to contact their respective providers seeking answers to questions about the safety and reliability of their Internet connection. The technique behind the website is available for organisations in other countries that are willing and able to run the tool.

Stop. Think. Connect.

In this awareness raising program based in the United States, the Anti-Phishing Working Group, the National cybersecurity Alliance and the Department of Homeland Security work together to raise the awareness of Internet users and present them with ways to be safer on the Internet. In its own words:

"Take security precautions, understand the consequences of your actions and behaviors and enjoy the benefits of the Internet.

[90] https://www.check-and-secure.com/start/

[91] https://www.Internet.nl/

STOP: Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

CONNECT: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

Protect yourself and help keep the web a safer place for everyone."[92]

The program advocates itself internationally and is adopted in several countries outside the United States.

Global Forum on cybersecurity

The Global Forum on Cyber Expertise (GFCE) was launched at the Global Conference on Cyber-Space 2015[93] and currently has 48 international members from governments, IGOs and private sector. It was set up to assist in the global effort to strengthen cyber capacity. It is a key initiative which gives momentum to global cyber capacity building and makes technical expertise and new funding available. The GFCE is designed as a pragmatic, action-oriented and flexible platform for policymakers, practitioners and experts from different countries and regions. Its goal is to share experiences, identify gaps in global cyber capacities, and to complement existing efforts in capacity building. Under the umbrella of the GFCE, members are pushing forward capacity building initiatives which are centered on the four main themes of the GFCE; cybersecurity, cybercrime, e-governance and data protection[94].

Initiatives are brought forward by one or more organisations from different regions and/or stakeholder communities who can in different constellations lead, fund, discuss, give or receive these initiatives. The GFCE is looking for action programs.

This BPF concludes that there is a need and want for practical training at the technical level in Africa and given the potential of the GFCE platform, sees an opportunity for involved stakeholders to connect there.

NaWas

The Dutch national scrubbing centre is an initiative of an association of hosting centres called Nationale Beheersorganisatie Internet Providers (NBIP). This association started because of the legal obligation of Internet providers to have taps placed in their networks when a court order allows law enforcement to do so. "Because smaller organizations had difficulties complying with the Dutch telecom laws, a Shared Service Center was constructed"[95]. In 2013 NBIP thought up the concept of organisations working together to mitigate DDoS attacks. Only a few months later it opened its functionalities. In the initiative stakeholders from different communities participate. With all the botnet traffic going into NaWas other possibilities arose. "In 2015 the NBIP started research together with the University of Amsterdam to find out if pattern recognition for DDoS mitigation could work and to find out which "DDoS cannons" should be targeted first by law enforcement agencies"[96]. The next step foreseen step is NaWas-LEA cooperation. NaWas is a public - public participation.

DINL

[92] http://www.stopthinkconnect.org/ (accessed 25-09-2015)

[93] https://www.gccs2015.com/

[94] Taken from an email to W. de Natris from the GFCE, shared with the list. The website is launched: http://www.thegfce.com/

[95] NaWas case study. NBIP (2015), provided by Ludo Baauw.

[96] Ibidem

DINL, the Digital Infrastructure Association NL, is the representative and voice of providers of Digital Infrastructure in the Netherlands. Participants of DINL are: AMS- IX (Amsterdam Internet Exchange); DDA (Dutch Datacenter Association); DHPA (Dutch Hosting Provider Association); ISPConnect; Stichting NLnet; SIDN (Foundation for Internet Domain Registration in the Netherlands) and SURFnet. It is established to voice the core messages of the participants, who come from different backgrounds in the Internet industry, and thus influence government policies.

This initiative is beyond the topic of mitigating unsolicited communication. However, this BPF noticed that nearly all members of DINL are involved in one or more mitigation actions against unsolicited communication, which makes DINL a potential partner to discuss this topic with. The full contribution of DINL can be found in Annex 14 to this report[97].

Working group for Organizing Coordinated Disclosures (OCD)

This informal Workgroup was created during the Global Conference on Cyber-Space[98], following the parallel session responsible disclosure[99]. It has as members from the hacker community, large corporations, a district attorney, policymakers, representatives of CSIRT and others. The purpose of the Working group is to find a way to allow researchers, i.e. ethical hackers, to do their work, without fear of prosecution or persecution, while at the same time protecting the vendors from unnecessary actions, exposure and/or damage. It is one of the first active initiatives in the Global Forum on Cyber Expertise, sponsored by governments and industry. The full text of the contribution is in Annex 15 to the report[100].

CyberGreen

CyberGreen seeks to aggregate data and provide metrics to measure risk conditions globally through collaboration and data sharing partnerships. National CERTs are partnering with CyberGreen to share and consume risk metrics. A central goal for CyberGreen is to assist policymakers in identifying areas of the Internet that need additional attention and resources due to their risk conditions. CyberGreen would partner and assist the existing organizations that play a significant role in remediation efforts such as cleanups, botnet take downs and identifying and remediation vulnerable node. National CERTs and Network operators are encouraged to sign up and explore CyberGreen's portal to give CyberGreen guidance and feedback on what would most help for CERT engage their policy makers[101].

CyberGreen is in need of funding in order to carry on its work.

[97] DINL has presented itself at the IGF on one of the open forums. See https://igf2015.sched.org/event/4bRD/open-forum-dinl-digital-infrastructure-association

[98] https://www.gccs2015.com

[99] Find the session description here: https://www.gccs2015.com/programme?programme=2 You can view the video here: https://www.youtube.com/watch?v=INpAGZUr5TE&t=9685

[100] The contribution is made by Mr. Inbar Raz, member of the Working group.

[101] http://stats.cybergreen.net/

Annex 13

Public - Private Partnerships

Limited-Term partnerships

The Canadian Task Force on Spam

2005-2006

Review global messaging abuse from the Canadian perspective, develop best practices and recommendations, report to Minister of Industry[102]. The task force held multi-stakeholder participation.

DNSChanger Working Group (2010-2012)

DNSChanger was a DNS hijacking Trojan active from 2007 to 2011. The work of an Estonian company known as Rove Digital, the malware infected computers by modifying a computer's DNS entries to point toward its own rogue name servers, which then injected its own advertising into Web pages.

The DNS Changer Working Group (DCWG)[103] was created to help remediate Rove Digital's malicious DNS servers. The DCWG is an ad hoc group of subject matter experts, and includes members from organizations such as Georgia Tech, Internet Systems Consortium, Mandiant, National Cyber-Forensics and Training Alliance, Neustar, Spamhaus, Team Cymru, Trend Micro, and the University of Alabama at Birmingham working in collaboration with the FBI, the NASA-OIG and Estonian police.

Longer term partnerships

M^{3}AAWG

The Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG)[104] is an international non-profit, industry-led organization founded to fight online abuse such as botnets, phishing, fraud, spam, viruses and denial-of service attacks that can cause great harm to both individuals and national economies. M^{3}AAWG draws technical experts, researchers and policy specialists from a broad base of Internet service providers and network operators representing over one billion mailboxes, and from key technology providers, academia and volume sender organizations. The multi-disciplinary approach at M^{3}AAWG includes education, advice on public policy and legislation, development of industry best practices, guidance in the development of industry standards, and the facilitation of global collaboration.

FIRST

The Forum of Incident Response and Security Teams (FIRST)[105] an organization dedicated to incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

[102] http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00317.html

[103] http://www.dcwg.org

[104] http://M3AAWG.org

[105] http://first.org

It currently has as Special Interest Group (SIG) on the topic of this BPF. Its goal is to "share experiences about botnet mitigation and remediation and to identify different approaches and best practices that can be implemented to address this problem"[106].

Anti-Phishing Working Group

APWG[107] is the worldwide coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors. APWG's membership of more than 2000 institutions worldwide is as global as its outlook, with its directors, managers and research fellows advising: national governments; global governance bodies like ICANN; hemispheric and global trade groups; and multilateral treaty organizations such as the European Commission, Council of Europe's Convention on Cybercrime, United Nations Office of Drugs and Crime, Organization for Security and Cooperation in Europe and the Organization of American States. The APWG is also on the steering group of the Commonwealth Cybercrime Initiative of the Commonwealth of Nations.

Team Cymru

Team Cymru Research NFP[108] is an Illinois non-profit and a US Federal 501(c)3 organization. "We are a group of technologists passionate about making the Internet more secure and dedicated to that goal. We work closely with and within Internet security communities, as well as with all manner of other organizations - after all, almost every organization in the modern world is connected to the Internet in some way or another, and they all need help to ensure that their parts of the network remain safe and secure".

London Action Plan

The London Action Plan (LAP)[109] was founded in 2004 with the purpose of promoting international spam enforcement cooperation and address spam-related problems, such as online fraud and deception, phishing, and dissemination of viruses. Since inception, LAP has expanded its mandate to include additional online and mobile threats, including malware, SMS spam and Do-Not-Call.

LAP membership includes representatives from the government regulatory and enforcement community and interested industry members. Through annual meetings and bimonthly teleconferences, members stay connected and share information that is critical for any organization engaged in anti-spam regulation and enforcement.

National Cyber-Forensics & Training Alliance

The National Cyber-Forensics & Training Alliance (NCFTA)[110] is a non-profit corporation focused on identifying, mitigating, and ultimately neutralizing cybercrime threats through strategic alliances and partnerships with Subject Matter Experts (SME) in the public, private, and academic sectors.

Through NCFTA initiatives, hundreds of criminal (and some civil) investigations have been launched, which otherwise would not have been addressed. Currently, NCFTA has aided in successful prosecutions of more than 300 cyber criminals worldwide.

INHOPE

INHOPE[111] is an active and collaborative network of 51 hotlines in 45 countries worldwide, dealing with illegal content online and committed to stamping out child sexual abuse from the Internet.

[106] https://www.first.org/ (Accessed 25-09-2015)
[107] http://www.antiphishing.org
[108] http://www.team-cymru.org
[109] http://londonactionplan.org
[110] http://www.ncfta.net
[111] http://www.inhope.org

Annex 14

Contribution of DINL, Digital Infrastructure Association of the Netherlands.

by Michiel Steltman, Director of DINL

DINL, the Digital Infrastructure Association NL is the representative and voice of the providers of Digital Infrastructure in the Netherlands. Next to the Rotterdam Harbor and Schiphol Airport this sector is referred to as the Netherland's Third Mainport. It forms the heart of the Dutch online economy. Because it hosts the AMS-IX, the world's largest Internet exchange, it plays a key role in the global Internet.

Participants of DINL are: AMS- IX (Amsterdam Internet Exchange); DDA (Dutch Datacenter Association); DHPA (Dutch Hosting Provider Association); ISPConnect; Stichting NLnet; SIDN (Foundation for Internet Domain Registration in the Netherlands) and SURFnet.

What are DINL's core messages?

A Free open and safe Internet is the basis and requirement for economic growth. Digital Infrastructure is the basis and condition for:

- NL digital gateway to Europe, as the ideal location for online services[112];
- Tomorrow's ICT in the cloud;
- Digital Innovation and transformation;
- The knowledge-based economy of tomorrow.

Core themes of DINL - with respect to government policy ; and the open forum on IGF:

Is the ambition to develop, in the public domain, general policy principles to match with the (new) laws and regulations and Government operation in the digital domain. That is also, in our view, the biggest challenge for all countries. As policy principles we use:

- Free, open and safe Internet (GCCS2015[113] and WRR report[114];
- Multi-stakeholder approach on all (3) governance layers as defined by ICANN, with private-public cooperation as a basis.

The "NL"model of "polderen", where multi-stakeholder and PPC are in our genes, strongly works in our favor with respect to many other countries. Its provides us with an opportunity to show the way forward.

That has, we think, consequences for policy. What is no longer possible?

- · Using outdated terms, definitions from the ICT and telecom sectors, indicating the Online economy in those terms;
- Interventions of all kinds (economic, security services, Justice) in parts of the online world that should be protected according to the WRR report[115];

[112] http://digitalgateway.eu

[113] https://www.gccs2015.com/

[114] 'De publieke kern van het Internet. Naar een buitenlands beleid'. D. Broeders. (WRR 2015). (*"The public core of the Internet. Towards a foreign policy"*, translation Wout de Natris) In this report it is advised that the basic protocols and standards that make up the Internet have to be seen as a global common good and such need to protected from any state or other interference.

- Unilateral government action, and considering sector/companies as opponents;
- Policy considerations with insufficient attention for the interests of the online economy;
- Preventing Balkanisation of the Internet.

What will this take, what are DINL's goals?

- Consistency in laws and regulations in the digital economy;
- Introducing and agreeing on concepts and definitions that reflect the structure and dynamics of the online world;
- Bringing those in line with current laws and definitions (slight tweaking);
- Recognizing the tiered structure of the online economy (ICANN, DINL, WRR, analysys mason report model[116]);
- Recognizing the mainport metaphor, and the leverage function of digital infrastructure and Internet for the economy;
- Always consider the balance between safety (privacy), security (justice/services) and economic interests in policy making;
- Approach to fighting cybercrime with PPC/multi-stakeholder initiatives such as "barrier models" and codes of conduct;
- Focus on international harmonisation and cooperation;
- “Double funnel” model for operational communication: Cooperation on operational improvements such as interfaces between services, National cybersecurity Center, Politics, Autoriteit Consument en Markt , Team High Tech Crime, and other supervisory services and authorities, - with centralized non-profit facilitators for the online sector (example NBIP[117]);
- Cooperation model (Example NaWaS , abuse-Hub, and others.)

In the IGF forum we plan to present this approach as “the only way forward” for an open, safe, and free Internet; for Economic development and transformation that will result from growing and stimulating that Digital economy.

Issues that we see:

- Governments do not sufficiently understand the difference between ICT, Telecommunication and the Internet (economy);
- Traditional stakeholders still dominate the discussion, an do have insufficient consideration for the interests of small and innovative companies in the online sector;
- Online companies are often seen as mavericks and cowboys, not to be taken seriously;

Given the age of the sector, there is still a difficulty to organize the sector and to fund this properly.

[115] Ibiden

[116] http://www.analysysmason.com/

[117] See NaWas example (Annex 12)

Annex 15. Working Group for Organizing Coordinated Disclosures (OCD)

by Inbar Raz, Working group member

The workgroup was created at the GCCS 2015 Conference in The Hague, on 16-17 April 2015. It was created by the participants of the Parallel Session on Ethical Hacking, as well as some of the spectators who requested to join.

- Session description: https://www.gccs2015.com/programme?programme=2
- Session video: https://www.youtube.com/watch?v=INpAGZUr5TE&t=9685

The purpose of the workgroup is to find the way to allow researchers to do their work, without fear of prosecution or persecution, while at the same time protecting the vendors from unnecessary actions, exposure and/or damage. The key word here will be Ethics.

Pilot in Israel

Israel is a small country. As a result, the security Community in Israel is a rather small group with a <2 degrees of separation factor. Because of this advantage, I chose to carry out the OCD's first step in Israel, as I am easily able to bring both Security Researchers, Hackers of various morals, Police, and Government to the same table. We decided to create a process with the intended result of creating a Government-sanctioned procedure, that will allow the Responsible Research of security vulnerabilities, as well as the Coordinated Disclosure process, while trying to guard the interests of all involved parties (General Public, Vendors, and Researchers) - the largest dilemma here.

Initial meetings have been held with the Israeli National Cyber Bureau (INCB), as well as the Israeli Police Cyber Unit (LAHAV 433). Both parties responded very positively about the initiative and are eager to take part in it.

As the work progresses, I will be happy to update the Forum. Our intention is to finish the work in Israel in a relatively short term, and then leverage it as a precedence for other countries interested at this, as well as our own effort at OCD Workgroup.

In the meantime, if you would like to get a general idea of the subjects that need to be discussed in this process, I'll refer you to two resources:

1. A 30-minute presentation titled "Hacking Ethics in Education", by Jeroen van der Ham. It was given at the CCC conference in Hamburg on December 2014:
https://www.youtube.com/watch?v=ugtQ7CUcxWk

2. A 15-minute presentation titled "15 Minutes on Ethical Hacking", by myself, that was given at the 5th Annual Internatonal Cybersecurity Conference in Tel-Aviv on Jjune 2015 (skip to 4:55 if you are only interested in OCD):
http://video.tau.ac.il/events/index.php?option=com_k2&view=item&id=6134:15-minutes-on-ethical-hacking&Itemid=559

The questions that will need answering, and are at the heart of the discussion, are divided into three tracks:

1. What is a "proper way" to conduct research on someone else's vulnerabilities?

- How can you perform the research without causing damage to existing data and services?

- How can you perform the research without breaching an unnecessary level of privacy?

2. What is the "proper way" to report the vulnerability to the vendor?

- How long after the research has been completed, must you report?

3. What is the "proper way" to publish your research results?

- Are there any timing constraints?

- Can the vendor impose a time frame? If so, who regulates that time frame?

- Are you required to supply the vendor response?