Identification of Anti-Spam Regulation Model for Indonesia

Takdir
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
takdir.rex@students.itb.ac.id

***Abstract*— Spam is growing into a massive attack in cyberspace. According to the Incident Monitoring Report ID-CERT 2013, CERT of Indonesia, spam places the highest reported case with 64,514 of 133,297 cases or 48.4%. However, currently there is no regulation positioning spam in law to take action to the spammer in Indonesia. We analyze the characteristics of cyber-attacks, especially spamming action, in Indonesia. Then we explore various approaches in handling spam by technical and regulation in some countries. As a result, we provide a regulation model that suitable for Indonesia by adjusting with the real condition of ICT in Indonesia. Our recommendation can be used as a consideration for constructing anti-spam regulation to reduce the impact and occurrence of spam.**

Keywords— spam; regulation; Indonesia; cyber-attack; cyberspace; cyber crime

I. INTRODUCTION

Electronic or digital addresses (e.g. e-mail, cellular phone number, and instant messaging account) are growing in quantity and variety. They enable one sending and receiving information easily with minimal or free of charge. Most of them accept message directly from every sender without user's agreement. This fact brings the "electronic spam" term into the computer world, especially in cyberspace, where all devices are connected by network that enables open communication. There are many kinds of spam, but in this paper we limit the discussion to electronic spam.

We simply define spam as message containing unwanted information. The message can contain commercial advertise, phishing URL, virus, or malware script. In the beginning of appearance, spam is classified as computer-related fraud. However, in many respects, spam could even be considered a denial of service attack against the entire Internet [1]. It is becoming a threat for user's privacy and computer system security.

According to the Incident Monitoring Report of ID-CERT, CERT of Indonesia, 2013 [2], spam places the highest reported case with 64,514 of 133,297 cases or 48.4%. It potentially damages and wastes Indonesian internet bandwidth besides affecting economics with financial frauds. However, mitigation and prevention of spam are still handled by internet user or company.

Jakarta's police station (Polda Metro Jaya) has established a cybercrime division which aims to investigate information technology, telecommunication, electronic transaction, and intellectual property. They provide a contact center to collect cybercrime reports from citizen. Problems thus arise because there is no legal position of spam in law. Currently, the cybercrime division refers to the Law of The Republic of Indonesia Number 11 of 2008 on Electronic Information and Electronic Transaction which does not include regulation about spam.

In this paper, we study about various approaches to construct spam's law regulation in other countries. After that, we analyze the regulation model that suitable for Indonesia by adjusting with current state of ICT in Indonesia.

II. ANTI-SPAM LAW IN SOME COUNTRIES

A. European Union

The Council of the European Union has Directive 2006/24/EC of The European Parliament and of The Council of 15 March 2006 [3]. It is the basis reference for the anti-spam laws of all the European Union member countries. Each member countries are allowed to present their own regulation based on that Directive. Some points related to spam presented in the Directive are [4]:

- Cover email, SMS, and MMS spam,
- Applies to all electronic communications received by or sent from networks in the European Union,
- A single email may be regarded as spam according to its content
- It is unlawful to disguise or conceal the identity of the sender

B. Canada

Bill C-28, the Fighting Internet and Wireless Spam Act (FISA), is Canada's anti-spam legislation that received Royal Assent on December 15, 2010 [5]. It contains technology neutral specifications of anti-spam. Technology-neutral implies that all means of telecommunications are captured under the new law, including Short Message Services (SMS or text messaging), social media, websites, uniform resource locators (URL) and other locators, applications, blogs, and Voice over Internet Protocol (VoIP).

In this legislation, all telecommunications channel are captured under the law. Metadata that contains background information that provides further details about one or more aspects of the data, including means of creation of the data, purpose of the data, time and date of creation and the creator or author of the data are recorded and maintained for law purpose.

C. Australia

Australia has a detailed legislation special for regulating spam named Spam Act 2003 [6]. There are 3 main rules stated in Part 2—Rules about sending commercial electronic messages:

- Unsolicited commercial electronic messages must not be sent,
- Commercial electronic messages must include information about the individual or organization who authorized the sending of the message,
- Commercial electronic messages must contain a functional unsubscribe facility.

It also has rules about address-harvesting software which can generate dummy email addresses to be used as spam senders. The rules disallow supplying, acquiring, and using address-harvesting software and harvested-address lists.

D. United States

Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM Act 2003) is the law applied in United States [7]. CAN-SPAM has been repeatedly amended to accommodate some aspects which are not covered. Commercial e-mails are allowed to be sent to the correct recipients based on the promoted content. Recipient has right to unsubscribed to such email. There are conditions which email marketers must meet in terms of their format, their content and labeling:

- Unsubscribe compliance. Unsubscribe mechanism should be clear for user
- Content compliance. Content should be arranged in friendly form, accurate sender information, and use labeling if required (e.g. adult content)
- Sending behavior compliance. Message should not be transmitted in non-standard way, including through an open relay, false header, and null message.

In the beginning of implementation, this regulation has the criticized opposite effect of making spam legal instead of prohibiting it. However some reports show the significant decrease amount of spam after applying CAN-SPAM.

III. Cyber-Attacks and ICT Condition in Indonesia

A. Cyber-attack

According to the ID-SIRTII Annual Report 2013 [8], total number of cyber-attacks in Indonesia is around 42 million attacks with 81% severity high category. The largest attack type is SQL injection for about 70%. Source of the attack average about 60% came from Indonesia followed by China, and other source countries outside Indonesia.

Country	%	Country	%	Country	%
Januari		Februari		Maret	
	67,30%		76,48%		80,81%
	16,90%		12,24%		5,83%
	4,29%		1,75%		1,08%
April		Mei		Juni	
	71,50%		43,66%		40,45%
	9,36%		36,92%		28,32%
	2,20%		7,02%		10,99%
Juli		Agustus		September	
	27,91%		41,55%		46,65%
	26,50%		15,86%		28,57%
	16,31%		9,32%		6,50%

Fig. 1. Sources of attacks

Besides, it is known that around 30% to 40% utilization of traffic Internet international goes to access negative content particularly pornography, warez activity and illegal multimedia content [9]. The impact of access to negative content is the increase of incident from malware/malicious code. Based on statistic data from internet security forum, more than 40% malicious code is spread out through negative content and rest through spam.

Meanwhile, talking about information security issues at the government currently, Directorate of Information Security, Directorate General of Information Application, Ministry of Communications and Information Technology described them into [9]:

1. The awareness of government agencies and the public (especially in Region) on information security and cyber security is still below the standard.
2. Coordination among government agencies is still not optimal regarding cyber security.

3. Implementation of ICT security in Indonesia is still not integrated / working separately.
4. Immaturity level of ICT governance and information security management systems in government agencies.
5. The high digital divide in Indonesia.

In the current Law of The Republic of Indonesia Number 11 of 2008 on Electronic Information and Electronic Transaction Article 15, the electronic system organizer shall be responsible for the organization and proper operation of his/her electronic system. As illustration, if someone sends spam messages from internet café, the owner of the café can be involved doing cybercrime. The limitation of electronic system organizer, especially for small company, to filter large amount of cybercrime possibilities makes this regulation not fair in the organizer's point of view.

There are a lot of efforts presented by government and internet service provider associations to stop spamming. APJII (Indonesian Internet Service Provider Association) has provided DNS filtering system to block malicious and negative contents. However, the increasing numbers of blocked content show that spam successfully penetrate into Indonesia. It proves the note that legal and technical efforts implemented separately to stop spam are ineffective [10].

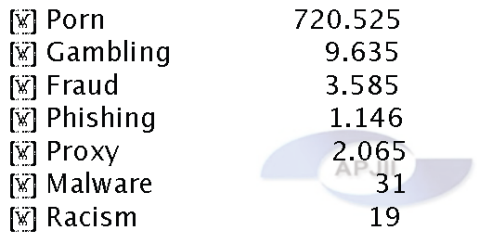

Fig. 2. Web blocked by APJII's DNS Filtering System

IV. Proposed Anti-Spam Regulation model for Indonesia

Lack of awareness of government on IT security in Indonesia causes low quality Spam filtering, including the regulation. The "silo" model of ICT implementation makes difficult to control the behavior of the systems and therefore this condition should be considered in anti-spam regulation model. We define some criteria that should be followed in the model:

- Electronic transactions should be captured and its log should be maintained. Capturing communication channel will maintain log for every transaction that can be used as evidence for judgment purpose. This criterion refers to the fact in point 1 and 4 above. The loss of log cause proof of crime difficult.
- Enable enforcement of unsubscribe functionality by government ICT agencies. Although unsubscribe feature is available for user and has been stated in all spam regulations, the lack of awareness of user cause it is not enough to prevent distribution of spam and malicious content.
- Account registration should be improved and maintained, including cellular number, e-mail address and another account related to the cyberspace. It comes from the fact that most of spam containing negative content and pornography that should be forbidden for some age categories.
- The regulation should be integrated and synchronized with national ICT infrastructures regulation. The high number of attacks coming from Indonesia itself shows there are vulnerabilities that are potential to be misused by insiders.

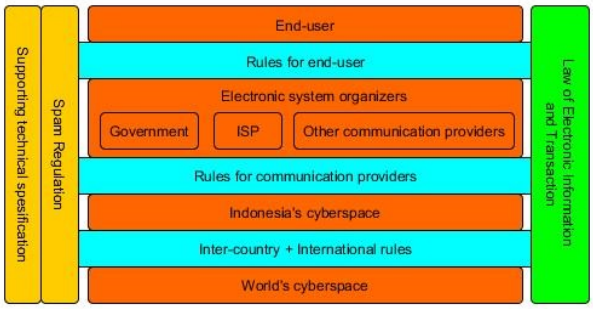

Fig. 3. Proposed Anti-Spam Regulation Model

One of the differences from existing law in our model is the involvement of end-user. Technical specification is required to realize this rule, including specification for ICT infrastructures and governance, communication metadata and log, and user account registration.

Our proposed regulation and monitoring model close to the Bill C-28 Canada where all electronic communications are captured and maintained under the law. Capturing communication channel will keep log for every transaction that can be used as evidence for judgment purpose. Other suitable rules from various countries of course can be adopted as the complement of the model, such as covering email, SMS, and MMS spam in European Union directive, and content compliance in CAN-SPAM.

V. Conclusion

Indonesia becomes top rank in cyberspace communities with the involvement of the number of Internet users. In line with it, cyber-attacks are growing up in quantity and variety. Spamming is one of an easiest attack to do and has the highest occurrence coming in many forms in Indonesia. Current ICT condition in Indonesia should be considered to produce suitable regulation combating spam. We identified some criteria to be used as consideration in constructing ideal anti-spam regulation in Indonesia combining technical and legal aspects. Furthermore, we invite researchers to improve our model by adding other data source to enrich the analysis.

REFERENCES

[1] P. Moderator, M. Clifford, D. Faigin, and M. Bishop, "Miracle Cures and Toner Cartridges : Finding Solutions to the Spam Problem Panelists : Position Statements," no. Acsac, 2003.

[2] I. Computer and E. Response, "Pertemuan tahunan vi id-cert 2014 bandung, 21 april 2014," no. April, 2014.

[3] T. H. E. E. Parliament, T. H. E. Council, O. F. The, and P. Union, "DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006," no. March 2004, pp. 54–63, 2006.

[4] K. Šolić, D. Šebo, F. Jović, and V. Ilakovac, "Possible Decrease of Spam in the Email Communication," pp. 1512–1515, 2011.

[5] M. O. F. Industry, "HOUSE OF COMMONS OF CANADA BILL C-28 PROJET DE LOI C-28," 2010.

[6] C. Office of Parliamentary Counsel, "Spam Act 2003," no. 129, 2014.

[7] 108th United States Congress, "Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM Act 2003)." 2003.

[8] ID-SIRTII, "ID-SIRTII Annual Report 2013," 2013.

[9] I. M. of C. and I. Technology, "ICT White Paper Indonesia 2012," 2012.

[10] D. Dickinson and D. Dickinson, *An Architecture for Spam Regulation An Architecture for Spam Regulation*, vol. 57, no. 1. 2004.