International Journal of Software Engineering & Computer Systems (IJSECS)
ISSN: 2289-8522, Volume 2, pp. 1-9, February 2016

DOI: http://dx.doi.org/10.15282/ijsecs.2.2016.1.0012

A PROPOSED FRAMEWORK TO CONTROL RUMOUR PROPAGATION ON TWITTER FOR CRITICAL NATIONAL INFORMATION INFRASTRUCTURE (CNII) ORGANISATIONS

Nor Faiz Muhammad Noor*, Omar Zakaria, Puteri N. E. Nohuddin

Universiti Pertahanan Nasional Malaysia
Kem Sungai Besi 57000 Kuala Lumpur
*Email: norfaiz@outlook.com

ABSTRACT

Critical National Information Infrastructure (CNII) organisations in Malaysia consist of many crucial sectors that not solely effect on national e-sovereignty, but also on economy, social and politic matters. Due to the widely usage on social media especially on Twitter, harmful rumour can easily propagate without any restrictions on any CNII organisations. For instance, the harmful rumour can damage the function of affected CNII such as reputation, perception and even worse can lead to disability to function. Up to this moment, there is no proper control to stop rumour propagation on Twitter for CNII. Therefore, this paper proposes a framework on controlling rumour propagation on Twitter for Malaysian CNII.

Keywords: Rumour, Rumour Control, Microblogging, Twitter, Critical National Information Infrastructure (CNII)

INTRODUCTION

Twitter, a microblogging service that allows users to publish and exchange 140 character messages called tweets is one of the online social media that rapidly growth in last few years. Information sent on Twitter get replied quickly and propagated relatively far away, even though most of the conversations on Twitter last for a short period of time (Ye, Shaozhi, & S., Felix Wu, 2010). Its structures and features also allow the spread of unverified information in large amounts among people (Herman & Noam, 2008) and efficient (Doerr et al., 2012).

The statistics provided by the Malaysia Computer Emergency Response Team (MyCERT) showed that the cyber incidents in the category that related to the use of online content such as content related and cyber harassment accident increased in the second quarter compared to the first quarter in 2013 (Malaysia Computer Emergency Response Team, 2013). Malaysia's CNII was not exception from these cyber incidents. Therefore, CNII organisations must be fully protected from associated cyber threats which in turn can help to achieve the government's goal to bring Malaysia on par with advanced nations in digital economy (BERNAMA, 2013).

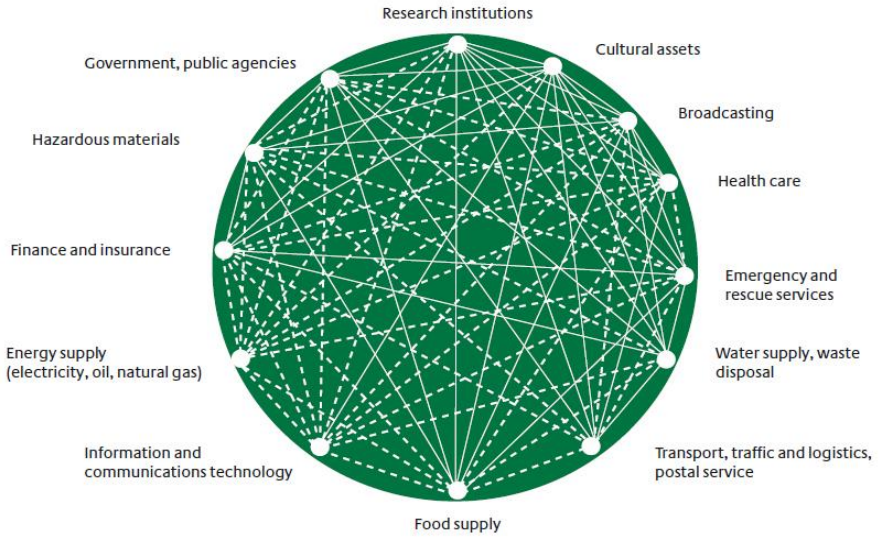

Figure 1. Interdependencies of selected critical infrastructures. Source: German Federal Ministry of the Interior, Protection of Critical Infrastructures. Risk and Crisis Management. Guidelines for Companies and Authorities, Berlin, May 2011, 10.

Critical National Information Infrastructure (CNII)

The CyberSecurity Malaysia defined the Critical National Information Infrastructure (CNII) as an organisation which the destruction or disruption of its assets (real and virtual), systems and functions would significantly affect the nation's image, economic strength, defence and security, government capabilities to function and public health and safety (CyberSecurity Malaysia, 2013). The government of Malaysia considers that there are ten sectors which there are critical elements; national defence & security, banking & finance, information & communications, energy, transportation, water, health services, government, food and agriculture and emergency services (CyberSecurity Malaysia, 2013).

Most of the CNII in Malaysia today is an information infrastructure which consisting of numerous networks connection such as internet, intranet, extranet and etc. Its interdependence with other critical infrastructures demanded the protection.

The dependency on digital information systems and it interdependencies between other infrastructure escalating vulnerabilities and risks among others include cybercrimes such as harassment, content related, malicious code, denial of service attacks, hacking, intrusion and fraud.

The growth of cyber threats to the CNII need comprehensive cyber security implementation not only from the physical attack, but also from syntactic and semantic attack. The National Cyber Security Policy (NCSP) has been put in place to protect the e-sovereignty of the nation (Shamir, 2011). However, the semantic attack in the form of rumours which has been spreaded on the Twiter is now being looked as something to be reckon with. The semantic attacks can be more serious than physical or syntactic attacks (Schneier, 2000).

RUMOURS ON TWITTER

The spreading of rumours on Twitter that related to CNII in Malaysia are becoming more common in recent years. Several cases of spread of rumours on twitter that directly affect CNII in Malaysia has been reported such as Bangladeshi phantom voters during 13th General Election (New Straits Times, 2013); Sabah invasion by Sulu terrorist (The Edge Malaysia, 2013) and racial clashes in Sungai Petani (BERNAMA, 2012, and New Straits Times, 2012).

The rumours spread on Twitter have implications to the social, economic and political, directly and indirectly such as panic buying, a drop in investor and tourist confidence, racial tensions, racism discrimination, panic buying, xenophobia, foreigner phobia and diplomatic relations. Some of the CNII which have been affected by these rumours are the Malaysian government, the Royal Malaysia Police, Malaysian Armed Forces and the Ministry Of Home Affairs.

The rumours circulated on Twitter, if not controlled, will give a worse effect on the related CNII organisation and the nation as a whole. At present, there are no guidelines and rules can be adopted by CNII in Malaysia to control the spread of rumours on Twitter. The Malaysian government currently do not have any plans to shut down the Twitter as is done by some countries to prevent the uncontrolled dissemination of information (Malaysia Today, 2011).

Therefore, a framework needs to be developed to assist the Malaysian CNII to control the spread of rumours that could have a negative effect not only on their organisation, but also to the nation.

LITERATURE REVIEW

The literature review in this paper will explain the definition of rumours, relationship rumours and cybercrime, rumour monitoring, rumour detection and later on rumour control.

Glimpse of the Rumours

Definitions of rumour has been widely varying by the research across sociology, psychology, and communication studies (Pendleton, Susan Coppess, 1998). Rumours have been described as public communications that are infused with private hypotheses about how the world works (Rosnow, R, 1991), or more specifically, ways of making sense to help us cope with our anxieties and uncertainties (Rosnow, 1988 and 25].

Grover summarised that rumours are unverified information and the potential to spread rapidly among people (Grover, 2008). Among the variables that lead to the existence of the rumour as defined by scholars are anxiety (Allport, Gordon W., and Leo, 1947), harmony (Allport, Gordon W., and Leo, 1947), lack or plentiful news (Shibutani, 1966), mistrust (Rosnow, Ralph L., and Gary, 1976), paucity of information (Koenig, Fredrick, and Fredrick Koenig, 1985), ambiguity (Rosnow, 1976 and Rosnow, 1988) and uncertainty (Rosnow, 1976 and Rosnow, 1988).

Rosnow and Foster proposed basic law of rumours which the strength of rumours is directly proportional to the significance of the subject of the individual concerned and the uncertainty of the evidence at hand (Rosnow Ralph L., and Eric K Foster, 2005). In particular, rumours happen when there is no clear relationship exists

between the people and the right information, thus leading to ambiguity about the source and validity of the information (Bordia, Prashant, and Nicholas DiFonzo, 2004).

Compared with the positive rumours, negative rumours spread more easily (Knapp & Robert, 1944). The spread of negative rumours not only affects the individual but also to an organisation. Among the negative impact of rumours to the organisations are demoralisation and undermine employee productivity, market value losses and damage to business reputation (Nicholas et al., 1994, DiFonzo, and Prashant 2000, Michelson, V. Suchitra, 2001 and Dubois et al., 2011).

Is the Creator and Disseminator of Rumour is A Cyber Crime?

In the definition of cyber security incidents provided by Malaysia Computer Emergency Response Team (MyCERT) in their website, there is no definition of rumour. However, based on the review on the definition of rumour above, rumour can be classified under content related or cyber harassment incident. According to MyCERT, content related incident is a material which is offensive, morally improper and against current standards of accepted behaviour which includes also nudity and sex (Malaysian Computer Emergency Response Team , 2013)

Besides, cyber harassment incident covers a wide range of offensive behaviour (Malaysian Computer Emergency Response Team , 2013). It is commonly understood as behaviour intended to disturb or upset. In the legal sense, it is behaviour which is found threatening or disturbing. In conclusion, we can conclude that harmful rumours are cybercrime based on the definition provided by MyCERT.

Rumour Monitoring and Detection on Twitter

Continuous monitoring of the tweet that related to the CNII organisation is necessary to ensure that the rumours generated can be traced and combat quickly. Thus, it is crucial to have a systems that can automatically detect rumours circulating on the Twitter networks.

Seo et al. proposed algorithm to identifying rumours and their sources (Seo, Prasant, and Tarek, 2012) while Castillo et al. used a machine leaning technique to classify rumours and non-rumours (Castillo et al., 2011). However, the research did not cover the aspect of continuous monitoring.

The framework developed by Leskovec et al. to identify rumours on mainstream media sites and blogs (Leskovec et al., 2009) perhaps the most suitable framework that can be modified to be used on Twitter as it can perform automatic identification. This possibility will be explored in our future work.

Rumour Control

Up to this moment, there is no study on controlling rumours propagation on Twitter for CNII. Most researchers (Kapferer, 1990, and Kimmel, 2004) concurred that simply denying a rumour fails to eliminate its negative impact, but few remedies have been offered to counteract negative rumours. In an exception, Tybout et al. proposed that a re-association strategy (Tybout et al., 1981), whereby the negative stimulus (e.g. worm meat) associated with the target brand (e.g. McDonald's) is re-associated with a positive stimulus (e.g. the French use worm meat in their cuisine), can reduce the rumours' negative effects on consumers' attitudes toward the brand. Yet, re-association might

sometimes prove problematic, either because of the difficulty of finding positive stimuli that can offset the negative effect, or because of the monetary and cognitive costs necessary for customers to learn new associations (Meyers et al., 1989).

Dubois et al. suggested an alternative strategy to counter rumours; making communicators explicitly question whether they can be certain of their beliefs based on the information they received (Dubois et al., 2011). Asking consumers to question or reconsider whether they can be certain of a belief they have heard may lead them to focus on and reconsider how certain the sender of the information was. This should help to reduce recipients' certainty in cases in which the sender was initially uncertain.

Research on controlling rumours has been done earlier in the field of marketing (Dubois et al., 2011). Dubois et al. added and tested that there are three strategies of combating rumours: denial, re-association and questioning. In the experiment, they found that questioning strategy is the most effective way for combatting rumours compared to denial and re-association in the field of marketing strategy. Does this strategy can be applied to combat rumours on Twitter? The following explanation will try to answer the question.

From our findings, it is not impossible to apply the questioning and re-association strategy on Twitter. If we apply this strategy on Twitter, we need to ask each user's which tweeted the rumours. It may be possible if the number of tweet is small and the rumourmongers just about to spread the rumours. However, Twitter only allowed a user to tweet up to 1000 tweets per day and if the user keeps tweeting with the same message, the account will be recognised as a spam account (Twitter, 2013). In addition, a tweet can only have 140 characters per message. Therefore, this research cannot adapt questioning and re-association strategy.

For this research, denial strategy is the most suitable approach to control rumours for CNII organisation. This can be done with the official statement that will be issued via their official Twitter account. The official statement to deny the rumour is the control method which is part of the proposed framework that will be discussed in the next section.

PROPOSED FRAMEWORK FOR CONTROLLING RUMOUR PROPAGATION ON TWITTER FOR CNII

The proposed framework is a set code of practice and principles that will includes process and procedures than can be used by the CNII organisations to protect and govern their organisation from the cyber-threat come in the form of rumour. It can also be used as a guideline to provide a method of establishing, implementing, reviewing, maintaining and improving the level of readiness in facing a cyber-threat and attacks throughout the CNII organization.

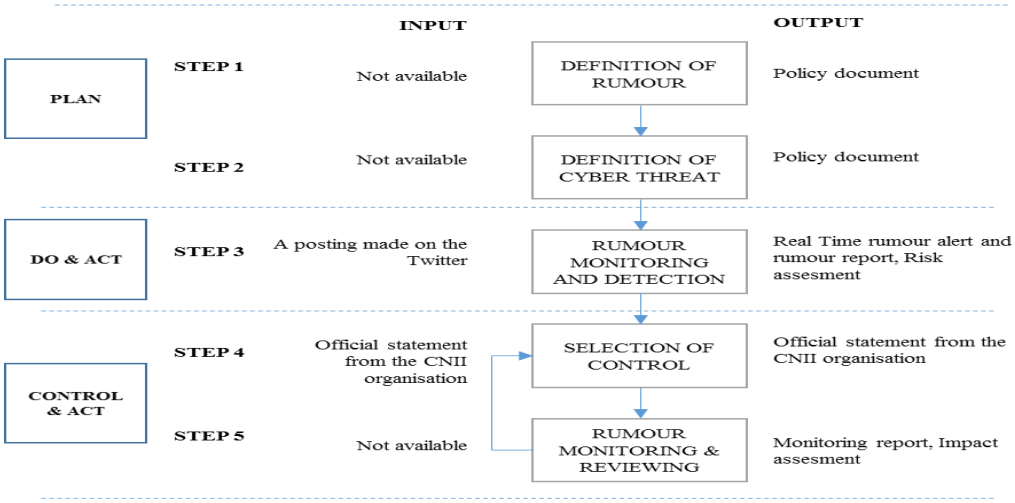

Figure 2. The Proposed Framework for Controlling Rumour Propagation on Twitter for CNII is adapted from ISMS 27001: 2005

This framework was originally developed based on the literature review and the Plan-Do-Check-Act" (PDCA) process model which have been adapted by the ISO/IEC 27001:2005 to be applied to the structure of all the processes in ISMS. Although ISO 27001:2005 will be replaced with the new edition of ISO 27001:2013, the ISMS processes in PDCA is still relevant for a security implementer to plan, do, check and act on each security processes.

The framework consists of five steps of defining the rumour, defining the cyber threat, rumour monitoring and detection, selection of control and rumour monitoring and reviewing. The first and second step is a plan stage where the output is a policy document. This is important to the CNII organisation to understand the problem domain and define the information that can be classified as a harmful rumour which could potentially damage their organisation. The third step of rumour monitoring and detection is a combination of the do and act stage of the PDCA. At this stage, the rumour which the characteristics has been identified at earlier stage will be identified. The detection system should have the ability to provide real time alert and report to the administrator so the risk assessment can be conducted immediately. The outcome of the risk assessment then will be used by the decision maker to issue the most appropriate statement to deny the rumour. This should be done within a short period of time in the fourth step to prevent the rumours to spread more widely. Continuous monitoring and reviewing the rumours propagation trend after publishing the official statement is necessary to ensure that the rumours did not resurface and has completely disappeared from the twitter sphere.

CONCLUSION

In this paper, a rumour propagation control on Twitter has been proposed to help the CNII organisation in Malaysia to control rumours propagation on twitter. In our future work, the framework will be validated with the sample of rumours derived from Twitter. Other than that, this paper may help to shows the CNII organisation on the effectiveness of controlling the rumours on Twitter and provide better understanding on the impact of controlling rumours on social media.

ACKNOWLEDGEMENT

The authors would like to acknowledge the Ministry of Education Malaysia for granting the Fundamental Research Grant Scheme (FRGS, Ref: FRGS/2/2013/ICT01/UPNM/02/1) to us and the Universiti Pertahanan Nasional Malaysia (UPNM) for providing research facilities.

REFERENCES

Allport, Gordon W., and Leo Postman (1947). The psychology of rumor 1947.

BERNAMA (2013). Malaysia's Critical National Information Infrastructure Must Be Fully Protected - Muhyiddin. Last modified November 26, 2013. http://www.bernama.com/bernama/v7/ge/newsgeneral.php?id=996257.

BERNAMA (2012). Police Monitoring Social Sites, Blogs To Check Speculation About Rioting In Sungai Petani. modified December 19, 2012. http://www.bernama.com/bernama/state_news/news.php?cat=nt.

Bordia, Prashant, & Nicholas DiFonzo. (2004). Problem solving in social interactions on the Internet: Rumor as social cognition. *Social Psychology Quarterly*. *67*(1), 33-49.

Castillo, Carlos, Marcelo Mendoza, & Barbara Poblete (2011). Information credibility on twitter. Proceedings of the 20th international conference on World wide web, 675-684.

CyberSecurity Malaysia (2013). CNII Portal. Accessed November 25, 2013. http://cnii.cybersecurity.my/main/about.html.

DiFonzo, Nicholas, & Prashant Bordia (2000). How top PR professionals handle hearsay: corporate rumors, their effects, and strategies to manage them. *Public Relations Review*, *26*(2), 173-190.

Doerr, Benjamin, Mahmoud Fouz, and Tobias Friedrich (2012). Experimental analysis of rumor spreading in social networks, *Design and Analysis of Algorithms*. Springer Berlin Heidelberg, 159-173.

DuBois, David and Derek D Rucker (2011). How to Stop Rumors Before They Ruin Your Brand. Forbes, September 16, 2011.

Dubois, David, Derek D. Rucker, & Zakary L. Tormala (2011). From rumors to facts, and facts to rumors: The role of certainty decay in consumer communications. *Journal of Marketing Research, 48* (6), 1020-1032.

Grover, Aditi (2008). A Study on Propagation and Quelling of Rumors. n.p. ProQuest, UMI Dissertations Publishing.

Herman, Edward S., and Noam Chomsky (2008). Manufacturing consent: The political economy of the mass media. Random House.

Kapferer, J.,-N. (1990). Rumors: Uses, interpretations, and images. *New Brunswick, NJ: Transaction*.

Kimmel, A. J (2004). Rumors and rumor control: A manager's guide to understanding and combatting rumors. *Mahwah, NJ: Erlbaum*.

Knapp & Robert H (1944). A psychology of rumor. *Public Opinion Quarterly, 8*(1), 22-37.

Koenig, Fredrick, and Fredrick Koenig (1985). Rumor in the marketplace: The social psychology of commercial hearsay. *Auburn House Publishing Company*.

Leskovec, Jure, Lars Backstrom, & Jon Kleinberg (2009). Meme-tracking and the dynamics of the news cycle. Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 497-506.

Malaysia Computer Emergency Response Team (MyCERT) (2013). MA-355.082013 : MyCERT 2nd Quarter 2013 Summary Report. Last modified August 6, 2013. http://www.mycert.org.my/en/services/advisories/mycert/2013/main/detail/931/index.html.

Malaysia Today (2011). PM vows no Internet censorship despite FB, Twitter influence. Last modified February 12, 2011. http://www.malaysia-today.net/mtcolumns/newscommentaries/38089-pm-vows-no-internet-censorship-despite-fb-twitter-influence.

Malaysian Computer Emergency Response Team (MyCERT). "Definitions of Incidents." Accessed November 20, 2013. http://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/799/index.html.

Meyers-Levy, Joan, & Alice M., Tybout (1989). Schema congruity as a basis for product evaluation. Journal of Consumer research, 39-54.

Michelson, Grant, and V. Suchitra Mouly (2002).'You Didn't Hear it From Us But…': Towards an Understanding of Rumour and Gossip in Organisations. *Australian Journal of Management*, 27(1), 57-65.

New Straits Times (2013). Bangladeshis voting in GE13 'a fabrication'. Last modified June 4, 2013. http://www.nst.com.my/top-news/bangladeshis-voting-in-ge13-a-fabrication-1.293255#ixzz2a2Gd34eH.

Nicholas DiFonzo, Prashant Bordia, and Ralph L. Rosnow, (1994). Reining in Rumors, Organizational Dynamics, 23, 47–62.

Pendleton and Susan Coppess (1998). Rumor research revisited and expanded. *Language & Communication*, 18(1), 69-86.

Rosnow, R., L. (1991). Inside rumor: A personal journey. *American Psychologist*, 46, 1991: 484-496.

Rosnow, R., L (1974). On rumor. *Journal of Communication*, *24*(3), 26-38.

Rosnow, Ralph L., & Eric K., Foster (2005). Rumor and gossip research. Psychological Science Agenda, *19* (4).

Rosnow, Ralph L. and Gary A., Fine (1976). Rumor and gossip: The social psychology of hearsay. *Elsevier*.

Rosnow, Ralph L., James L., Esposito, & Leo Gibney (1988). Factors influencing rumor spreading: Replication and extension. *Language & Communication*, *8* (1), 29-42.

Seo, Eunsoo, Prasant Mohapatra, and Tarek Abdelzaher (2012). Identifying rumors and their sources in social networks. *SPIE Defense, Security, and Sensing. International Society for Optics and Photonics*.

Shamir b. Hashim, M. (2011). Malaysia's National Cyber Security Policy: The country's cyber defence initiatives, *Second Worldwide Cybersecurity Summit* (WCS), 1-7.

Shibutani, Tamotsu (1966). *Improvised news*. Ardent Media.

The Edge Malaysia (2013). IGP: 700 invasion force nothing but mere rumours." Last modified March 8, 2013. http://www.theedgemalaysia.com/political-news/232550-igp-700-invasion-force-nothing-but-mere-rumours.html.

Twitter (2013). Twitter Help Center | The Twitter Rules. Accessed November 25, 2013. https://support.twitter.com/articles/18311.

Tybout, Alice M., Bobby J. Calder, & Brian Sternthal (1981). Using information processing theory to design marketing strategies. *Journal of Marketing Research* ,73-79.

Ye, Shaozhi, and S., Felix Wu (2010). Measuring message propagation and social influence on Twitter.com. *In Social informatics*, 216-231.