Internet Roadmap topics: Freedom and Security in Cyberspace - A Cyber Defense perspective

- Area: COMBINED INTERNET GOVERNANCE PRINCIPLES AND ROADMAP
- Entitled by: Roberto Uzal Daniel Riesco Germn Montejano
- Region: Argentina
- Organization: Universidad Nacional de San Luis
- Sector: Academia

- Keywords: Internet-roadmap; Freedom&Security; Cyber-Defense; Cyber-Attacks; Cyber-Espionage

- Doc Attached: Click here to see the doc 1

Abstract

This contribution is aimed at elaborating an Internet Roadmap; specifically at improving inter-State Cyberspace relations. Cyber Defense proposals are included. Current technological state-of-the-art could allow for an Internet where freedom, privacy and security can exist together in a context where human rights are the main reference point. International organizations should acquire concepts and tools for a reasonable Cyberspace control in order to minimize Cyber Attacks and Cyber Espionage.

Document

Introduction

Cyber Attacks (CA) could be included in “letter and spirit” of Article 51 of the United Nations (UN) Charter. Cyberspace (CS) has been recognized as a new domain in warfare but, currently, and also probably in the mid-term, without an international Cyber Defense (CD) agreement, unilateral “solutions” will most likely continue to unfortunately play a central role in the field of CD incidents (Uzal, 2012) (Geiss & Lahmann, 2013).

The problem of CA attribution is a main challenge, both for state nations and for international organizations (Geiss & Lahmann, 2013).

Core topic: Detecting botnets and CA Command and Control (C&C) Servers, using Large Scale Net Flow Analysis (LSNFA) is feasible, both from technological and economic points of view. Successful detection rate is high and false positive rate is low. Pattern Recognition (PR) approach increases the effectiveness of LSNFA (Baieli, Cunha, Uzal, 2014).

It is demonstrated that for real-time detection of botnet and CA C&C Servers using LSNFA is possible. If international organizations like UN begin using LSNFA, the problem of CA and Cyber Espionage attribution could be successfully faced (Bilge et al, 2012) (Brauckhoff et al, 2009) (Claise, 2004) (Cook, et al 2005) .

The ideal data source for Large Scale botnet and CA C&C Servers detection does not currently exist but there are alternatives data sources widely available such us Net Flow data (Bilge et al, 2012) (Baieli, Cunha, Uzal 2014) (Uzal, Montejano, Riesco, 2013 / 14).

Current technological knowledge could allow for an Internet where freedom, privacy and security can exist together in a context where human rights are the main reference points. International organization cyberspace control could be executed without privacy rights violations.

Last but not least, we remark that concepts and tools described in this contribution could have an extra “value added”: It could be an interesting approach to the use of LSNFA in the fight against money laundering specially with the alternative called Cyber Money Laundering – Cyber Gambling, being the most effective one. At the end, we propose the contribution conclusion and the contribution references.

State nations Cyber Attacks

Scholars accept that CA could be included both in letter and in spirit of Article 51 of the UN Charter. Experts also admit that a precise definition of “Armed Attack”, within the Cyber context, is feasible to be agreed upon; however, problems come from the denominated “Problem of Attribution”.

“Inter-State Cyber Security (Geiss, Lahmann, 2013) has unfortunately been treated predominantly as a military issue and as a consequence debate has, by and large, revolved around the question of whether, and under which conditions, measures of self-defense pursuant to Article 51 of the Charter of the UN are feasible and permitted in response to CA”. Referenced experts argue that, “while self-defense certainly cannot be ruled out, the Problem of Attribution will preclude its proper application in many, if not most, instances (Geiss, Lahmann, 2013).

An international Cyber Defense agreement need

We point in advance that currently, and also likely in the mid-term, without an international CD agreement, unilateral remedies will most likely continue to play a central role in cases of CD incidents. We named as CD incident those CS conflicts where actors are state nations.

This contribution presents a proposal that complements the “traditional” unilateral focus based on Article 51 of UN Charter. Contribution presents technological aspects and new incumbencies / responsibilities to be faced by international organizations like UN / International Telecommunication Union or others to be discussed.

The technological aspect of this contribution is based on recent developments both in the field of Net Flow Analysis and in PR area of knowledge and applications. Detecting botnets and CA C&C Servers is a currently feasible task. Anyway, the use of presented technological focus makes sense only in the context of an ad hoc international CD

agreement.

The problem of Cyber Attacks attribution

A precise definition of ‘Armed Attack’ within the Cyber context is needed but, the most important challenge for the application of the doctrine of Self Defense (Article 51 of UN Charter) to the new “Cyber Weapons” is the attribution of “unlawful conduct” to the aggressor state nation.

The core of this contribution is giving fundamentals and tools to solve “The Attribution Problem”.

Large Scale Net Flow Analysis and Pattern Recognition use

Currently it is possible to use large-scale, wide-area Botnet / CA C&C detection systems that incorporate a combination of techniques to overcome the challenges posed by the use of Net Flow data. There are several groups of features that allow these systems to distinguish C&C channels from benign traffic using Net Flow records. To reduce these systems false positive rate, they incorporate a number of external reputation scores. Authors have developed evaluations that demonstrate that it is able to perform close to real-time detection of botnet and CA C&C Servers (Bilge et al, 2012) (Baieli, Cunha, Uzal 2014).

Tools based on these ideas work in two phases: A training phase where samples are used to build detection models. A detection phase where detection models are used to classify IP addresses as benign or associated with CA (Bilge et al, 2012) (Baieli, Cunha, Uzal 2014). PR concepts and tools are very useful in these schemes. It is understood that PR is the automated identification of shapes and others patterns. In this contribution context, PR is an important field of Computer Science concerned with recognizing patterns, particularly, in this case, Net Flow statistical histograms.

Freedom, privacy and security in Cyberspace

In the Introduction of this contribution we, in advance, remarked that current technology state could allow for an Internet where freedom, privacy and security can exist together in a context where human rights are the main reference point. International organization CS control could be executed without privacy rights violations. Recommended tools analyze just Net Flow statistical histograms. Private data will not be accessed. Freedom and privacy will be protected.

Extended "value added": Concepts and tools to fight against Cyber Money Laundering – Cyber Gambling

In the context of Argentina Council of Foreign Relations, authors have developed a seminar about Cyber Money Laundering – Cyber Gambling (Uzal, 2013). This seminar was replicated in Argentina's Army Polytechnical School (Escuela Superior Técnica del Ejército de Argentina) organized by Armed Forces Communications and Electronics Association. Seminars were successful.

Authors think that the use of LSNFA / PR in the fight against money laundering could be interesting, especially the alternative called Cyber Money Laundering – Cyber Gambling, as we anticipated in the Introduction, the most effective one.

Conclusions

1. Cyber Attacks can be included in “letter and spirit” of Article 51 of the UN Charter. Cyberspace has been recognized as a new domain in warfare.

2. Currently, and also probably in the mid-term, without an international Cyber Defense agreement, unilateral remedies will most likely continue to play a central role in the field of Cyber Defense incidents.

3. The problem of Cyber Attacks attribution is the main challenge.

4. Core topic: Detecting botnets and Cyber Attacks Command and Control Servers using Large Scale Net

5. Flow Analysis is feasible both from technological and economic point of view.

6. Researchers have demonstrated that it is feasible to perform close to real-time detection of botnet and Cyber Attacks C&C Servers using LSNFA. If international organizations like UN start using LSNFA, the problem of Cyber Attacks and Cyber Espionage attribution could be successfully faced.

7. The ideal data source for large-scale botnet and Cyber Attacks C&C Servers detection does not currently exist, there are, however, alternatives data source such us Net Flow data.

8. Current technology level could allow for an Internet where freedom, privacy and security can exist together in a context where human rights are the main reference point. International organizations

9. Cyberspace control could be executed without privacy rights violations.

10. It could be also an interesting approach to the use of Large Scale Net Flow Analysis / Pattern Recognition in the fight against money laundering specially with the alternative called Cyber Money Laundering – Cyber Gambling, being the most effective one.

References

(Uzal, 2012) R. Uzal “Guerra Cibernética” Visión Conjunta” Año 4, Número 1, 2012 (Armed Forces Joint War College Magazine – Argentina)

(Geiss & Lahmann, 2013) R. Geiss, & H. Lahmann “Freedom and Security in Cyberspace”, http://www.ccdcoe.org/publications/books/PeacetimeRegime.pdf, Tallin, 2013

(Bilge et al, 2012) L. Bilge et al “DISCLOSURE: Detecting Botnet Command and Control

Servers Through Large-Scale Net Flow Analysis”, 2012 http://www.cs.ucsb.edu/~chris/research/doc/acsac12_disclosure.pdf

(Brauckhoff et al, 2009) D. Brauckhoff, X. Dimitropoulos, A. Wagner, and K.Salamatian. “Anomaly extraction in backbone networks using association rules”. ACM Internet Measurement Conference (IMC'09), 2009.

(Claise, 2004) B. Claise, “Cisco systems Net Flow services export version 9”, 2004.

(Cook, et al 2005) E. Cooke, F. Jahanian, and D. McPherson. “The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets”. 1st Workshop on Steps to Reducing Unwanted Traffic on the Internet, pages 39- 44, 2005.

(Baieli, Cunha, Uzal 2014) C. Baieli, I. Cunha, R. Uzal. Claudio Baielli MSc Thesis work (I. Cunha – UFMG & R. Uzal – UNSL are the thesis development advisors)

(Uzal, Montejano, Riesco, 2013 / 14) On going research work at Universidad Nacional de San Luis – Argentina

(Uzal, 2013) R. Uzal, www.cari.orghttp://argentina.afceachapters.org/wp-content/uploads/2013/07/presentacionDrUzal.pdf