DDoS Cyber-Attacks Network: Who's Attacking Whom and Why?

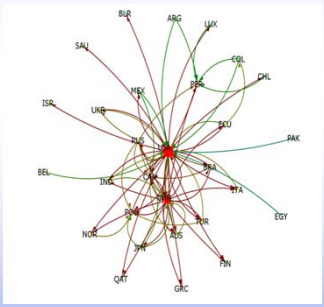
Sumeet Kumar
sumeetku@cmu.edu

Prof. Kathleen M. Carley
kathleen.carley@cs.cmu.edu

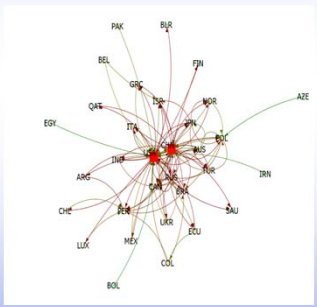
Carnegie Mellon
Ph.D. Program in Computation, Organizations & Society

Introduction

•Cyber-attacks aimed at breaking into networks, stealing data and bringing websites down have become an every-day phenomenon. However, there is minimal clarity on where are the attacks originating, who are the top targets, what is the trend of attacks, what are the motivations?
•DDoS attacks data shared by Arbor Networks from June 2013 to Mar 2016 is used to build a cyber-attacks network.
•Using aggregate country-to-country attacks, we summarize the major players and trends in cyber-attacks in graphs below:



Attacks Received Network



Attacks Sent Network

•In charts above, node size reflects the attacks sum of received/sent by a country and the edge color reflects the mean attack bandwidth. Edges less than 200 Gbps are hidden.
•China and US share center positions in both the graphs.

Correlation and QAP Analysis

Two types of correlation analysis: a) Country (node) level correlation and, b) Network level correlation. Country level analysis uses the Pearson's correlation coefficient and related significance testing. Network level analysis uses the Quadratic Assignment Procedure (QAP).

Results

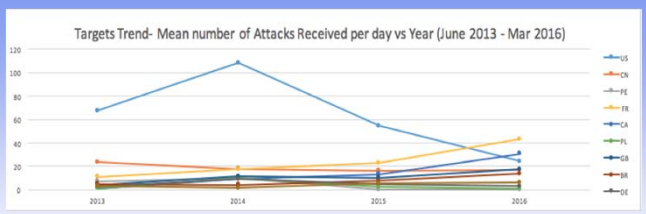
	Network Bandwidth	GDP Per Capita	Internet Users per 100 population	ICT (World Bank)	ICT Import as Percent of Trade	CPIA	Sentiment Score (USNA data)
Attacks Sent	**0.53** (P =0.000)	0.15 (P = 0.0544)	0.17 (P = 0.0283)	0.18 (P = .0194)	0.19 (P =.0116)	-0.11 (P = .1591)	-0.028 (P=.7197)
Attacks Received	**0.49** (P = 0.000)	0.12 (P = 0.122)	0.15 (P =0.0549)	.16 (P = .0418)	.25 (P = .0009)	-.098 (P = .2031)	-0.063 (P =0.4178)

Bandwidth of cyber attacks has medium correlation with internet bandwidth, and small correlation with GDP per capita, Internet Users per 100 population and ICT index of a country.

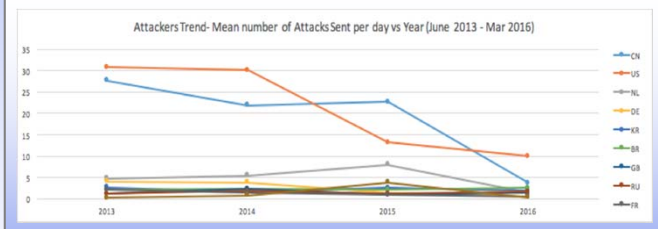
Variable Description	Correlation	Significance	Euclidean Distance
Network: Alliance_Hostility	0.**023**	0.000	101901.944
Network: common_language_network	-0.009	0.181	101906.443
Network: corruption_network	0.**029**	0.004	101883.500
Network: Country_to_Country_Average_Sentiment	0.014	0.024	101897.645
Network: GDP_PC_Difference	0.**032**	0.013	2688571.100
Network: Internet_Bandwidth_Difference	0.**116**	0	60197247.030
Network: min_distance_network	0.008	0.150	702619.996

QAP correlation indicate low correlation with Internet bandwidth, GDP per capita difference, Corruption index network and Alliance hostility network.

Cyber-Attacks Trend



Attacks target trend indicates that the average number of DDoS Attacks per day on the USA decreased from 2014 (108.5) to 2015 (54.6). In contrast, attacks on some European countries like France has increased 2014 (17.5), 2015 (22.8) to 2016 (43.08).



Attackers trend indicates that the attacks originating from the USA, China, Netherlands and Germany decreased in last three years, but attacks from other countries have remained stable.

Discussion & Future Work

•US was the top target of DDoS attacks during June2013 to Mar 2016. US received 23832 attacks, followed by China (10670 attacks), Peru (3530 attacks), France(3270 attacks) and Canada (3043 attacks).
•Majority of attacks originated from China (20,443 = 27.4%) attacks followed by the USA (20356), Netherlands (5436), Germany (2695),Korea (2122) and Brazil (1926).
•Average number of DDoS Attacks per day on the USA decreased from 2014 (108.5) to 2015 (54.6). In contrast, attacks on European countries like France increased 2014 (17.5), 2015 (22.8) to 2016 (43.08).
•Attacks originating from the USA, China, Netherlands and Germany decreased in last three years, but attacks from other top attacking countries like South Korea, Brazil, UK and Russia remained stable.
•DDoS attack are more concentrated in high internet bandwidth countries (Corr: 0.53, pval = 0.00).
•Weak correlation (Corr=0.032, P = 0.013) of cyber attacks network with GDP network (per captia difference) indicates wealth (economic) difference to be an important factor.
•Alliance hostility network shows a very weak correlation (Corr= 0.023. P = 0.00) with cyber attacks network. This is contrary to our expectation. Need to relook at our alliance hostility network data and explore the relationship further.

This work was supported in part by the NSA under Award No. H9823014C0140, by a MURI N000140811186 on adversarial reasoning, and the Center for Computational Analysis of Social and Organization Systems (CASOS). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the National Security Agency, the Office of Naval Research, or the U.S. government.