The Impact of US Cyber Policies on Cyber-Attacks Trend

Sumeet Kumar*, Matthew Benigni†, Kathleen M. Carley†
*Department of Electrical and Computer Engineering
†School of Computer Science
Carnegie Mellon University
5000 Forbes Ave, Pittsburgh, PA 15213, USA
Email: {sumeetku@cmu.edu, (mbenigni, kathleen.carley)@cs.cmu.edu}

***Abstract*—There is a general belief that cyber attacks on the United States are increasing, as indicated by the 30% increase in cyber-attack related news from 2014 to 2015. During the same time frame, however, the USA government enacted several policy measures meant to reduce or mitigate cyber-attacks. These recent developments have lead us to ask two questions, a) Have cyber-attacks on the United States actually increased, as perceived in the news media? b) What is the impact of changes in US cyber-policy on this trend in cyber-attacks? Our initial investigation reveals that in contrast to the perception, there has been a drop in the number of DDoS cyber-attacks on the USA.**

In this research, we compare the perceptions and the reality of cyber attacks by considering recent trends in cyber-related news and cyber-attacks (specifically DDoS type attacks). The analysis makes three important contributions: a) Using GDelt data, we show that from 2014 to 2015 the amount of news referring to cyber events have increased, but the sentiment expressed in such news has become more negative. b) Using DDoS-attacks data shared by Arbor Network, we show that from 2014 to 2016, there has been a marked decrease in the number of cyber-attacks on the USA. c) Using a time series intervention analysis, we show that the decline in cyber-attacks appears to be related to the changes in US cyber policy. In particular, the US President's authorization to prosecute malicious cyber actors significantly decreased the DDoS-attacks on the US.

I. INTRODUCTION

The internet has brought people and services together by making information exchange easier and faster. However, because of that information's value, these services have become a target of cyber threats, and these threats are a challenge to defeat. Malicious attacks are cheap, easy [1] and often pose little risk in terms of attribution [2], but their impact is significant [3]–[5]. Not surprisingly, this has lead many governments to develop organizations and policies designed to improve cyber defense. The increased emphasis in cyber-related policy is well placed, but effectiveness should be assessed empirically.

Cyber attack tactics and techniques have been studied extensively [6], [7], and cyber-policies have received a great deal of attention as well [8], [9]. However, little has been done to examine the relationships between cyber-policies and cyber-attacks. We address this deficit using a two-step strategy. Using GDelt news data [10], we first find the trend of news related to cyber-attacks and the sentiment associated with such news. This news corpus analysis provides an insight into media perceptions with respect to cyber attacks, and helps to identify major cyber-related events in time. We then consider cyber attacks as a time series using Arbor Network data. We examine the link between changes in attack rates or trends and important changes in the United States' cyber policy, and argue this type of analysis offers a means to assess the effectiveness of cyber policies. An assessment of this type lays the groundwork for understanding the relationship between cyber policies and the consequent changes in reality of cyber attacks. As such, this study may be useful in helping to formulate future cyber-policies and to assess their impact.

This paper is organized as follows. First we discuss related work (sec II). Then in section III, we describe our data sources. In section IV, we show the news trend and the trend of sentiment associated with such news. In the next section (V), we use Arbor Networks data to observe cyber-attack trends. In section VI, we use intervention analysis to find the impact of important cyberspace events. Finally, we present a conclusion and suggest future directions for this type of research.

II. RELATED WORK

A. Cyber Attacks

Gen. Keith Alexander, former director of the National Security Agency and commander of United States Cyber Command, argued that cyber theft constitutes the "greatest transfer of wealth in history" [11]. It is estimated that the actual damage by cyber attacks on world economies could run in billion of dollars [9]. Some recent events highlight the impact of cyber attacks [3], [5], [9], [12].However, because it is also difficult to quantify the value of and risk associated with breaches of information security, the exact impact of attacks is difficult to measure. To add to the complexity, cyber-attacks are often unreported by companies and organizations in an attempt to minimize financial loss. In a few cases, cyber-attacks directly impact public services. For example, the Estonia cyber attack in 2007 had a devastating [4] impact on the country. It resulted in temporary degradation or loss of service for many commercial and government servers and, lasted for around twenty-two days. In this attack, DDoS was considered to be the primary tool for disruption. There are other more recent examples as well. A recent notable theft was the data compromise of the US government Office of Personnel Management information [13], in which background investigation records of 21.5 million Federal employees and contractors was stolen.

B. Cyber Policies

Lipson [2] argued that tracking and attributing cyber-attacks is 'primitive at best' in today's network architecture, and

Shackelford [14] used the Estonia example to highlight that the absence of enforcement provisions in international law has made cyber attacks difficult to litigate, even when attribution is known. In the case of large-scale, state-sponsored cyber crime we note that even though it may be difficult to identify specific attackers or attack origins, effective policy should be identifiable due to longitudinal changes in attack trends. Collectively this work speculates a relation between policies and attacks trend.

C. Intervention Analysis

Policies are in effect interventions designed to change behavior. To gauge the impact of such policies, given longitudinal data, intervention analysis can be used. Box et al. [15] used intervention analysis with applications to two problems, first dealing with a photochemical smog data in Los Angeles, USA and the second with changes in the consumer price index. Endersa1 et al. [16] used intervention analysis to understand the effectiveness of anti-terrorism policies. They found that policies designed to reduce one type of attack may affect other attack modes because of complements and substitutes of attacks. In this paper, we use intervention analysis to assess the impact of changes in the USA's cyber policy on the perception and reality of cyber-attacks. We use the library shared by Brodersen et al. [17] for measuring causal impacts.

III. Datasets

We generate our dataset from two sources. The first source is the events data from Gdelt news [10]. We used the everyday-event files shared by GDelt to find the trends in cyber news, and the sentiment expressed in those news items. Our second source is the ddos-attacks data from Arbor Networks [18]. Arbor Networks and Google Ideas together created the website (www.digitalattackmap.com) to visualize global DDOS attacks threat. In addition to visualizing recent attacks, the site also allows users to explore historical trends of attacks. We use Arbor Networks data collected from website (www.digitalattackmap.com) to quantify cyber-attacks trend.

IV. News Trend and Sentiment Analysis

The GDlet project [10] monitors the world's broadcast, print, and web news every day to create an open dataset. The dataset is comprised of events and knowledge graphs, and contains data for more than 12,900 days. We use GDelt events database that consists of over a quarter-billion records organized into a set of tab-delimited files by date. These events are mostly from news sources and, contain a date, the URL of news source, the actors involved, the overall sentiment and many other useful fields. Starting April 1, 2013, GDelt creates a daily file shared in zipped csv format. Since our attacks data starts from June 2013, we only use the gdelt data starting June 2013.

We filter all GDelt event data based on their URL to retrieve cyber events. Only if the URL contains the word 'cyber', we use that event in our analysis. Given that many news sources use news-heading in their URL, we expect such a sampling to give a reliable representation of cyber-events. We call this filtered news set *cyber-news* in rest of the paper. An alternate approach of creating cyber-news is to browse all URLs in the GDelt events, to find if they relate to cyber. This method not feasible given the vast amount of data that is available in the news media.

1) News Trend: To obtain a trend of cyber-news, we plot the percentage of new articles that are related to cyber each day. The trend of cyber-news is shown in Fig:1. The red line represents the percentage of cyber-news in the total news. The blue line indicates the yearly average. Because year 2016 data is available only for four months, it is expected to be less accurate than other years.

From the trend (Fig:1), we can observe that the average daily cyber-news has increased form 2013 to 2014 (by 20%) and from 2014 to 2015 (by 30%). There was a slight decrease from 2015 to 2016 (by 9.9%), but since we only have first four months data for 2016, the trend may change.

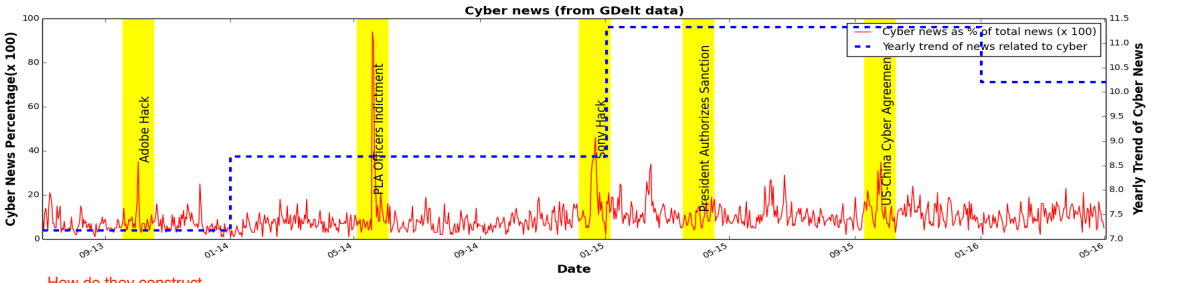
2) Sentiment Trend: For each article collected by Gdelt project, the Gdelt engine also computes a sentiment score (tone). The tone ranges from -100 (extremely negative) to 100 (extremely positive), but common tone values range between -10 and +10, with 0 indicating neutral. The trend of tones of cyber-news is shown in Fig:2. To create the plot, we averaged the tone for each day, i.e. (Sum of tones of all articles published in a day / Total number of articles published in a day). In the plot (Fig:2), the red line indicates the daily-average tone and the blue line indicates the yearly-average tone. We can observe that tone of cyber-news has gone more negative from 2014 to 2015 (by 28.9%) and, from 2015 to 2016 (by 6.6%). Reverse approach: identify events with spikes

3) Finding important cyber events: We can find important events in the cyber world by observing the significant changes in volume or sentiment with respect to cyber-news. Our analysis finds these changes are related to cyber-events or cyber-policy decisions. In this analysis, we used visual inspection to find the significant change points (spikes), but it can easily be automated using any peak detection algorithm. To find the event related to an anomaly, we use the advanced feature of Google news search. We take the spike time and create a time window of two weeks around the spike. We then use Google news advanced-search to search 'cyber Attacks' for that time frame. Google returns many news stories and topics as a result of the search, and we select the top topic as the event. For the sake of demonstration, we have highlighted some of the spikes and associated events in the trend plot (in Yellow). More details on these events are in section VI. Opposite Trends: Why?

Using the two plots (1, 2), we can say that news related to cyber-attacks are increasing, and the sentiment associated with cyber-news are getting more negative. This trend is in contrast to the cyber-attacks trend, that has decreased over last three years, as we will see in the next section.

Limitations: We would like to highlight that GDelt Tone analysis is not completely transparent. We observed a change in scale of tone around Feb-March 2015 time frame. Before Feb 2015, the average tone score is almost always positive, but after March 2015 the average tone is almost always negative. To get a continuous trend, we inverted the average tone score before Feb 2015. Note that since this work mostly uses peaks

Obvious Bias: GDELT reports about any cyber-related events not only the attacks



How do they construct a yearly trend?

Note the second scale here

Fig. 1: Cyber-News Trend and Yearly Pattern

Can we statistically test the difference between the average intensity of cyber-related news across different years?

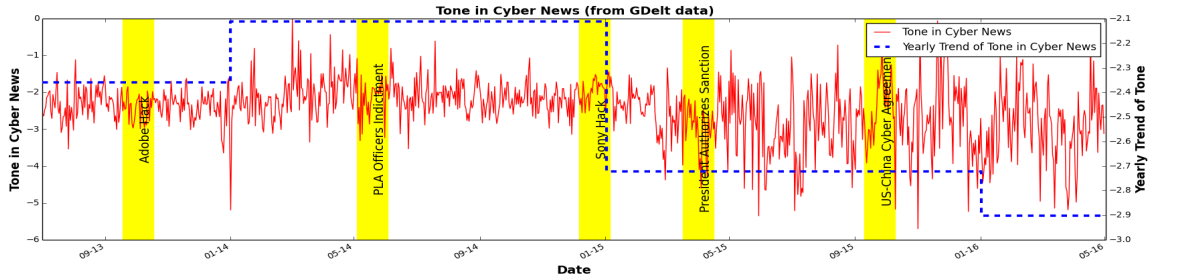


Fig. 2: Sentiment in Cyber-News and Yearly Pattern

in news and tone trend, tone scale change is unlikely to impact the major conclusions.

V. Attacks Trend and Analysis

Distributed Denial of Service (DDoS) attacks have been used in many high-profile cyber attacks and have evolved over the years. In a DDoS attacks, attackers try to overwhelm a service with multiple requests so that the legitimate users cannot gain access. More recently, they are increasingly being used as a diversionary tactic, wherein in the cover of DDoS attacks, attackers inject malware into the network.

For this study, We use the data shared by Arbor Networks on website www.digitalattackmap.com to analyze attacks trend. The website mentions that the shared data captures the top 2% of DDoS attacks reported by Arbor Networks; however, we will show that even this sample is enough to correlate changes in attack trends with cyber-policy decisions. Note that because a comprehensive dataset on other types of attacks is not available (at least not known to us), this study is limited to DDoS attacks data.

Fig:3 shows the trend in DDoS attacks received by the USA from other countries. In addition to the attack bandwidth trend (left axis), we also show the yearly average number of attacks. The trend shows that there is an increase in attack on the USA from 2013 to 2014 (61%), and then, a decrease in attacks from 2014 to 2015 (50%) and again a decrease in attacks from 2015 to 2016 (55%). A similar decreasing trend (Fig:5) was observed for self-attacks i.e. attacks originating from the USA and targeting the USA. The attacks decreased by 50% from 2013 to 2014, and again decreased by 50% from 2014 to 2015. If we consider attacks which are originating from the USA and are targeting other countries (Fig:4), we again see a decreasing trend from 2015 onward. But the decrease in attacks originating from the USA from 2015 to 2016 (18%), is not as significant as the decrease in attacks originating from other countries (55%).

VI. Impact of Policy Changes

The impact of an event or a policy change can be analyzed using Intervention analysis. In this research, we used intervention analysis to understand the effect of three cyber-policy related events. The three interventions (see section:IV) and their date of occurrences are listed below.

a) US indicted five PLA officers on 5/19/2014 (PLA Officers Indictment): The USA Department of Justice charges five Chinese military hackers for cyber espionage against U.S. Corporations and a Labor organization for commercial advantage. More information is available on the department of Justice website [19].

b) The president authorizes sanctions against malicious cyber actors on 4/1/2015 (President Authorizes Sanction). More information is available on the WhiteHouse website. [20].

c) US China cyber security agreement signed on 9/25/2015 (US-China Cyber Agreement): President Xi Jinping of China and President Barack Obama reached a Cyber Agreement, during China's president state visit in September 2015 [21].

The general idea behind intervention analysis is to use time-series data for a time-range before intervention, and develop a model that quantifies uncertainty associated with future time periods. In this research, we use DDoS-attacks data to build a model, and then use the model to predict future outcomes. If there is a large deviation in the prediction and the actual trend after the intervention point, we attribute the change in behavior to an intervention. For our analysis. we use R library 'CausalImpact' shared by Brodersen et al. [17] for

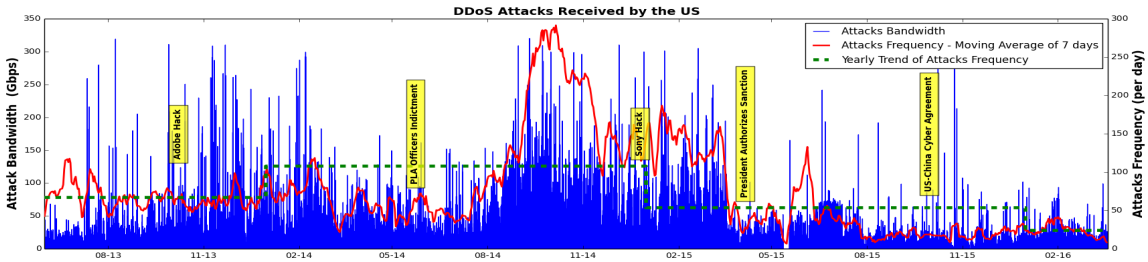


Fig. 3: DDoS Attacks Trend: Total Attacks Received by the USA

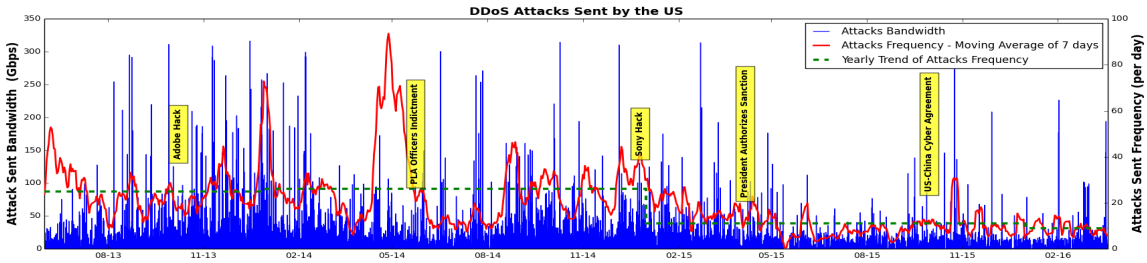


Fig. 4: DDoS Attacks Trend: Attacks Sent by the USA

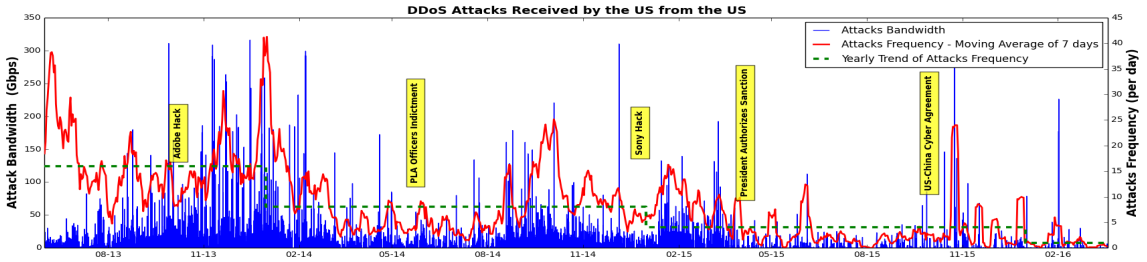


Fig. 5: DDoS Attacks Trend: Attacks Received by the USA and originating from the USA

inferring causal impact. We use a four months time window (two before and two after the event) to estimate the impact. 'CausalImpact' is based on state-space model, establishes a relationship between covariates and treated time series, and uses Markov chain Mote Carlo for posterior inference. Like other no-experimental approaches to causal inference, 'CausalaImpact' also makes some strong assumptions. It assumes that the relationship remains stable throughout the post-period, based on which 'CausalaImpact' allows a causal attribution even without a randomized experiment. Next, we use 'CausalImpact' to analyze the impact of various events.

The Table:I summarizes the intervention impact scores using attacks-frequency. A similar analysis using attacks-bandwidth trend, another way to measure ddos-attacks, is summarized in Table:II.

TABLE I: Intervention Analysis using Attacks Frequency

	Attacks From US	**US Self Attacks**	**Attacks on US**
Indictment	-74% p = 0.001	-31% p = 0.024	+12% p = 0.098
Sanction	-44% p = 0.001	-29% p = 0.048	-25% p = 0.009
Agreement	+36%. p = 0.001	+150% p =0.001	+8% p = 0.194

TABLE II: Intervention Analysis using Attacks Bandwidth

	Attacks from US	**US Self Attacks**	**Attacks on US**
Indictment	+35% p = 0.164	-48% p = 0.064	+99% p = 0.003
Sanction	-46% p =0.069	-58% p = 0.041	-59% p = 0.012
Agreement	+77% p =0.159	+83% p = 0.004	+19% p = 0.356

Next we analyze the three events in detail.

1) Impact of PLA Officers Indictment: Following the PLA Indictment event (fig:6), based on 'CausalImpact' model, we would have expected an average daily-attack frequency of 52, with a 95% interval of [43, 61]. However, the attack frequency had an average value of 58. In relative terms, the attacks frequency showed an increase of +12%. The 95% interval of this percentage is [+6%, +28%]. This means that, although the intervention appears to have caused a positive effect, the positive effect observed during the intervention period is not statistically significant (p = 0.098) and is likely to be due to random fluctuations.

Based on attack-bandwidth trend, following the PLA Indictment event, we would have expected an average attack bandwidth of 154.24Mbps, with a 95% interval of [53.26

Mbps, 259.87 Mbps]. However, the attack bandwidth had an average value of approx. 307.52 Mbps. The causal effect the intervention had on the attack bandwidth is 153.28 Mbps with a 95% interval of [47.64Mbps, 254.26Mbps]. The probability of obtaining this effect by chance is very small (Bayesian one-sided tail area probability p = 0.003). This means the causal effect can be considered statistically significant.

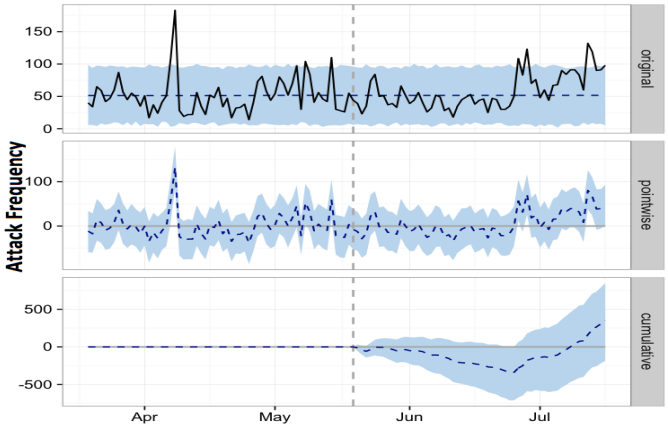


Fig. 6: Analysis of PLA indictment event

To summarize, using attacks-bandwidth trend, the PLA indictment event was followed by a +99% increase in cyber-attacks bandwidth trend, and is statistically significant (p = 0.003). Using attacks frequency, the event increased attacks frequency by 12%, however, the impact cannot be considered significant (p = 0.098).

2) Impact of Presidential sanction: Following the Presidential sanction event (fig:7), based on 'CausalImpact' model, we would have expected an average daily-attack frequency of 75, with a 95% interval of [59, 92]. However, the attack frequency had an average value of 56. In relative terms, the attacks frequency showed a decrease of -25%. The 95% interval of this percentage is [-47%, -4%]. This means that the positive effect observed during the intervention period is statistically significant (p = 0.009) and is very unlikely to be due to random fluctuations.

Based on attacks bandwidth trend, following the 'Presidential sanction' event, we would have expected the attack bandwidth to be 205.76 Mbps, with a 95% interval of [100.93Mbps, 316.61Mbps]. However, the attack bandwidth had an average value of approx. 84.09 Mbps. The 95% interval of this counterfactual prediction is [100.93Mbps, 316.61Mbps]. Subtracting the predicted value from the observed response yields an estimate of the causal effect the intervention had on the response variable. This effect is -121.67 Mbps with a 95% interval of [-232.52Mbps, -16.84Mbps]. This means that the negative effect observed during the intervention period is statistically significant. The probability of obtaining this effect by chance is very small (Bayesian one-sided tail-area probability p = 0.012).

To summarize, using attacks-bandwidth trend, the Presidential sanction was followed by a 59% decrease in cyber-attacks trend, and is statistically significant (p = 0.012). Using attacks

How good is the prediction model?

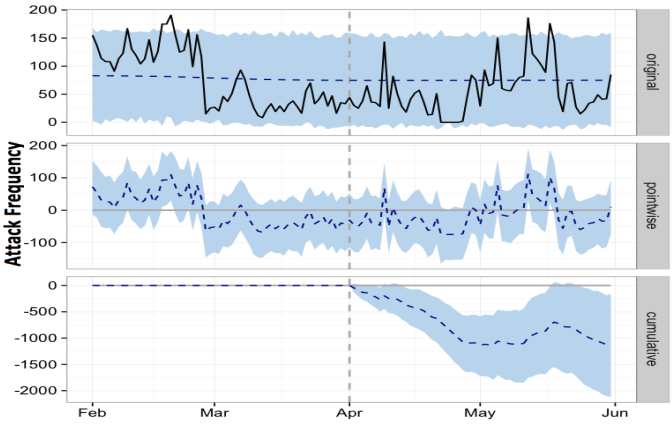


Fig. 7: Analysis of Presidential Sanction

frequency, the event decreased attacks frequency by 25%, and the impact could be considered significant (p = 0.009).

3) Impact of US China cyber security agreement: Following the cyber security agreement (fig:8), based on 'CausalImpact' model, we would have expected an average daily-attack frequency of 18, with a 95% interval of [15, 22]. However, the attack frequency had an average value of 20. In relative terms, the attacks frequency showed an increase of +8%. The 95% interval of this percentage is [10%, +25%]. This means that, although the intervention appears to have caused a positive effect, the positive effect observed during the intervention period is not statistically significant (p = 0.194) and is likely to be due to random fluctuations.

Based on attacks bandwidth trend, following the 'US China cyber security agreement', we would have expected the average attacks bandwidth to be the 246.65 Mbps, with a 95% interval of [3.29Mbps, 491.39Mbps]. However, the attack bandwidth had an average value of approx. 292.84 Mbps. Subtracting this prediction from the observed response yields an estimate of the causal effect the intervention had on cyber-attacks bandwidth. This effect is 46.2 Mbps with a 95% interval of [-198.54Mbps, 289.55Mbps]. This means that, although the intervention appears to have caused a positive effect, this effect is not statistically significant when considering the entire post-intervention period as a whole. The apparent effect could be the result of random fluctuations that are unrelated to the intervention. The probability of obtaining this effect by chance is p = 0.356.

To summarize, using attacks-bandwidth trend, the 'US China cyber security agreement' was followed by a +8% increase in cyber-attacks trend, and is statistically not significant (p = 0.194). Using attacks frequency, the event increased attacks frequency by +19%, and again, the impact could be not considered significant (p = 0.356).

VII. CONCLUSION AND FUTURE WORK

In this research, we used cyber-related news from Gdelt and, compared the news trend with DDoS cyber-attack data from Arbor Network. Our analysis highlights that although cyber-related news increased by 30%, there was 50% decrease in DDoS cyber-attacks on the USA from 2014 to 2015. When we considered attacks originating from the USA and targeted

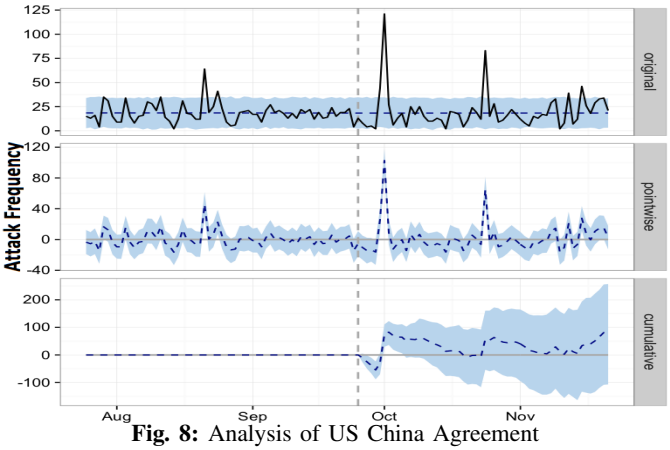


Fig. 8: Analysis of US China Agreement

to other countries, and observe that the reduction is not as significant as the decline in attacks originating from other nations and targeted to the USA. We also found the decline in cyber-attacks could be linked to a few US cyber policy using time series intervention analysis. Using global ddos-attacks data available on www.digitalattackmap.com, the study argued that the 'Presidents authorization to prosecute malicious cyber actors' had the largest impact on decreasing the attacks. Using trend of attacks-bandwidth, we observed that the event was followed by a decrease in cyber-attacks by 59% and the causal effect was significant (p = 0.012). If attacks-frequency was used, again a strong decrease (-25%, p = 0.009) was observed. 'The indictment of five PLA officers' event followed by an increase in the attacks by +99% (+12% in attacks frequency) in two months, and the effect observed by the intervention was again statistically significant (p = 0.003). Finally, the 'US-China cyber-security' agreement had the smallest quantitative impact on cyber-attacks. The agreement followed by an increase in cyber-attacks by +19% (+8% in attacks frequency), but the effect may not be considered statistically significant (p = 0.356).

To summarize, this research is unique in that it quantitatively analyzes the impact of cyber policies on both the perception and the reality of cyber attacks. This study finds that as new policies have been enacted there is a growing discussion of cyber issues in the news, and a growing negative sentiment, yet a decrease in actual DDoS attacks. This suggests that while embracing new policies may serve to decreases the number of actual attacks, the creation of such policies increases awareness of the attacks and stirs the sentiment against such attacks. Thus, we find that the major news sources portray cyber-attacks as a major and increasing concern, but in reality, the total cyber-attacks on the USA and, the number of cyber-attacks sent by the USA have been going down. The analysis concludes that 'The Presidential Sanction' considerably decreased the cyber-attacks and has positively impacted the cyber threat situation.

VIII. Acknowledgments

This work was supported by the NSA under Award No. H9823014C0140 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 or the U.S. government.

References

[1] P. Shankar, "DoS Attacks and free Dos attacking tools." [Online]. Available: http://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/

[2] H. F. Lipson, "Tracking and tracing cyber-attacks: Technical challenges and global policy issues," DTIC Document, Tech. Rep., 2002.

[3] E. Nakashima, "US Target of Massive Cyber-Espionage Campaign," *Washington Post*, 2013.

[4] R. Ottis, "Analysis of the 2007 cyber attacks against estonia from the information warfare perspective," in *Proceedings of the 7th European Conference on Information Warfare*, 2008, p. 163.

[5] G. O'Hara, "Cyber-Espionage: A growing threat to the American economy," *CommLaw Conspectus*, vol. 19, p. 241, 2010.

[6] "Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis." [Online]. Available: https://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764

[7] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.

[8] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante, "Dimensions of cyber-attacks: Cultural, social, economic, and political," *Technology and Society Magazine, IEEE*, vol. 30, no. 1, pp. 28–38, 2011.

[9] J. Lewis and S. Baker, "The economic impact of cybercrime and cyber espionage," *Center for Strategic and International Studies, Washington, DC*, pp. 103–117, 2013.

[10] K. Leetaru and P. A. Schrodt, "Gdelt: Global data on events, location, and tone, 1979âĂŞ2012," in *ISA Annual Convention*, vol. 2. Citeseer, 2013.

[11] J. ROGIN, "NSA Chief: Cybercrime constitutes the âĂIJgreatest transfer of wealth in historyâĂİ," *http://foreignpolicy.com*. [Online]. Available: http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

[12] S. Kumar and K. M. Carley, "DDoS Cyber-Attacks Network: Who's Attacking Whom," in *Intelligence and Security Informatics (ISI), 2016 IEEE International Conference on*, Tucson, Arizona USA, Sep. 2016.

[13] O. , "OPM recently discovered two separate but related cybersecurity incidents." [Online]. Available: https://www.opm.gov/cybersecurity/cybersecurity-incidents/#WhatHappened

[14] S. Shackelford, "From nuclear war to net war: analogizing cyber attacks in international law," *Berkley Journal of International Law (BJIL)*, vol. 25, no. 3, 2009.

[15] G. E. Box and G. C. Tiao, "Intervention analysis with applications to economic and environmental problems," *Journal of the American Statistical association*, vol. 70, no. 349, pp. 70–79, 1975.

[16] W. Enders and T. Sandler, "The Effectiveness of Antiterrorism Policies: A Vector-Autoregression-Intervention Analysis." *American Political Science Review*, vol. 87, no. 04, pp. 829–844, 1993.

[17] K. H. Brodersen, F. Gallusser, J. Koehler, N. Remy, and S. L. Scott, "Inferring causal impact using Bayesian structural time-series models," *Annals of Applied Statistics*, vol. 9, pp. 247–274, 2015.

[18] "www.digitalattackmap.com." [Online]. Available: http://www.digitalattackmap.com/

[19] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 2014. [Online]. Available: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[20] "Expanding Our Ability to Combat Cyber Threats." [Online]. Available: https://www.whitehouse.gov/blog/2015/04/01/expanding-our-ability-combat-cyber-threats

[21] J. Rollins, "U.S.âĂŞChina Cyber Agreement." [Online]. Available: https://www.fas.org/sgp/crs/row/IN10376.pdf