# Incompetents, criminals, or spies: Macroeconomic analysis of routing anomalies

Pablo Moriano[a,*], Soumya Achar[a], L. Jean Camp[a]

[a]*School of Informatics and Computing, Indiana University, Bloomington, IN 47408*

**Abstract**

Routing anomalies, beyond simple leaks, are occurring on the order of tens of thousands a year. These may be accidents, but there is anecdotal evidence that indicates criminal intent. There are case studies that illustrate the use of these for national intelligence. Any given anomaly could be an accident, a crime, or an attack. Although it is impossible to directly observe the motivation of those who generate these anomalies, aggregate data about the sources of these anomalies is available. Here we leverage tools of macroeconomics to provide insights into the possible nature of these anomalies. We offer an empirical investigation using multiple linear regression and unsupervised learning to analyze data over a four-year period in order to better understand the nature of routing anomalies. If routing anomalies are a result of limited technical competence, then countries with low levels of education, few technology exports, and less expertise should be over-represented. If routing anomalies are leveraged by criminals for profit, then economic theories and analytical approaches from criminology should show statistical significance. Or, if routing anomalies are primarily used by national intelligence agencies to attack either internal dissidents or those outside their borders, then the presence of conflict and measures of quality of governance are possible indicators. We examine anomalies as likely due to incompetence,

*Corresponding author

*Email addresses:* pmoriano@indiana.edu (Pablo Moriano), soachar@indiana.edu (Soumya Achar), ljcamp@indiana.edu (L. Jean Camp)

A final version of this paper was published in Computers & Security at https://doi.org/10.1016/j.cose.2017.06.011

potential ecrime, or intelligence operations using macroeconomics by leveraging three theories from criminology and global measures of technology adoption. We found that exports of technology were not statistically significant, undermining the argument for incompetence. We also found support for the possibility that anomalies are driven by crime, specifically for the guardianship and relative deprivation theories of crime. In addition to these findings from regression analysis, clustering indicates that civil conflict and surveillance are associated with the disproportionate origination of routing anomalies. This supports the possibility of use of routing anomalies for national intelligence.
*Keywords:* BGP Security, Prefix Hijacking, Ecrime, Surveillance, Macroeconomics, Statistical Modeling, Clustering Analysis

---

## 1. Introduction

Routing security is a complex technical, social, and economic problem. A given route anomaly may be an accident, a for-profit crime, or an intelligence operation. Understanding the economics and political dynamics of this threat can inform effective defenses. Solutions that mitigate risk from one possible source should not exacerbate the other. For example, a lack of expertise as a source of anomalies cannot be dismissed as an explanation out of hand. If so, security solutions that increase the complexity of network operations may perversely increase rather than decrease anomalies. Alternatively, trust models that are optimized to address for-profit crime may increase opportunities for intelligence operations.

This paper presents an empirical analysis to better understand the nature of routing anomalies. We began with three hypotheses: anomalies result from (1) a lack of technical expertise, from (2) criminal activity, or from (3) national intelligence operations. We determined the factors that would indicate expertise, criminality, and active intelligence, then operationalized these with linear regression and unsupervised clustering. We then identified correlations to reject (or not) these three possible explanations for anomalies. Using empirical data,

we could not reject the second or third hypothesis. Although we found evidence of correlation with the second and third, this is not, of course, causation.

More specifically, the method of this work is a longitudinal analysis of anomalous routing events. The analysis leverages macroeconomics, theories of crime, and unsupervised learning. Our empirical analysis explored the correlation of control-plane anomalies with indicators of expertise, ecrime, and national intelligence activity. We used publicly available data from Argus, which is an academic project dedicated to the detection of anomalies (Shi et al., 2012), for the dependent variable (i.e., anomalies). Macroeconomic variables, i.e., independent variables, are from the World Bank. These data sources and necessary preprocessing are detailed in Section 3.

Routing anomalies appear to be increasing (Vervier et al., 2015).[2] One possible explanation is that, as the Internet expands, the increase in routers and operators results in more routing errors. The expertise of individual operators is also increasingly diverse. Network engineers sometimes argue that the problem is that there is a decrease in the amount of average expertise among operators. Failures of technical competence may be inadvertent, but they can still be harmful.

Given the history of route leaks and challenges of usability in routing, we could not dismiss the hypothesis that anomalies other than leaks are also result of errors. To illustrate the similarities and differences between leaks and other anomalies, we provide several examples in the next paragraphs. A route leak occurs when a customer of two larger Internet service providers (ISPs) broadcasts each providers' route table to the other. Since larger ISPs prefer customer routes over non-customer routes, all traffic then tries to traverse the hapless customer resulting in loops and a lack of connectivity. A notable leak was that of a small Australian ISP in 2012; one which took the continent offline for hours. In this case, a small ISP obtained service from one ISP and back-up service from

[2]Routing anomalies are those incidents that happen on the control-plane at the Border Gateway Protocol (BGP) level.

the other. This small ISP then announced every route from each of these larger ISPs to the other. Telstra's routes were announced to Dodo, and Dodo's to Telstra. The two larger ISPs updated and began to dump all their traffic on the new, confused customer that had announced all the routes (Toonk, 2012). This outage was immediately apparent, and recovery was completed within hours. All three ISPs can be said to have directly suffered the outage but the entire continent was affected. This is a straight-forward failure of human factors and operational policy. It is so common that it has its own moniker: fat fingers.

Route leaks are difficult to prevent, but readily observable and overwhelmingly the result of technical errors. In contrast, when an entity purposefully misrepresents its location in a path, rather than inadvertently leaking, the errors are less obvious. A route hijack occurs when incorrect or misleading route information is published so that the paths of packets are perturbed. To distinguish hijacks from leaks we provide two examples of hijacks for crime (Bitcoin (Greenberg, 2014) and Domain Name System (DNS) resolvers (Dagon et al., 2008)). We also offer one example of a hijack that was the result political manipulation (Pakistan's censorship of YouTube (Hunter, 2008)), and one as yet unexplained anomaly (Facebook traffic through China (Kirk, 2011)).

Beyond operator and organizational errors, another explanation for anomalies is that hijacks can be used by criminals for profit. When a prefix is hijacked, traffic might continue to be delivered. Such routing configurations can remain stable for long periods. In addition, short burst of traffic can be difficult to detect. In one example, repeated BGP hijacks lasting only minutes were used to attack a collaborative of investors in digital currency. These hijacks leveraged the lack of authentication between miners of the digital currency Bitcoin and their coordinating mining pools to steal up to $9000 a day. (Bitminers form collaboratives where their shared processing power leverages economies of scale in Bitcoin transactions. Normally, coins that are created are transferred to the collective pool shared by the collaborators.) Using BGP to hijack traffic to hosting providers, including Amazon, the attacker directed the miners to place the coins into the attacker's pool. The hijacks were detected only after 22 bursts

over four months (Greenberg, 2014).

Another possible criminal use of hijacks is to pollute paths to DNS resolvers. Pollution of paths to DNS resolvers is an attack that has been widely observed and monetized (Dagon et al., 2008), although the attacks typically have not used BGP hijacking. The fact that control-plane disruptions have not been more widely commoditized may either reflect the inherent resilience of BGP or the shape of things to come.

Beyond crime, anomalies have been created by nations for political ends. Madory, for example, provides six vignettes of malicious hijacks, combining for-profit and national intelligence incidents (Madory, 2015).

A famous political control-plane incident was initiated by Pakistan in 2008, when Pakistan identified several YouTube videos as sufficiently problematic as to block all of YouTube. An internal address for YouTube was intended to be announced within Pakistan by Pakistan Telecom. Instead, it spread across northern Africa and Europe and denied access to YouTube for hours (Hunter, 2008). The intention to block within Pakistan was political, yet the diffusion of the information across the globe could be considered a human factors problem. The efficacy of attacks of nation-states on the reachability of the Internet for their residents was further illustrated during the Arab Spring, as rapid drop-offs for Egyptian and Libyan populations were easily observable but less easily repairable (Dainotti et al., 2011; Bowman & Camp, 2013).

In another more subtle case, Facebook traffic was routed through China. Facebook updates were not encrypted at the time. Thus, a significant amount of global traffic was routed via a nation where Facebook adoption is remarkably low (Kirk, 2011). At that time there were more than 100,000 American troops in two active conflicts in Iraq and Afghanistan whose updates were routed through the Great Firewall of China. The Department of Defense noted that a major concern during that time was troops inadvertently leaking information via posts about their activities on Facebook (Phillips et al., 2011), exactly the traffic that appears to have been hijacked.

The perception that such attacks are constant, often not detected, and rarely

reported motivates calls for a ubiquitous cryptographic solution (Wählisch et al., 2012). Yet, as the experience with certificate authorities issuing rogue X.509 certificates shows, political attacks and sheer incompetence are difficult to prevent and detect with an all-or-nothing cryptographic model of trust. Sometimes authorities are necessarily trusted for purposes of access, interoperability, availability, or even politics when their intent or competence does not indicate trustworthiness (Cooper et al., 2013).

In a nutshell, the nature and distribution of control-plane anomalies are rife with open questions, and some of these are political and economic questions which can inform the design of security solutions. Here we address the question of the role of ecrime and politics in BGP anomalies using macroeconomic analysis and unsupervised learning.

In addition to the results of the statistical analysis itself, we offer a framing through which to view the threat by drawing on the growing literature on ecrime. Using standard regression, we identify the variables that are found to be significantly correlated with the origination of anomalies. Our analysis found that the (1) density of secure Internet servers, (2) quality of national governance, and (3) density of broadband subscribers are significant while (4) per person wealth and (5) information technology workforce were not found to be statistically significant. (Correlation with the information technology workforce was instrumented using the World Bank data on the adoption and export of computer, communications, and related services.)

The next step in the analysis was to use the density of secure Internet servers and the quality of national governance in unsupervised learning. The goal of the unsupervised learning was to identify potential clusters and patterns that would not be apparent in regression analysis. The result was two clusters which showed highly developed and developing countries as distinct. More importantly, this complementary analysis found that these clusters reflect the importance of national conflict in the origination of routing anomalies.

The remaining sections are organized as follows. Section 2 discusses related work in empirical analysis of ecrime, BGP manipulation for political operations,

and routing security. Section 3 provides a description of the data sources (along with their preprocessing) and the statistical model that was used in the analysis. Section 4 shows the results of the cross-country longitudinal analysis and the identification of clusters. Section 5 discusses the implications of the results based on the assumptions made and their implications for the economics and politics of routing anomalies. Finally, Section 6 presents concluding remarks and areas for future research.

## 2. Related work

It is an open debate as to whether routing anomalies are primarily criminally motivated, used for political operations or, alternatively, a result of operator error. Consequently, this analysis is informed by past research on ecrime, manipulation of the Internet operation for intelligence operations, and routing security. Here, we provide an overview of related works in these three areas.

### *2.1. Ecrime*

Much of the research on ecrime has been strictly empirical. For example, Kanich et al. examined the value chain in pharmaceutical spam, where the payment services processors were identified as the weakest link (Kanich et al., 2008). This technical analysis enabled an effective policy response, significantly decreasing the prevalence of pharmaceutical spam. Christin focused on monetary returns rather than the mechanics of the attacks (Christin, 2013). That analysis of underground markets illustrated the stability of the supply of online narcotics and estimated the revenue of the market operators.

Nation and region of origin have been found to be relevant in analyses of spam, both by industry researchers (Microsoft, 2011) and academics (Garg et al., 2013). Macroeconomic analysis of malware illustrates the significance of state-level variables, including the economic variables that we use in the proposed research (van Eeten & Bauer, 2008; Garg & Camp, 2013). Our analysis also draws on three different criminology theories that have been correlated with the production of spam using macroeconomic techniques (Garg et al., 2013).

Afroz et al. provided a window into the geographic and political distribution of online crime by analyzing linguistic groupings in online criminal marketplaces (Afroz et al., 2013). Moore et al. examined temporal patterns and value chains in phishing and theft, providing guidance for coordinated law enforcement responses (Moore et al., 2009). Later work by van Eeten et al. considered the role of industry and national policies in the spam ecosystem (van Eeten et al., 2010). van Eeten et al. also found adoption of the guidance in Moore et al. to be correlated with a decrease in infected machines for ISPs in Europe.

Other related research investigates the relationship between short-lived BGP hijacks and malicious activities such as spamming and denial of service (DoS) attacks. Specifically, Clayton described pollution of registry databases by attackers (Clayton, 2015). This attack enabled miscreants to claim official ownership of IP space in order to subvert automatic filtering of invalid route announcements. These misidentified IP addresses were then used in spam and malware campaigns.

Additional empirical analysis had shown that a significant amount of spam is received from IP addresses that correspond to short-lived, possibly hijacked IP prefixes (Ramachandran & Feamster, 2006). Hu and Mao also discussed the possible use of BGP hijacks for conducting DoS attacks (Hu & Mao, 2007). The analysis of these types of attacks provides an interesting indirect link among the causal factors that are related to the origin of hijacks. More importantly, these findings suggested that BGP hijacks may be becoming part of the commoditized ecrime ecosystem.

### *2.2. Political operations*

There is evidence of the manipulation of the Internet control-plane with political intent. Earlier work analyzed the technical signatures around particular Internet censorship events, which can be considered political attacks on the Internet. In particular, Dainotti et al. presented evidence on how Internet communications were disrupted—through BGP-based disconnection—in several

North African countries in response to civilian protests and threats of insurrection (Dainotti et al., 2011).

Similarly, the use of deep packet inspection (DPI) has been examined as a political and technical phenomenon across different ASes. In particular, Asghari et al. identified the economic and political drivers that have a significant correlation with DPI (Asghari et al., 2012). This work found that high levels of governmental censorship and weak privacy protections are associated with a pervasive use of DPI.

The research presented here was also informed by insights from case studies of specific routing incidents. Hiran et al. analyzed the impact of the China Telecom incident in terms of the origin of prefixes that were announced (Hiran et al., 2013). In this incident, China Telecom claimed a significant percentage of the the IPv4 address space (Toonk, 2010). Their results suggest that most of the hijacked prefixes correspond to organizations in the U.S., followed by organizations in China, South Korea, Australia, and Mexico. After detailed inspection, they found that the U.S. shows a lower rate of hijacked prefixes based on the global distribution of Internet prefixes across the globe. Conversely, countries in the Asia-Pacific region (e.g., China, South Korea, Australia) were more affected by the incident based on the global distribution of prefixes.

Arnbak and Goldberg reported on the manipulation of BGP and DNS protocols to divert U.S. traffic abroad—where it can be collected under a different and more permissive jurisdiction (Arnbak & Goldberg, 2015). In addition, the manipulation of the BGP protocol to take network traffic through unusual paths has also been studied in several incidents (Benton & Camp, 2016). For example, Cowie described how traffic intended to be delivered from one Denver ISP to another Denver ISP was subject to a detour (through Iceland) and possibly interception or manipulation (Cowie, 2013). It is certainly difficult to believe such a detour was optimal when the endpoints were located in the same city.

These cases identify possible causal factors relating to political intentions in traffic redirection. More importantly, this previous research suggests that BGP hijacks may be becoming an attack vector for intelligence operations.

*2.3. Routing security*

The dependent variable in this work is the geographical distribution of routing anomalies. Thus, it is important to address the detection of such anomalies. Anomaly detection techniques have been used widely for the identification of routing incidents. The three current approaches for identifying routing anomalies can be categorized as (1) control-plane, (2) data-plane, or (3) hybrid.

Control-plane approaches examine inconsistencies at the router-level. Kruegel et al. detected malicious inter-domain announcements by analyzing the consistency of update messages with respect to the local network topology and the geographical location of ASes (Kruegel et al., 2003). Lad et al. suggested that anomalies can be identified simply by finding unique prefixes originating from multiple ASes—also known as Multiple Origin AS conflicts. This requires timely notification of the AS origin changes, i.e., using information provided by the owner of the prefix (Lad et al., 2006). In contrast, Khare et al. developed a method that correlates suspicious routing update messages with past network routing announcements (Khare et al., 2012). These control-plane methods have been shown to be effective in identifying very large-scale events but suffer from a large number of false positives (Zhao et al., 2001). If our data source had a large number of false positives, then the results would be biased by a higher correlation of issued updates being identified as malicious updates.

Data-plane approaches monitor changes in Internet traffic of the victim to detect anomalies. For example, Zheng et al. introduced a method to detect traffic path changes by sampling from multiple vantage points (Zheng et al., 2007). Building on this methodology Zhang et al. later proposed iSPY, a monitoring system that relies on the identification of prefix unreachability from a set of peer ASes (Zhang et al., 2010). Contrary to control-plane methods, data-plane approaches are able to detect any path changes in the traffic resulting in higher accuracy. However, traffic monitoring changes are mostly deployed at the AS neighborhood level and have not been proven at large-scale, i.e., they suffer from poor scalability (Xiang et al., 2011).

Hybrid approaches use control-based detection frameworks to inform data-

plane measurements. For example, the work by Hu and Mao identified anomalous routing updates by determining when a prefix is announced by multiple ASes and then examining associated data-plane information (i.e., verified through reachability of IP addresses using tools such as *traceroute*) (Hu & Mao, 2007). In this type of approach, the detection delay can be on the order of minutes. Later, Shi et al. proposed Argus, another hybrid approach (Shi et al., 2012). In contrast with the work by Hu and Mao, Argus correlates data-plane signatures (verified through *ping*) with reported control-plane anomalies over a given time period. This approach allows detection of a wider range of anomalies than those given by simply seeking a bad origin or path. Moreover, hijack detection delay is on the order of seconds.

For a comprehensive discussion on BGP hijacking detection methods, we refer the reader to the survey lead by Butler (Butler et al., 2010).

## 3. Methods

We performed a longitudinal cross-country empirical analysis of the macroeconomic factors that correlate with the number of IP prefixes associated with potentially malicious control-plane events. That is, we focused on the originators and not the targets of BGP control-plane incidents. In Section 3.1, we provide details on the data source and types of incidents we examined. In the following sections, we refer to the data on *hijacks and other anomalies excluding route leaks* as simply "anomalies" or "hijacks."

The research presented here is based on 322,466 incidents that were identified not only as anomalies but also as possible hijacks by Argus (Shi et al., 2012). This data may include false positives. A false positive, in this case, is the identification of a routing event as anomalous when it is not. Possible sources of false positives include route flapping, organizational changes, or unusual but not malicious responses to changes in the control-plane from outages or congestion. Our investigation is based on the argument that the possibility of BGP attacks systematically being used for profit and for surveillance cannot be dismissed.

BGP control-plane attacks as a tool for ecrime or espionage has implications for investments, policy, possible targets, and possible solutions.

We used macroeconomic variables that have been found to be relevant to global analyses of ecrime, grounded in traditional theories of crime (Pratt & Cullen, 2005), as well as prior research focused on understanding the economic incentives behind malware (Garg et al., 2013). We then used standard regression techniques, specifically multiple linear regression using ordinary least squares, to examine these theoretically important independent variables. As a dependent variable, we considered the number of hijacked IP prefixes that originated in a particular country using the data set provided by Argus. We analyzed data over a nearly four-year period, from 2011 to 2014.

Following our identification of the significant variables, we used cluster analysis to further explore the relationships among those variables. We identified two clusters, one of affluent, highly developed countries and one of less wealthy nations. These clusters show the importance of governance indicators in the number of anomalies originated in a given country.

### *3.1. Data sources*

In this section, we will detail all of the data sources (along with their preprocessing) that were used to perform the analysis. We start by describing the independent variables and dependent variable, then the statistical model used to arrive at the results.

#### *3.1.1. Independent variables*

The independent variables used in this research are based in traditional theories of crime, in particular: (*i*) routine activity theory, (*ii*) economic deprivation, and (*iii*) social support (also known as altruism theory). These variables have been instrumented using publicly available data from the World Bank.[3] Although there is a dispute over the way some of these measures are implemented, biases in these measures are likely consistent across countries and over time.

[3]Available for public download at `http://data.worldbank.org/`

The World Bank provides a consistent and systematic measure of country-level macroeconomic variables, and has been used widely in economic, criminology, and jurisprudence research (Ika et al., 2012). Equally important, the World Bank provides uniform and consistently available measures that are likely to be reproduced by other researchers. We grouped the independent variables into factors and described them in detail below (see Table 1).

The routine activity theory of crime states that the probability of a crime is a function of motivated offenders, available targets, and lack of guardianship (Felson & Cohen, 1980). The first independent factor is **availability** of users, i.e., a larger population of Internet users is more likely to produce more hijack attacks. This means that we make no assumptions about the distribution of motivation between categories or classes of users but rather assume that with more users there is a larger pool of people who could be motivated to commit online crime. To determine if this is a significant variable, we considered the number of fixed broadband Internet subscribers (FBIS) in a given country. We normalize the number for comparisons across countries by evaluating the number of fixed Internet broadband subscribers per 100,000 people (FBISper100).

A second independent factor is **guardianship**. Guardianship has been modeled in other works as community oversight. High guardianship indicates that the community has and enforces norms of non-criminal and safe behaviors. In the case of online crime, this can be indicated by private investments in the existing information and communications technology (ICT) infrastructure. We operationalized this factor using the measure of secure Internet servers (SIS) and SIS per million people (SISperM) to account for the differences in population. The World Bank defines SIS as "servers using encrypting technology in Internet transactions."

Economic deprivation theory suggests that crime is driven by blocked legitimate opportunities or **economic** deprivation (Blau & Blau, 1982). This is the third independent factor in our analysis, and the only factor we examine for the economic deprivation theory of crime. Certainly, a lack of economic opportunity encourages individuals to perform criminal activities if these are profitable. To

measure this factor, we consider the gross domestic product (GDP) per capita by purchasing power parity (PPP). Simultaneously, GDP per capita by PPP (GDP PPP) indicates the relative deprivation with respect to other countries given the low cost of global connectivity.

The social support or altruism theory posits that an individual lack of economic resources can be alleviated by appropriate **governance** through public investments (Cullen, 1994). This motivates the inclusion of a fourth independent factor in our analysis. For ecrime, government influences take the form of subsidies or incentives for the adoption of technologies. Conceptually, when a governance environment encourages the adoption of technologies, it also encourages increased access to ICT technologies. Under the altruism theory of crime, this would also decrease the incentive for routing attacks. To capture this factor, we operationalized government support using a subset of World Governance Indicators (WGI) (Kaufmann et al., 2011). The subset we included consists of (1) government effectiveness, (2) regulatory quality, (3) rule of law, and (4) control of corruption, i.e., perception of corruption within a country. Government effectiveness captures the perceived quality of the services, policy formulation, and the credibility of the governance. Regulatory quality refers to the perceived degree of alignment toward the development of the private sector. Rule of law measures the degree to which the legal framework is operationalized in practice. For example, corruption can decrease the effectiveness of the legal framework. Control of corruption measures the misuse of public power for private gain.

Finally, recall that one possible explanation of routing anomalies is a lack of **technical competence**. This is the fifth and final independent factor. Superior governance in the specific domain of ICTs would be indicated by high levels of local expertise. Local expertise and ability in computing is commonly identified in macroeconomic analysis by higher levels of exports in those industries. To measure local skills, we used the percentage of exports of computers, communications, and other services (CCS) as the corresponding macroeconomic variable. This measure is intended to quantify the degree to which a country has developed ICT markets. A larger ICT market implies more personnel who

are trained in basic security practices. In fact, hijacking routes requires a minimum level of expertise in security and minimum technological requirements to perform, particularly in comparison with simple email confidence scams such as advance fee fraud. In contrast, creating a route leak requires a lack of expertise or due care. We recognize that guardianship and competence interact, and address this in our analysis.

*3.1.2. Dependent variable*

The dependent variable corresponds to the number of unique affected IPv4 prefixes by country (based on the origin of the malicious prefix), i.e., each event corresponds to a prefix being rerouted. We depended upon the Argus data set for the identification of anomalies. For the purpose of collecting routing anomalous events, we compiled data over the 43 months from June 2011 to December 2014 from the Argus[4] API, as of December 20, 2015 (Xiang et al., 2011; Shi et al., 2012).

Argus defines three categories of anomalies. Specifically, the data we used relies on the output of the Anomaly Monitoring Module (AMM). The AMM detects (1) origin, (2) adjacency, and (3) policy anomalies. An origin anomaly is detected when an AS is advertising a prefix that it does not own. To identify origin anomalies, Argus maintains a database that tracks the expected origin of prefixes. An adjacency anomaly occurs when there is a path which has two AS numbers that are not normally seen to be connected. This could be considered a bad or an unlikely hop. To detect adjacency anomalies, the AMM monitors changes in AS-path segments. Given the exponential number of possible combinations of segments in the updates, the AMM only verifies neighboring pairs in an AS-path. To detect policy anomalies, the AMM takes into account the type of commercial relationship between ASes. Specifically, customers are not expected to announce routes from their providers. A bad segment of three hops means a policy anomaly. Note that by considering these three types of

[4]Available for public download at `http://argus.csnet1.cs.tsinghua.edu.cn/`

anomalies, the AMM is able to detect a wide range of hijacks and other events.

Based both on Argus' description of their practices and the sheer number of events reported, we can assume flapping is filtered out. (Flapping occurs when a route oscillates between two or more possible paths that are themselves relatively stable.) We do acknowledge that some BGP alarms might be due to benign BGP engineering practice or misconfiguration, including events specifically classified as anomalous in this data. The common characteristic of the incidents examined below is that the IP prefixes and ASes are used to divert Internet traffic.

The hijacks reported by Argus are based on a mixed strategy between control- and data-plane methods, i.e., it correlates control-plane anomalies and data reachability to improve detection accuracy. This strategy enables Argus to distinguish hijacks from other types of anomalies. In the subsequent analysis, we did not consider the effects of the false positives detected by the Argus system. That is, we assumed that each anomaly identified by Argus was, in fact, identified correctly.

#### *3.1.3. Data preprocessing*

In our work, we focused only on *origin anomalies*. Origin anomalies occur when there are multiple announcements of an IP prefix and Argus judges one of these as malicious. Thus, each event used in the data set corresponds to a unique prefix being rerouted. If there was an attack that resulted in multiple prefixes being rerouted, then that would appear in the data as two attacks.

Our data set excludes large-scale and easily-identifiable routing anomalous events to prevent these black swan events from biasing the results.[5] So, had we included the 179,000 prefixes announced by Malaysia (Toonk, 2015), the Chinese announcement of millions of addresses (Hiran et al., 2013), route leaks (Toonk, 2012), or large-scale outages (Dainotti et al., 2011) this would have biased the

[5]In the context of this research, a large-scale routing anomalous event is an incident that compromised thousands of IP prefixes in a single announcement. It constitutes an example of a black swan. A black swan is a highly improbable and high-impact event, such as the Lehman Brothers collapse in the U.S. or Malaysia announcing 179,000 prefixes.

results. Instead, our data set of "events" or "incidents" consists of those incidences identified by Argus as origin anomalies that were not large-scale events but focused on a single prefix. If the same prefix is announced again in a different timestamp, it was counted as a different event. In addition, the size of the prefix does not have any effect in the counting process, i.e, we did not distinguish between the announcement of a /18 from that of a /24 of event prefixes but treat them equally.

Our macroeconomic analyses required correlating an AS with a jurisdiction. The jurisdiction of the event is defined as the country from which the bogus route was announced. The mapping of IP addresses and ASes to country has been widely used in industry (Microsoft, 2011; Anti-Phishing Working Group (APWG), 2015; Cisco Systems, 2015) and academic macroeconomic research, e.g. (van Eeten et al., 2010). Geolocation is another related active research area, and improvements in geolocation could enhance this analysis. Here our approach to location is grounded in concurrent industry practice and related research (Quan et al., 2014).

We inferred the mapping between ASes and country membership from a data set provided by the Cooperative Association for Internet Data Analysis (CAIDA) (CAIDA, 2015). The geolocation data was also investigated over the fall of 2015 with multiple downloads of regional Internet registry (RIR) data. One goal in implementing downloads was to avoid the "phony, yet plausible, AS origins" that are used for ecrime. A false claim to an IP prefix would have to remain stable for a long time to pollute our data. There also would have to be a significant number of these to bias the results of our analysis.

Most of these anomalies in the Argus database are short-lived, on the matter of seconds. Previous anecdotal discussions (Madory, 2015) described cases that appear to be both intelligence activities and criminal activities. Like the Bitcoin miner attack, apparently criminal incidents are short-lived. Other than anecdotes, we have no basis for asserting that a short-lived hijack is a crime while a long-lived hijack is evidence of international intelligence activity. Given that there is clearly malicious activity that occurs in short bursts, we included

all the data in our analysis rather than creating an arbitrary threshold.

### *3.2. Statistical model*

Equation 1 summarizes the behavior that we captured.

$$\begin{aligned} A &= \beta_0 + \beta_1 \times \text{AVA} + \beta_2 \times \text{SEC} + \beta_3 \times \text{ECO} \\ &+ \beta_4 \times \text{LEG} + \beta_5 \times \text{EDU} + \epsilon \end{aligned} \tag{1}$$

In Equation 1, $A$ refers to the number of hijacked prefixes (i.e., the dependent variable). Every independent variable is captured by the factors AVA, SEC, ECO, LEG, and EDU respectively as we defined in Table 1. The terms $\beta_0, \ldots, \beta_5$ are the regression coefficients of the model. In addition, $\epsilon$ is the error term. Equation 1 was evaluated using multiple linear regression with ordinary least squares (OLS). In an effort to validate the OLS assumptions, we examined the model for the (absence) of multicollinearity[6] and heteroskedasticity[7].

To address the absence of multicollinearity in the predictors, we calculated the variance inflation factor (VIF) per year and in the aggregate data. We found that the four indicators of WGI are highly correlated, i.e., government effectiveness, regulatory quality, rule of law, and control of corruption have VIF $> 5$ (Zuur et al., 2010). Thus, in the subsequent analysis, we combined all of these indicators into a single score by adding them up. We called this new variable WGI. For the remaining predictors, the VIF values did not indicate that multicollinearity is an issue, i.e., FBIS, FBISper100, SIS, SISperM, GDP PPP and CCS have VIF $< 5$.

[6]Multicollinearity is observed when two or more independent variables are highly correlated, i.e., at least one of the independent variables can be expressed as a linear combination of the rest to a statistically significant degree. For collinear independent variables, the results of the OLS regression may be misleading.

[7]Heteroskedasticity is observed when the residuals (errors) of a model are not normally distributed. A test of absence of heteroskedasticity determines the regression model's ability to predict values of a dependent variable over all its range. For heteroscedastic residuals regression results should not be trusted.

We examined the distribution of the residuals of the model to check the absence of heteroskedasticity. We tested for normality using the Shapiro-Wilk test under the null hypothesis that the residuals were normally distributed. For the model described by Equation 1, the test for the distribution of the residuals produced a $p$-value of 0.464. This suggests that we failed to reject the null hypothesis that residuals are normally distributed. In other words, there is not enough evidence in favor of heteroskedastic errors, and the condition is satisfied. To avoid the regression being affected by particular outliers, we log transformed independent variables with a long-tail distribution. We determined these variables by examining their distributions in box plots and identifying outliers. The independent variables that were log transformed were (1) GDP PPP, (2) FBIS, (3) SIS, and (4) SISperM.

Similarly, given that the OLS regression makes additional assumptions, we explored the distribution of the dependent variable. In particular, OLS assumes that the dependent variable is continuous and normally distributed. In doing so, we tested for normality using the Shapiro-Wilk test per year and in the aggregate. We found that the normality assumption was not satisfied, in other words, the $p$-value $\approx 0$. This indicated that the dependent variable is unlikely to be normally distributed. Thus, the dependent variable was log transformed to satisfy the assumptions underlying the linear regression.

## 4. Results

Here we describe how our results indicate that lack of technical expertise does not affect the initiation of hijacks but the presence of conflict and the macroeconomic indicators of crime are statistically significant.

The results presented in this research are based on the analysis of the Argus' and World Bank data sets. The details of the data compilation can be found in Section 3.1. Given the wealth of data, a combination of statistical methods was applied. We used time-series analysis to examine significant trends in the Argus' data set (Section 4.1). We found that the distribution of the number

of hijacks per country was heavy-tailed and remained stable during the observation period, i.e., the majority of attacks are generated from a few countries (Section 4.2). To test our hypothesis of the influence of macroeconomic factors in the variance of the number of attacks originating from a certain country, we used multiple linear regression with independent variables from the World Bank (Section 4.3). The model reveals that the leading factors that are associated with hijack events are **guardianship**, which is operationalized through the number of SIS, and **governance**, which was estimated using the WGI. Finally, to further study the distribution of countries in the guardianship and governance dimensions, we analyzed the clusters that are formed (Section 4.4). In particular, countries with poor governmental practices are also associated with a higher frequency of originated hijacks. A high frequency of hijacks also corresponds to the existence of national conflict.

### *4.1. Anomaly time series*

The total number of IP prefixes that were impinged by an anomaly for each year during the observation period is 54,087, 90,607, 105,600 and 72,172 for 2011, 2012, 2013, and 2014, respectively. The data have a surprising level of variance. In particular, there is an increase of 67.5% between 2011 and 2012, an increase of 16.5% between 2012 and 2013, and a decrease of 31.7% between 2013 and 2014. This suggests that although the number of affected prefixes has been growing since 2011, it suddenly dropped at some point in 2014.

To further investigate the decrease in the number of hijacks in 2014, we analyzed the daily time series of anomalies. Fig. 1 shows the number of reported events during the observation period, i.e., the number of hijacked IP prefixes. The dashed line represents the unweighted LOESS fit. The shaded area corresponds to the 95% confidence interval of the regression model. It is worth noting that the data have very high variance. In particular, the number of hijacks spans four orders of magnitude. This means that reporting the average number of events is highly influenced by outliers and can be misleading. To take into account this constraint, we applied a non-parametric regression method—

unweighted LOESS—to perform local regression and derive a non-linear fitted smooth curve (the dashed one) that captures the trends in the time series. We also plot the 95% confidence interval of the regression line in the shaded area. Although the smooth curve does not reveal a significant trend, it is possible to infer that in 2014, there were two periods in which there are not records of incidents. These periods correspond to the days between January 3 to April 22 and May 22 to July 29. We iterated the analysis to confirm this empirically. The decrease in the number of incidents in 2014 is likely a result of some downtime because there appears to simply be missing data. Only Argus could confirm this; however, it offers one possible explanation. We cannot reject the explanation that hijacks have become more difficult to detect, but we find it unlikely. The rate of incidents appears to be increasing over time; however, missing data makes this an uncertain observation.

### *4.2. Anomaly distribution*

To take into account the origin of the bad routes, we mapped the AS origin of the bad route to the country corresponding to the one in which the AS is registered (based on a CAIDA data set) (CAIDA, 2015). We then measured the corresponding number of incidents that were reported in any given country. Fig. 2 shows the Complementary Cumulative Distribution Function (CCDF)[8] of the number of incidents per country during the observation period. The distribution is heavy-tailed suggesting that the majority of the reported hijack incidents originated from a small set of countries.

We determined the distribution that best fit the data by estimating parameters for different possible distributions and evaluating the goodness of fit. Specifically, we examined the best fit parameters for the empirical distribution by using the maximum likelihood among a set of power-law, log-normal, and exponential parametric distribution candidates. They are very well known to be

[8]For a random variable $X$, the CCDF is the probability that $X$ will take a value greater than a fixed value $x$, i.e., $\Pr(X > x)$.

a good fit for heavy-tailed distributions. We followed the procedure explained in (Clauset et al., 2009). Second, we calculated the goodness-of-fit for the proposed distributions by using the Kolmogorov-Smirnov (KS) test (Massey, 1951). The KS test evaluates the hypothesis that two samples of data are drawn from the same distribution. In this case, we tested if the observed distribution was statistically significantly different from the best fit of the parametric model. In particular, we computed the proportion of times that the test failed to reject the hypothesis that the distribution of compiled data and the synthetic data are drawn from the same distribution for a significance level of 0.05. In tests of $10^4$ synthetic distributions, the analysis of the synthetic data under the power law model failed to reject the null hypothesis in 99% of the cases, followed by log-normal at 98%, and exponential at 0%. From this analysis, we ruled out the exponential distribution as a potential candidate.

The dashed line in Fig. 2 shows the CCDF of the best power law model for the aggregate date, including all observations between 2011 and 2014. The estimated parameters of the power law distribution are $\alpha = 2.13$ for the scaling exponent and $x_{min} = 958$ for the threshold at which the power law begins.[9] Although the best fit is given by the power law distribution followed by a log-normal distribution, there was not enough evidence to entirely rule out the option of the log-normal distribution. Moreover, there are still some deviations from the dashed line in the tail, i.e., for countries with a large number of hijacks. We discuss this further in Section 5.

To determine how these distributions changed over time (and the possible transition from one distribution to another), we applied the KS test to determine if the distribution of hijacks per country changed from one year to the next through 2011 to 2014. We found that there were no comparisons where we were able to reject the hypothesis that the distributions were the same ($p$-value $\gg$ 0.05). Fig. 2 illustrates this fact by showing that the CCDF over the period of

[9]Remember that a random variable $X$ that follows a power law distribution has a probability density function given by $\Pr(X = x) = x^{-\alpha}$.

study is visually similar.

To further study the behavior of the countries that are the origin of the majority of the anomalies, we plot the number of anomalies per country for countries that are in the upper 2.5% tail of the anomaly distribution during a particular year. Specifically, Fig. 3 shows the changes for the countries that are the origin of the majority of the anomalies. This shows the number of reported anomalies per year for those countries that are in the upper 2.5% tail of the anomaly distribution for a specific year. Interestingly, the U.S. is the country to which the majority of the anomalies are attributed throughout the observation period. Brazil and India appear in three of the four years during the observation period, although their relative ranks change. Russia and Turkey appear twice, and China and Romania each show up once.

### *4.3. Regression analysis*

We ran a multiple linear regression for the aggregate data during the observation period using the entire set of measures from 2011 to 2014. Remember that the target variable is the number of hijacked prefixes in a particular country i.e., OLS was applied to Equation 1. Table 2 shows the OLS regression estimates. The model estimates and standard errors have been presented by taking heteroskedasticity into account. The linear regression quantifies the individual relative importance of a single feature when considering the effect of the others constant.

There are three statistically significant factors, nominally, SIS, WGI, and FBIS, in order of decreasing importance. We did not count as a separate predictor SISperM because this is a normalized measure of SIS (an indirect measure). The coefficients of the OLS suggest that although there is a positive association between SIS and FBIS with the number of hijacked prefixes (i.e., countries with higher SIS and FBIS are more likely to produce more incidents), the association with WGI was negative (i.e., countries with poor governmental practices are more likely to produce more incidents). This analysis also suggests that our hypothesized macroeconomic factors explained a significant amount of variance in

the number of incidents originating in different countries (approximately 75.3% with $p$-value $\approx 0$).

We further explored the relationship between the number of anomalies and the number of SIS. Fig. 4 shows that there is a power relationship between the two variables (given by the linear tendency in a log-log plot) for both the aggregate data and for each of the individual years. For the aggregate, the association between the two variables (in the log scale) has a Pearson correlation coefficient of 0.79, which confirmed the idea of a strong association between the two variables. Fig. 4 also reinforces the results of the regression analysis. In other words, it suggests that countries with a high number of SIS are also the countries with a high reported number of anomalies. In this plot, we highlighted the country with the highest density of secure servers and the larger number of produced anomalies during the observation period, which was the U.S. every year.

The top five countries in terms of the number of SIS during the observation period remained the same: U.S., U.K., South Korea, Japan, and Germany. The U.S. reported half a million, with the others reporting on the order of hundreds of thousands. As we might expect from the positive association revealed in Fig. 4, the U.S. is the country with the highest number of SIS and the highest number of anomalies (see Fig. 3). Japan is the other country that reveals a similar pattern with respect to a positive association between the number of SIS and control-plane anomalies. On the other hand, Germany, South Korea, and the United Kingdom report a high number of SIS, but here this does not correspond to a larger number of anomalies (see Fig. 5).

We then investigated the association between the number of SIS and WGI. Fig. 6 shows the relationship between these two variables for every country during the observation period. Note that we only considered the number of SIS and WGI because they were the most significant predictors in the regression, i.e., we did not explore the effect of FBIS. Although there is a positive association between SIS and the number of hijacked prefixes, and a negative one between WGI and the number of hijacked prefixes (see Table 2), the relationship between

these two independent variables is exponential in the WGI (given by the linear tendency in the log-linear plot) both for the aggregate data and for each of the individual years. The correlation for the aggregated data has a Pearson correlation coefficient of 0.68. This fact reinforces the idea of a strong association between the two variables. It also suggests that, given the data, it is more likely that countries with poor indices of governance also have a smaller number of SIS and vice versa. But more importantly, any change in the WGI of a country is exponentially amplified and reflected in the number of SIS. It appears that small changes in the perception of governmental practices result in significant changes in the generation of anomalies, and thus significant changes in creation of risk in the global control-plane.

### *4.4. Cluster analysis*

For the cluster analysis, we first normalized the anomalies per country by the total number of ASes that belong to that country during a certain year. This transformation allowed us to have a fair metric to evaluate the likelihood of a country being the origin of the anomalies based on their technological resources. Fig. 7 illustrates the differences in the anomaly/ASes ratio across the SIS and WGI plane for 2011. A higher intensity (i.e., darkness) in the data points represents a higher anomaly/ASes ratio at the country level. The plot also depicts the contour of the two-dimensional density estimation of the distribution of the data points. For those unfamiliar with unsupervised learning, a description of the use of unsupervised learning to categorize data can be found in (Hastie et al., 2016, Chapter 14).

We did not implement an aggregate cluster analysis for the entire period because of the apparently missing data as shown in Fig. 1. We have implemented cluster analysis for 2012 and 2013 finding the same clusters and same outliers despite the changes in rank shown in Fig. 4. The only difference is that Somalia was not an outlier in 2013. All graphs were remarkable for their similarity. The following discussion of cluster analysis applies to 2011-2013, with data missing in 2014, and 2015 subject to further analysis.

Fig. 7 shows that there are two main clusters based on this distribution. The first cluster corresponds to countries with high WGI and more than $10^3$ SIS, i.e., the first quadrant. Not surprisingly, the majority of the countries in this cluster are developed countries. The U.S. and South Korea are outliers of this cluster and are labeled in the plot. Although the U.S. has a better WGI indicator and a larger number of SIS than South Korea; South Korea has a higher ratio of anomaly/ASes (which is represented by a darker point). Recall the U.S. and South Korea are outliers in all our cluster analyses. South Korea similarly has a higher ratio of hijack/ASes for all years.

The second cluster represents mostly countries with low WGI and less than $10^3$ SIS, i.e., the third quadrant. The majority of countries in this cluster are developing countries. Comoros has been labeled in the plot with the highest ratio of anomaly/ASes during 2011 despite democratic elections of presidents who rejected violent extremism and the first peaceful transfer of power in 2010. In 2011, Comoros saw the return of the United Nations, the Peace Corps after 20 years, and such basic governance activities as setting up the first national parks. Terrorism warnings for travel in Comoros are low, and there are rare incidents of mass violence. Thus, this may be an anomaly, a result of low Internet penetration, or an echo of the irregularities of the 2010 election. Alternatively, and the argument the authors find most compelling is that Comoros is a geographical anomaly. The island is a nexus of global fiber traffic despite a small number of ASes. For Comoros, the sheer density of connectivity has no correspondence to number of ASes.

Somalia is an outlier of this cluster in 2011 and 2012. Somalia was not an outlier in 2013 despite a continued lack of effective central government, prevalence of violent extremists, and a civil dispute over the state of Somaliland. It may be worth noting that Somalians have recently had some success in leveraging ecrime, however, their technical expertise as observed is quite limited (Gallagher, 2016).

Finally, we analyzed the evolution of the WGI for countries with poor governmental practices, such as low WGI and a limited guardianship, i.e., a relatively

low number of SIS. We considered countries that had WGI between -7 and -3, which is 20% of the countries. We further filtered that set to include only those where the number of SIS was between 0 and 10 (still in the third quadrant), and the anomaly/ASes ratio was greater than 1.5 (recall these are World Bank estimates of absolute numbers, not per population.) In comparison, the median ratio of anomaly/AS for the U.S. during the observation period is 1.5.

Fig. 8 shows the geographic location of the countries that satisfy these characteristics during the observation period (highlighted in red). Note that countries depicted with higher intensity (darkness) are evaluated by consistent global measures as having lower WGI, i.e., weaker, less consistent, or lower integrity of governmental institutions. Table 3 shows the evolution of the WGI of these countries during the observation period. Interestingly, most of these countries have been involved in civil protests and threats of civil war as has been reported in (Dainotti et al., 2011). In particular, Syria has been (during the observation period) constantly categorized as a country with a high ratio of anomaly/ASes. Other countries in the Middle East that appear on this chart, Iraq and Yemen, also have been embroiled in conflict. The analysis highlights other countries in Africa including Burundi, Comoros, Congo, Guinea, and Liberia, as well as Timor-Leste[10] in Asia. Please also note the strategic location of Comoros for undersea cables.

The states above are all characterized by governmental fragility and little rule of law. (In this list, Syria stands out before the current cataclysm, Syria had highly advanced infrastructure and an educated populace.) Low SIS is conflated with low technical expertise and the lack of infrastructure associated with fragile states. Thus, one possibility is that these are simply victims of more technologically advanced states seeking cover for malicious activities. As in the case of the possible use of the Icelandic AS with the hijack from Denver via Ukraine, low SIS could be an indicator of victimization rather than any

[10]Timor-Leste was previously known as East Timor until winning independence from Indonesia and then being established as a sovereign state in 2002.

maliciousness (Cowie, 2013).

Thus, although we have some evidence of nation state activity by virtue of the clustering of hijacks with current conflict, we cannot reject the possibility that intelligence activities drive hijacks. The states that are highlighted here are not unique in poverty but are more distinguished by state-level violence. The corresponding move of Timor-Leste and Comoros from fragile to more established governments with peaceful transfers of power (and out of the cluster of high anomalies) during the observation period must be considered with the corresponding movement of Yemen into a more chaotic state over the same period (and yet also outside the cluster).

## 5. Discussion

The purpose of this work is to use macroeconomics, unsupervised learning, and theories of crime to find correlations with control-plane anomalies. The motivation of this work is to investigate if solutions to control-plane anomalies should consider incompetence, crime, and national intelligence activities as possible sources. Information about the purpose of attacks can inform the design of defenses. For example, a solution that creates additional complexity for network engineers may increase anomalies caused by failures in human expertise. Alternatively, any solutions which embed national governments as roots of trust may be less than ideal if nation states are the source of these events. Our results reject incompetence as a systematic cause, but we cannot reject crime and national intelligence activities as possible explanations.

We have analyzed the routing anomalies identified by Argus and mapped to the jurisdiction of origin. We have evaluated the statistical significance of macroeconomic indicators corresponding to three theories of ecrime and those that correspond to likely technical expertise for each jurisdiction. This study has as a primary focus an empirical understanding of the variance of anomaly production at the cross-country level. Some limitations need to be taken into account before further discussing the results. The model relied on multiple linear

regression through OLS, but OLS cannot identify the underlying mechanisms for the regression estimates. We also do not know why variables appear more predictive in some countries than in others. The results suggested by the statistical model are based on correlation, which is not an indicator of causality. In that respect, the aggregation and analysis of more features can partially but not wholly improve the understanding of causes in future research. We have offered technical competence, theories of ecrime, and governmental action as candidates for explanations of these correlations. These theories are well-grounded in the literature, motivating their selection, yet the results are in no way deterministic.

We identified some patterns of interest in the data beyond statistical significance that could be partially explained by macroeconomic indicators. First, the overall results indicate that the concentration of anomalies originated in the U.S. is consistently the highest. This suggests that a solution that is deployed in the U.S. may have a disproportionate impact in the reduction of routing anomalies. It also indicates that policies which apply only in the U.S. may be effective despite the global nature of the Internet. The potential for high impact of technology and policy solutions is reified by observation of the two highlighted clusters. Second, we observed significant incidence of anomaly production in countries with poor governance practices and limited investment in security. Among these countries with a striking rate of anomaly production and poor government indicators, Syria is the only country that is highlighted during the entire observation period.

Focusing further on the cluster of countries with poor governmental practices, we identify that indicators of conflict occur more strongly than indicators of poverty, i.e., it is not all about economic deprivation or lack of technical expertise. This is revealed as we track the evolution of the WGI for countries in this cluster. Moreover, as we have shown in the analysis, the four dimensions of governance are not independent of one another (Kaufmann et al., 2011). In other words, although these variables measure different aspects of governance, they tend to be closely inter-related in a particular country. This is an important consideration because the original formulation of the WGI leverages other di-

mensions of governance such as voice and accountability, political stability, and absence of violence. This implies that the WGI indicator that we presented in this study is capturing some component of conflict in the highlighted countries. In other words, WGI can indicate surveillance of a nation's own people.

We found that the distribution of the number of anomalies is well-modeled by either a power law or log-normal distribution (see Section 4.2). As has been pointed out by (Clauset et al., 2009), in terms of data generation, it is arguably more reasonable to assume that the data are created by a log-normal process because of the distribution of ASes globally and within countries. The type of mechanisms that can be expected to produce these heavy-tailed distributions identifies that power law and log-normal distributions are quite naturally associated (Mitzenmacher, 2004). In particular, the generative mechanism behind hijacks has been attributed to a multiplicative process in this case, this means the more ASes, the more we expect anomalies. This observation has also been discussed by (Edwards et al., 2015). Applicably, a multiplicative process is one that can be characterized by Gibrat's rule of proportionate growth stating that the proportional rate of growth of a firm is independent of its absolute size (Samuels, 1965). Thus, we can apply the analogy to model the size of the countries based on economic, guardianship, and availability factors. It is reasonable to expect the number of hijacks generated in a given country to be proportional to that country's macroeconomic indicators.

Overall, our analysis offers surprises in terms of the role of macroeconomic indicators in anomalies. Much, however, remains to be done. For example, it will be interesting to investigate whether consistent patterns in terms of anomaly production are observable at the level of ASes and ISPs. This would allow us to better understand the microeconomic factors that are responsible for the variance of anomaly production around the globe.

Given that the statistical model relies on assumptions concerning the generation of observed data, the conclusions are also based on the quality of data that we have. It might be the case that the data is incomplete or prone to false positives. Thus, additional analyses on other data sources should be compared

with the results here.

Finally, if this analysis proves predictive over multiple years such that changes in the independent variables are leading indicators in changes of anomalies, then we could have some basis to claim causation.

## 6. Conclusion

Our analysis of BGP routing anomalies lends insight into hijacks as a geographical, economic, political, and technical challenge. We focused on the analysis of longitudinal cross-country macroeconomic data and its relationship with the frequency of produced routing anomalies. To do so, we collected a data set about BGP incidents from June 2011 to December 2014 and combined this with data from the World Bank. We provided statistical characterizations of the distribution of hijacks over the past four years. The higher–level research question is, whether these are crimes, and if so, can we characterize these empirically as attacks? The specific hypotheses we address focus on determining the economic factors that explain the variance in the number of hijacks originating from different countries.

There appears to be a high and consistently increasing number of BGP incidents, specifically those that are potential hijacks. If we assume that the lack of data for 2014 is just that—a lack of data—and not a lack of incidents, we can expect hundreds of thousands more incidents in the coming years. Although there are false positives, these incidents are not route leaks and cannot be reasonably assumed to be the result of simple technical incompetence. In fact, our analysis found no systematic evidence that these anomalies are a result of incompetence measured by exports of information and communications technologies. (We have no expectation that this would hold for route leaks, which we did not explore.) Other than errors, two remaining explanations are crime and national intelligence. Both of these can be quite difficult to observe. They can also be difficult to distinguish. We found evidence for both possibilities.

To answer the question if BGP attacks are crimes, we use the tools of crim-

inology informed by previous work in empirical analyses of ecrime. Specifically, we built on previous macroeconomic work in online crime using the factors that have been found to be significant in predicting malware, spam, and crowdsourced criminal labor (e.g. CAPTCHA solving). We created a model and evaluated data over time to determine if variables associated with routine activity theory (secure Internet servers, fixed broadband Internet subscribers), economic deprivation theory (GDP per capita by PPP), or structural theory (governance and education) were significant over multiple years. We found that one variable for two of the three theories was significant. Specifically, secure Internet servers and density of fixed broadband Internet subscribers were significant, supporting routine activity theory. Governance indicators were significant, supporting a structural theory of crime.

We found evidence for the possibility that BGP anomalies (including hijacks) are a new method of ecrime, one that is detected tens of thousands of times each month. If BGP hijacks are a common ecrime vector and follow the patterns of other online crime, the misdirection and filtering of information may be commoditized and become an industry.

A further cluster analysis showed mixed evidence for crime and national intelligence. South Korea and the U.S. are known for being targeted by specific types of ecrime. South Korea is notable for its high level of virtual goods and thus is a target for virtual theft. The U.S. is consistently highly ranked as being the most popular target and the most popular source of common online crime, such as phishing and spam. The U.S. maintains its role as an outlier in this analysis; however, South Korea has a greater density of anomalies per AS. Although South Korea is itself characterized by high levels of governmental transparency and competence, it remains technically at war with North Korea, as there is no peace agreement. North Korea has been indicated in virtual as well as physical attacks against South Korean nationals. Similarly, although the U.S. is transparent, wealthy, and competent by global measures, the U.S. has not only never recognized North Korea as a nation, it also is actively involved in warfare in Afghanistan as well as having a wide range of additional military

engagements. Given the extremely large investment in national intelligence and national defense as well as the current involvement in conflicts overseas by the U.S., plus the situation with respect to North Korea, their presence in anomalies can also be seen as supporting the national intelligence explanation.

For the other cluster, that of nations with low numbers of secure Internet servers, the increase in density of anomalies per operating autonomous systems shows a striking overlap with nations with civil disputes over the time period studied. The relatively small number of countries prevents meaningful statistical analysis of these few nations, but the overlap between national conflict and anomalies is striking.

In summary, our findings provide statistical evidence for one of the three proposed explanations for anomalies: crime. We found weaker evidence in terms of governance and clustering for a second explanation: national intelligence. We found no evidence for incompetence per se.

We conclude that any solution to the challenge of increasing router plane anomalies should consider crime and national state action as possibilities. This may particularly affect any solutions which indicate that nation states can be roots of trust. A solution that mitigates one source of hijacks should not exacerbate the other. Otherwise, such anomalies may not remain, in fact, anomalous.

## 7. Acknowledgments

This research was sponsored by NSF CISE #1565252: Living in the Internet of Things, Cisco Research #591000, and Google Privacy & Security Focused Research. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies or views, either expressed or implied, of the U.S. Government, Cisco, Google, or Indiana University. We would like to thank Argus for making data available, the anonymous reviewers for the valuable comments, Kevin Benton for his insights, as well as Steven Rich for his guidance.

Afroz, S., Garg, V., McCoy, D., & Greenstadt, R. (2013). Honor among thieves:

A common's analysis of cybercrime economies. In *eCrime Researchers Summit* (eCRS) (pp. 1–11). San Francisco, CA, USA.

Anti-Phishing Working Group (APWG) (2015). Phishing Activity Trends Report. `https://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf`.

Arnbak, A., & Goldberg, S. (2015). Loopholes for circumventing the Constitution: Unrestrained bulk surveillance on Americans by collecting network traffic abroad. *Michigan Telecommunications and Technology Law Review*, *317*.

Asghari, H., van Eeten, M. J. G., & Mueller, M. L. (2012). Unravelling the economic and political drivers of deep packet inspection. An empirical study of DPI use by broadband operators in 75 countries. In *7th Annual Global Internet Governance Academic Network Symposium* (GigaNet). Baku, Azerbaijan.

Benton, K., & Camp, L. J. (2016). Preventing data exfiltration via political and geographic routing policies. *Available at SSRN 2753133*, .

Blau, J. R., & Blau, P. M. (1982). The cost of inequality: Metropolitan structure and violent crime. *American Sociological Review*, *47*, 114–129.

Bowman, W. M., & Camp, L. J. (2013). Protecting the internet from dictators: Technical and policy solutions to ensure online freedoms. *The Innovation Journal: The Public Sector Innovation Journal*, *18*, 1–24.

Butler, K., Farley, T. R., McDaniel, P., & Rexford, J. (2010). A Survey of BGP Security Issues and Solutions. *Proceedings of the IEEE*, *98*, 100–122.

CAIDA (2015). The CAIDA UCSD AS to Organization Mapping Dataset. `http://www.caida.org/data/as_organizations.xml`.

Christin, N. (2013). Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international*

*conference on World Wide Web* (WWW '13) (pp. 213–224). Rio de Janeiro, Brazil.

Cisco Systems (2015). Annual Security Report. `http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf`.

Clauset, A., Shalizi, C. R., & Newman, M. E. J. (2009). Power-law distributions in empirical data. *SIAM Review*, *51*, 661–703.

Clayton, R. (2015). Badness in the RIPE Database. `https://www.lightbluetouchpaper.org/2015/10/02/badness-in-the-ripe-database/`.

Cooper, D., Heilman, E., Brogle, K., Reyzin, L., & Goldberg, S. (2013). On the risk of misbehaving rpki authorities. In *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks* HotNets-XII (pp. 16:1–16:7). College Park, MD, USA.

Cowie, J. (2013). The New Threat: Targeted Internet Traffic Misdirection. `http://research.dyn.com/2013/11/mitm-internet-hijacking/`.

Cullen, F. T. (1994). Social support as an organizing concept for criminology: Presidential address to the academy of criminal justice sciences. *Justice Quarterly*, *11*, 527–559.

Dagon, D., Provos, N., Lee, C. P., & Lee, W. (2008). Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority. In *Network and Distributed System Security Symposium* (NDSS).

Dainotti, A., Squarcella, C., Aben, E., Claffy, K. C., Chiesa, M., Russo, M., & Pescapé, A. (2011). Analysis of Country-wide Internet Outages Caused by Censorship. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (IMC '11) (pp. 1–18). Berlin, Germany.

Edwards, B., Hofmeyr, S., & Forrest, S. (2015). Hype and Heavy Tails: A Closer Look at Data Breaches. In *The 14th Workshop on the Economics of Information Security (WEIS 2015)*. Delft, Netherlands.

van Eeten, M., & Bauer, J. M. (2008). Economics of Malware: Security Decisions, Incentives and Externalities. In *OECD Science, Technology and Industry Working Papers, No. 2008/01*.

van Eeten, M., Bauer, J. M., Asghari, H., Tabatabaie, S., & Rand, D. (2010). The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data. In *The Ninth Workshop on the Economics of Information Security (WEIS 2010)*. Cambridge, MA, USA.

Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. *Human Ecology*, *8*, 389–406.

Gallagher, S. (2016). Pirates hack into shipping company's servers to identify booty. `http://arstechnica.com/security/2016/03/pirates-hack-into-shipping-companys-servers-to-identify-booty/`.

Garg, V., & Camp, L. J. (2013). Macroeconomic Analysis of Malware. In *Network and Distributed System Security Symposium Extended Abstracts* (NDSS).

Garg, V., Koster, T., & Camp, L. J. (2013). Cross-country analysis of spambots. *EURASIP Journal of Information Security*, *3*, 1–13.

Greenberg, A. (2014). Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins. `http://www.wired.com/2014/08/isp-bitcoin-theft/`.

Hastie, T., Tibshirani, R., & Friedman, J. (2016). The elements of statistical learning: Data mining, inference, and prediction. Springer Series in Statistics. (2nd ed.).

Hiran, R., Carlsson, N., & Gill, P. (2013). Characterizing large-scale routing anomalies: A case study of the china telecom incident. In *Proceedings of the 14th International Conference on Passive and Active Measurement* (PAM '13) (pp. 229–238). Hong Kong, China.

Hu, X., & Mao, Z. (2007). Accurate Real-time Identification of IP Prefix Hijacking. In *IEEE Symposium on Security and Privacy* (SP '07) (pp. 3–17). Berkeley, CA, USA.

Hunter, P. (2008). Pakistan YouTube block exposes fundamental Internet security weakness: Concern that Pakistani action affected YouTube access elsewhere in world. *Computer Fraud & Security*, *2008*, 10–11.

Ika, L. A., Diallo, A., & Thuillier, D. (2012). Critical success factors for World Bank projects: An empirical investigation. *International Journal of Project Management*, *30*, 105–116.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G. M., Paxson, V., & Savage, S. (2008). Spamalytics: An empirical analysis of spam marketing conversion. In *Proceedings of the 15th ACM Conference on Computer and Communications Security* (CCS '08) (pp. 3–14). Alexandria, VA, USA.

Kaufmann, D., Kraay, A., & Mastruzzi, M. (2011). The Worldwide Governance Indicators: Methodology and Analytical Issues. *Hague Journal on the Rule of Law*, *3*, 220–246.

Khare, V., Ju, Q., & Zhang, B. (2012). Concurrent prefix hijacks: Occurrence and impacts. In *Proceedings of the 2012 Internet Measurement Conference* (IMC '12) (pp. 29–35). Boston, MA, USA.

Kirk, J. (2011). AT&T Facebook traffic takes a loop through China. `http://www.computerworld.com/article/2507181/security0/at-t-facebook-traffic-takes-a-loop-through-china.html`.

Kruegel, C., Mutz, D., Robertson, W., & Valeur, F. (2003). Recent Advances in Intrusion Detection. chapter Topology-Based Detection of Anomalous BGP Messages. (pp. 17–35). Springer Berlin Heidelberg volume 2820.

Lad, M., Massey, D., Pei, D., Wu, Y., Zhang, B., & Zhang, L. (2006). PHAS: A Prefix Hijack Alert System. In *Proceedings of the 15th Conference on USENIX Security Symposium* (pp. 153–166). Vancouver, BC, Canada.

Madory, D. (2015). The Vast World of Fraudulent Routing. `http://research.dyn.com/2015/01/vast-world-of-fraudulent-routing/`.

Massey, F. J. (1951). The Kolmogorov-Smirnov Test for Goodness of Fit. *Journal of the American Statistical Association*, *46*, 68–78.

Microsoft (2011). Microsoft Security Intelligence Report. `https://www.microsoft.com/en-us/download/details.aspx?id=27605`.

Mitzenmacher, M. (2004). A Brief History of Generative Models for Power Law and Lognormal Distributions. *Internet Mathematics*, *1*, 226–251.

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *The Journal of Economic Perspectives*, *23*, 3–20.

Phillips, K. N., Pickett, A., & Garfinkel, S. L. (2011). *Embedded with Facebook: DoD Faces Risks from Social Media*. Technical Report DTIC Document.

Pratt, T. C., & Cullen, F. T. (2005). Assessing Macro-Level Predictors and Theories of Crime: A Meta-Analysis. *Crime and Justice*, *32*, 373–450.

Quan, L., Heidemann, J., & Pradkin, Y. (2014). When the Internet Sleeps: Correlating Diurnal Networks with External Factors. In *Proceedings of the 2014 ACM Conference on Internet Measurement Conference* (IMC '14) (pp. 87–100). Vancouver, BC, Canada.

Ramachandran, A., & Feamster, N. (2006). Understanding the Network-level Behavior of Spammers. *SIGCOMM Comput. Commun. Rev.*, *36*, 291–302.

Samuels, J. M. (1965). Size and the Growth of Firms. *The Review of Economic Studies*, *32*, 105–112.

Shi, X., Xiang, Y., Wang, Z., Yin, X., & Wu, J. (2012). Detecting Prefix Hijackings in the Internet with Argus. In *Proceedings of the 2012 ACM Conference on Internet Measurement Conference* (IMC '12) (pp. 15–28). Boston, MA, USA.

Toonk, A. (2010). Chinese ISP hijacks the Internet. `http://www.bgpmon.net/chinese-isp-hijacked-10-of-the-internet/`.

Toonk, A. (2012). How the Internet in Australia went down under. `http://www.bgpmon.net/how-the-internet-in-australia-went-down-under/`.

Toonk, A. (2015). Massive route leak causes Internet slowdown. `https://bgpmon.net/massive-route-leak-cause-internet-slowdown/`.

Vervier, P.-A., Thonnard, O., & Dacier, M. (2015). Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks. In *Network and Distributed System Security Symposium* (NDSS '15).

Wählisch, M., Maennel, O., & Schmidt, T. C. (2012). Towards Detecting BGP Route Hijacking Using the RPKI. *SIGCOMM Comput. Commun. Rev.*, *42*, 103–104.

Xiang, Y., Wang, Z., Yin, X., & Wu, J. (2011). Argus: An accurate and agile system to detecting IP prefix hijacking. In *Proceedings of the 19th IEEE International Conference on Network Protocols* (ICNP) (pp. 43–48). Vancouver, BC, Canada.

Zhang, Z., Zhang, Y., Hu, Y., Mao, Z., & Bush, R. (2010). iSPY: Detecting IP Prefix Hijacking on My Own. *IEEE/ACM Transactions on Networking*, *18*, 1815–1828.

Zhao, X., Pei, D., Wang, L., Massey, D., Mankin, A., Wu, S. F., & Zhang, L. (2001). An analysis of bgp multiple origin as (moas) conflicts. In *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement* (IMW '01) (pp. 31–35). San Francisco, California, USA.

Zheng, C., Ji, L., Pei, D., Wang, J., & Francis, P. (2007). A Light-weight Distributed Scheme for Detecting Ip Prefix Hijacks in Real-time. *SIGCOMM Comput. Commun. Rev.*, *37*, 277–288.

Zuur, A. F., Ieno, E. N., & Elphick, C. S. (2010). A protocol for data exploration to avoid common statistical problems. *Methods in Ecology and Evolution*, *1*, 3–14.

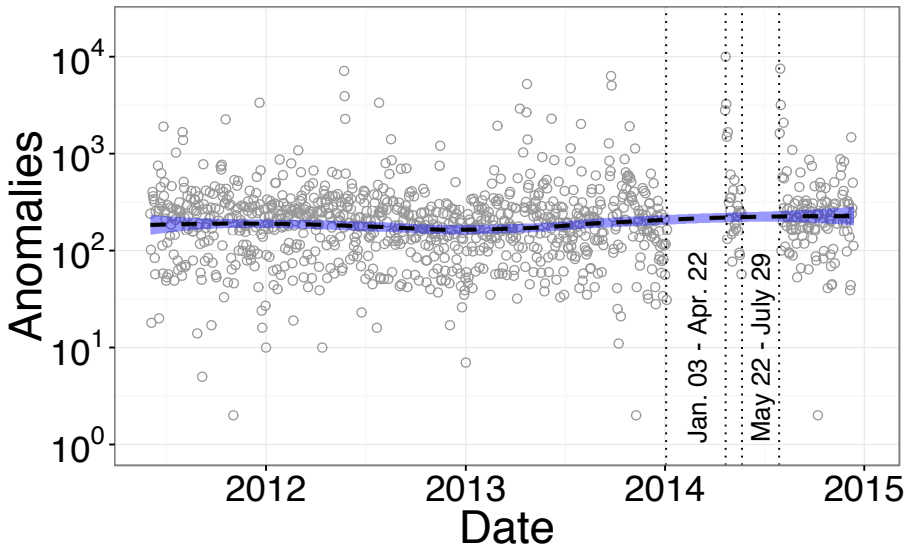


Figure 1: Daily number of anomalies. The dashed line represents the unweighted LOESS fit. The blue band corresponds to the 95% confidence interval of the unweighted LOESS fit.

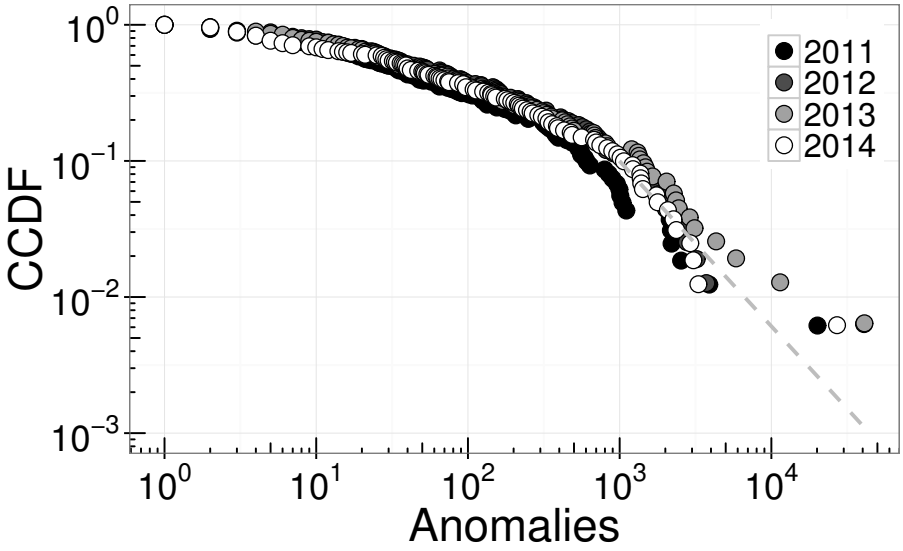


Figure 2: CCDF of anomalies originated per country.

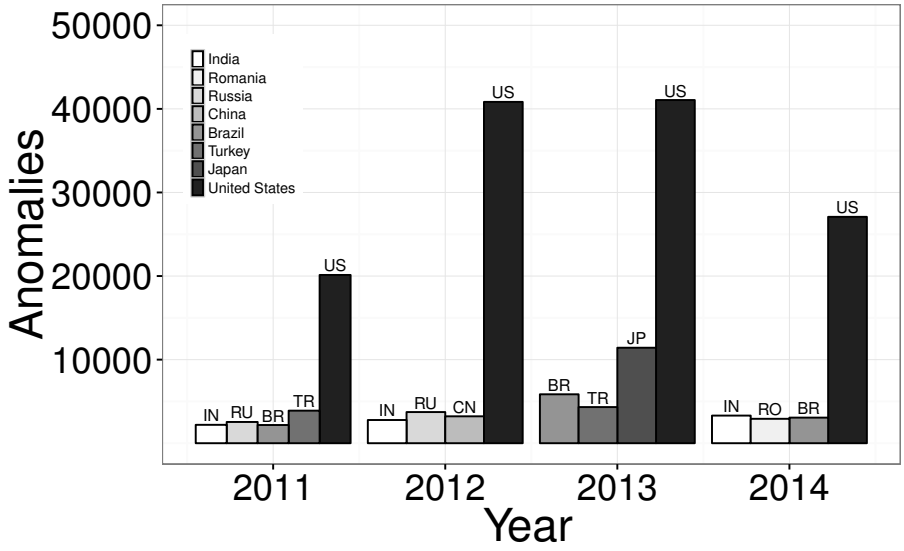


Figure 3: Anomalies per year for countries that are in the upper 2.5% tail of the anomaly distribution.

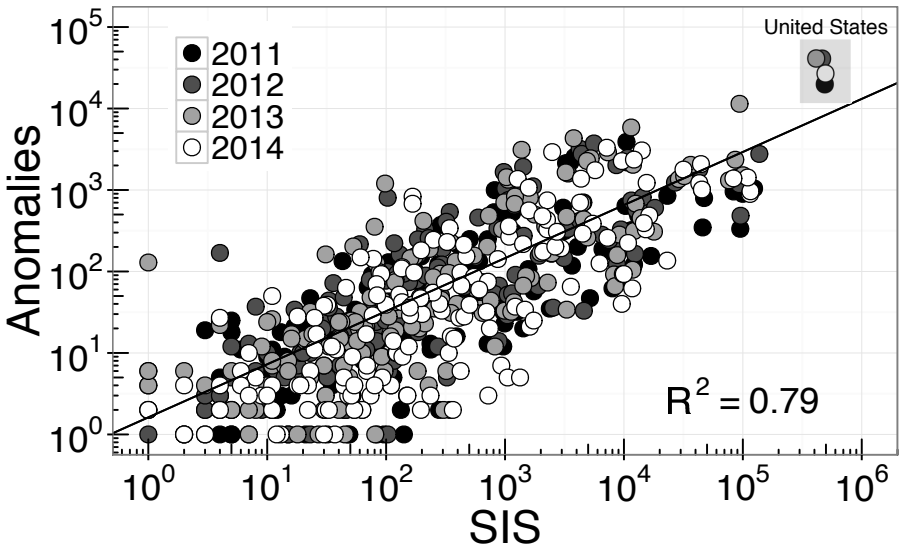


Figure 4: Anomalies vs. SIS per year per country.

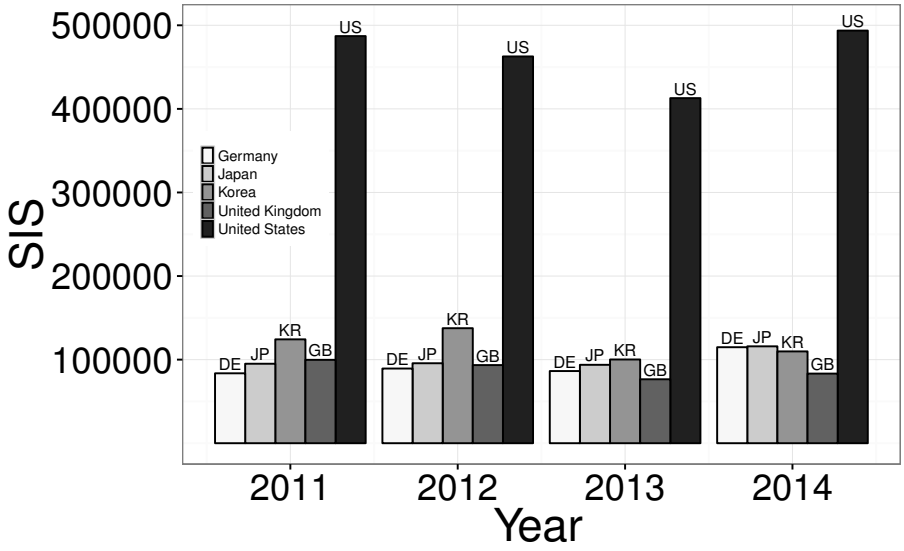


Figure 5: Distribution of the number of SIS per year for countries that are in the upper 2.5% tail of the SIS distribution.

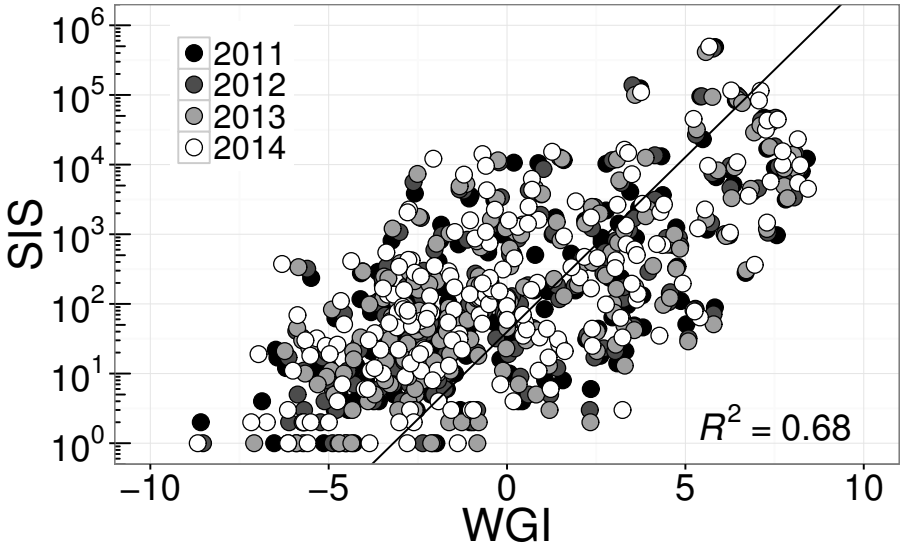


Figure 6: SIS vs. WGI for all countries over all years.

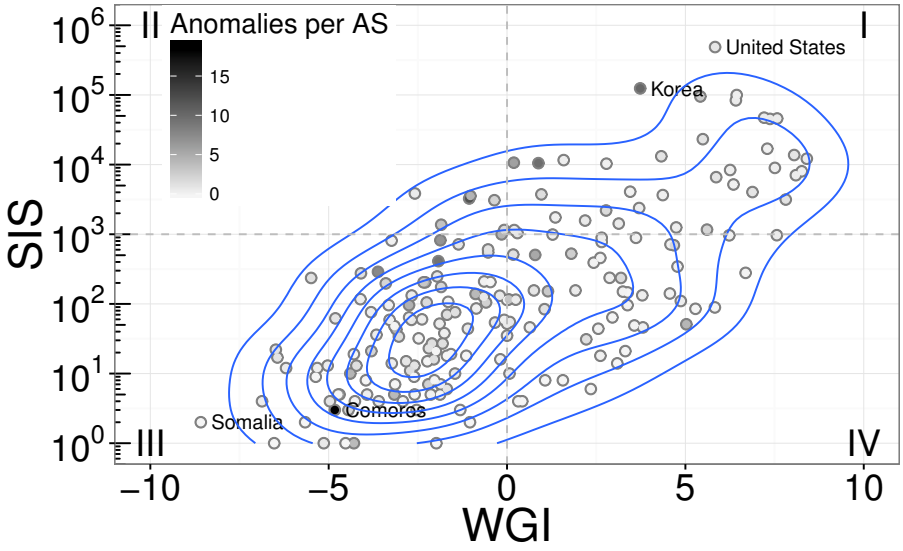


Figure 7: Anomaly/ASes ratio in the SIS versus WGI plane for 2011.

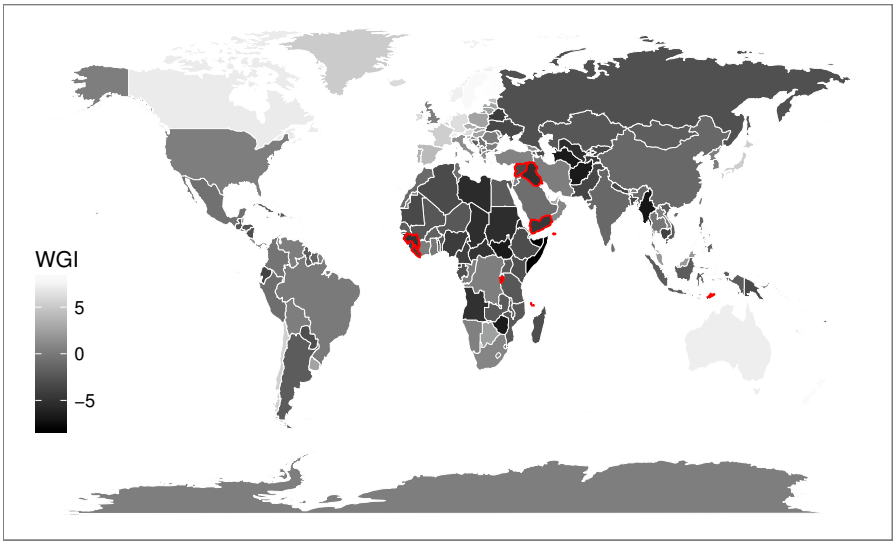


Figure 8: Geographic location of the countries with considerable high number of anomaly/ASes and poor governmental practices (measured through WGI) during the observation period.

Table 1: Five-dimensional regression model variables.

| **Model factor** | **Variable name** | **Acronym** |
|---|---|---|
| Availability (AVA) | Fixed broadband Internet subscribers | FBIS |
| | Fixed broadband Internet subscribers (per 100 people) | FBISper100 |
| Security of ICT infrastructure (SEC) | Secure Internet servers | SIS |
| | Secure Internet servers (per one million) | SISperM |
| Economic resources or affordability (ECO) | GDP per capita by PPP | GDP PPP |
| Governance of legal framework (LEG) | World Governance Indicators | WGI |
| Security skills or education (EDU) | Computer, comm., and other services (% exports) | CCS |

Table 2: OLS regression estimates.

| Variable | Estimate | Std. Error | t value | Pr(>\|t\|) |
|---|---|---|---|---|
| (Intercept) | -1.7231 | 0.7913 | -2.18 | $0.0300^{*}$ |
| log(FBIS) | 0.1700 | 0.0545 | 3.12 | $0.0019^{**}$ |
| FBISper100 | -0.0052 | 0.0096 | -0.54 | 0.5882 |
| log(SIS) | 0.7561 | 0.0654 | 11.57 | $\approx 0^{***}$ |
| log(SISperM) | -0.1758 | 0.0677 | -2.60 | $0.0098^{**}$ |
| log(GDP PPP) | -0.0090 | 0.1145 | -0.08 | 0.9372 |
| WGI | -0.1222 | 0.0326 | -3.75 | $0.0002^{***}$ |
| CCS | 0.0035 | 0.0024 | 1.47 | 0.1429 |

Signif. codes: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

Residual standard error: 1045 on 408 degrees of freedom

Multiple R-squared: 0.7576, Adjusted R-squared: 0.7534

$F$-statistic: 182.1 on 7 and 408 DF, $p$-value: < 2.2e-16

Table 3: Evolution of the WGI (in decreasing order) for countries with high anomaly/ASes per year.

| **Year** | **Country** | **WGI** | **Anomaly/ASes** |
|---|---|---|---|
| 2011 | Comoros | -4.83 | 19.0 |
| | Congo | -4.70 | 6.0 |
| | Timor-Leste | -4.45 | 2.0 |
| | Yemen | -4.39 | 4.5 |
| | Burundi | -4.29 | 4.0 |
| | Syria | -3.16 | 4.27 |
| 2012 | Iraq | -5.11 | 4.3 |
| | Syria | -5.06 | 6.2 |
| | Liberia | -3.73 | 4.0 |
| 2013 | Syria | -5.66 | 4.0 |
| | Guinea | -4.70 | 16.1 |
| | Liberia | -3.89 | 3.7 |
| 2014 | Syria | -6.01 | 7.1 |
| | Guinea | -4.75 | 3.9 |