Project Summary: **CI-SUSTAIN: Sustainable Tools for Analysis and Research on Darknet Unsolicited Traffic (STARDUST)**

For over a decade, the UCSD Network Telescope (UCSD-NT) instrumentation, which captures traffic sent to a large segment of unassigned IPv4 address space (darknet), has enabled global visibility into macroscopic Internet phenomena that few other data sources can provide. The relevance of this community research infrastructure for the study of the Internet is reflected in a vast literature in a broad set of sub-disciplines in CISE and beyond, from network and systems security and stability, to machine learning and big data processing techniques, and most recently to studies of cyberwarfare and political repression of communication. In 2011 we enhanced the Telescope instrumentation to enable access to raw and live telescope traffic data, which expanded the scope of possible research questions and the circle of researchers using the data. As of January 2017 we are aware of (a lower bound) over 100 publications – without UCSD co-authors – that used UCSD-NT data. Our exciting success with this project has triggered a new problem: the current state of this infrastructure is lagging behind the increasing demands in terms of storage, computing resources, and system administration. These issues hinder our ability to continue sharing UCSD-NT data with researchers, and have already required compromises that limit its utility to the community.

We propose a project to enable sustained long-term operation of the UCSD-NT infrastructure, while also increasing its utility to the research community. We organize our proposed scope of work into three inter-related tasks. First, we will upgrade and modernize the current infrastructure (network data capture and communication hardware and storage) to stabilize operations. Second, we will transition the data analysis computing infrastructure to a sustainable model based on virtualization, leveraging NSF-funded HPC platforms at SDSC. This task consists of three connected sub-tasks: deploying cloud-compute support using new virtualization features of the Comet environment; redesigning the software pipeline to take advantage of this new capability for transferring live streams of data; and collaborating with HPC researchers at SDSC to develop tools to support dynamic provisioning of Spark and Hadoop clusters as needed. Third, we will introduce meta-data semantics that simplify many tasks researchers typically want to do with UCSD-NT data, leaving them more time (and available HPC resources) to focus on their specific scientific questions. While mainly targeting long-term sustainability, our proposed solutions will also improve the research utility of this data, further lowering barriers for and thus increasing diversity of the user base of this research infrastructure.

Intellectual Merit. This project will result in an interdisciplinary collaboration between researchers from the field of computer networks and high-performance computing scientists and engineers to experiment with novel approaches leveraging HPC infrastructure for research on live traffic analysis. By upgrading the infrastructure to sustain predicted growth in use for many years, we are stabilizing and enhancing our ability to serve a diverse range of academic researchers, the vast majority of whom have no access to any other source of global Internet traffic data.

Broader impacts. We will disseminate project results via conferences, web sites, archived video lectures, blogs, and the proposed workshops and will continue our engagement of faculty and graduate students in the use of our tools and data. Project results will contribute to advancing knowledge in diverse CISE disciplines, e.g., enabling the development of efficient strategies for early detection and mitigation of security-related events, providing macroscopic Internet performance and reliability assessments, and providing a new domain for the application of live streaming big data analysis, and in situ machine learning techniques.

Keywords: Network Measurement; Internet Traffic Monitoring; Privacy-Sensitive Data Sharing

Project Description: CI-SUSTAIN: Sustainable Tools for Analysis and Research on Darknet Unsolicited Traffic (STARDUST)

1 Introduction, Motivation and Goals

Network telescopes – network instrumentation capturing unsolicited Internet traffic ("background radiation") sent to unassigned address space ("darknet") – allow global visibility into and historical trend analysis of a wide range of Internet phenomena. UC San Diego currently operates the largest network telescope (and one of only two) generally accessible to academic researchers [1] (*UCSD-NT* in the following).

The relevance of this data collection infrastructure for the study of the Internet is reflected in a vast literature. In operation since 2001, the UCSD-NT has been a key witness of a wide range of macroscopic Internet events and phenomena: the automated spread of malicious software such as Internet worms or viruses [2, 3, 4, 5]; random spoofed source denial-of-service attacks [6]; large-scale botnet activities [7, 8]; macroscopic Internet blackouts due to natural disasters [9], network failures [10] and state censorship [11]; trends in IPv4 address space utilization [12, 13]; various types of bugs and misconfigurations in popular applications [14]; etc. Measurement and analysis of such macroscopic phenomena are of key strategic importance for the security and reliability of the Internet infrastructure, and present social and economic relevance as well. CAIDA at UC San Diego, has carried out most of these studies (more than 20 publications, in collaboration with researchers from other institutions [15]). We have also leveraged the telescope infrastructure to enable several government-sponsored research projects [16, 17, 18]. More importantly, we made telescope data available to other researchers, and saw subsequent impacts across a broad range of CISE sub-disciplines (described in Section 3.1): **access to the UCSD Network Telescope has yielded more than 100 scientific publications and PhD theses *without* CAIDA co-authorship** [19].

In particular, in 2011, with NSF funding we extended access to data collected from the telescope by enabling access to raw and live telescope traffic data [20, 21]. Our goal was to (i) unlock research on recent darknet traffic observation and enable the study of diverse research questions and approaches, not limited to the availability of few specific subsets of traffic (in the past we often made available curated datasets covering the spreading of a specific worm, or a scan activity, etc.), and (ii) broaden research into live analysis of unsolicited Internet traffic [22]. Raw telescope data presents potential security and privacy concerns and challenges related to the amount of data[1], which we tackled by combining a "bring code to data" approach (i.e., we give vetted researchers access to CAIDA compute resources) operating within constraints of CAIDA's Privacy-Sensitive Sharing (PS2) framework [23]. While researchers used these telescope enhancements to great advantage, our success has triggered a new problem: the current state of this infrastructure is lagging behind the increasing demands in terms of storage, computing resources, and system administration. These issues **hinder our ability to continue sharing UCSD-NT data with researchers, and have already required compromises that limit its utility to the community.** We have had to decline some requests, and limit others, in terms of duration of access or computing power available.

Based on our research and data-sharing experience with telescope traffic data, **we propose a set of tasks that will enable sustained long-term operation of the UCSD-NT infrastructure, while also increasing its utility to the research community**. In summary, we plan to:

- ***Deploy new hardware to sustain operation of the infrastructure*** We will deploy new traffic capture infrastructure to sustain increased packet rates and additional storage capacity to

[1] As of end of 2016, 1 month of traffic takes about 36 TB of compressed files

support long-term use of the UCSD-NT.

- ***Transition the data analysis infrastructure to a sustainable model based on NSF HPC resources.*** We will use virtualization technologies and NSF compute resources (i.e., the Comet supercomputer at SDSC) to provide a scalable, sustainable platform for analyzing this data. We will stream live traffic as it is captured from the telescope to Comet virtual clusters, and deploy Big Data technologies such as Apache Spark [24] to implement scalable processing of telescope traffic data and meta-data.
- ***Reduce processing cost via pre-computation of high-value meta-data.*** We will enrich telescope traffic with meta-data tags (based on geography, topological properties, and our anti-spoofing heuristics) to reduce and simplify processing needed by many researchers.

While mainly targeting improved sustainability, our proposed solutions will also improve the research utility of this data and simplify its use, further lowering barriers for and thus increasing diversity of the user base of this research infrastructure.

2 Existing Infrastructure and Development History

A telescope's *resolution* depends on the size of address space it monitors; a telescope using a /16 address prefix will see more packets than one using a /24 prefix. The UCSD-NT [1] uses a /8 mostly *dark* (i.e., addresses are not assigned to any hosts) network prefix which corresponds to 16M addresses, 1/256th of the total IPv4 address space. We separate the legitimate traffic destined to the few reachable IP addresses in the darknet, and monitor only the traffic destined to the empty address space. Therefore, if a host sends packets to uniformly random Internet (IPv4) addresses, the UCSD telescope should see about 1/256 of those probes. We collect traffic data from the telescope using commodity hardware and WAND's WDcap [25] software suite, which stores files in compressed pcap [26] format. As of January 2017, the network telescope captures more than 1 TB of compressed traffic trace data per day.

Supported by our previous CRI project ("II-EN: Real-time Lens into Dark Address Space of the Internet", CNS-1059439, $500,000 Jul 2011 - Aug 2014, PI KC Claffy [21]), we deployed a single host dedicated to storing approximately the 60 most recent days of data from the UCSD-NT. Each day is represented by 24 compressed pcap files each containing one hour of data. Every hour the system automatically adds the most recent trace file to the collection, creating an almost real-time dataset with an effective latency of one hour. Data outside the 60-day window is archived to HPSS facilities at the National Energy Research Scientific Computing Center (NERSC), after which it is removed from local storage. In addition to creating hourly pcap traces, we use the Corsaro [27] software suite to create flow-level records (FlowTuple) that are sufficiently storage-efficient to accommodate local retention of the full set of historical data.

Since 2001 we have released 12 general telescope datasets [28] such as Backscatter data [29] as well as curated datasets focused on specific security events [30, 31, 32, 33]. CAIDA shares different forms of telescope data with different levels of disclosure control, to balance privacy risk with utility of research data [23]. To promote broad research use of data, we release some static snapshots of UCSD-NT traffic data where we delete or sanitize all payload in the packets, and anonymize IP addresses in the IP header using a common prefix-preserving technique. But many research applications of this data require unanonymized IP addresses, which we support with a more restrictive acceptable use policy. For example, in 2009, we released two days of raw (i.e., with actual source IP addresses) UCSD-NT traffic traces taken in November 2008, as a baseline from dates prior to known Conficker activity, and then three days of data during Conficker growth [34, 32]. Last year, we experimented with releasing an unprecedented 6 months of anonymized telescope data (from

January to June 2012) at a flow-level granularity [35].

The major sensitivity with unanonymized telescope traffic is that source IP addresses in packets are likely to be hosts compromised with some form of malware, and thus vulnerable. More recently captured traffic is more sensitive in this regard since the hosts are likely still not patched, in contrast to IP addresses in packets observed years ago. But researchers are often interested in studying recent (if possible, current!) data, for example, in order to correlate it with other sources of near real-time data (e.g., BGP, active probing). In response to research community needs, in 2011 we started providing near-real-time access to UCSD-NT traffic data [20, 21]. For this more sensitive form of data sharing, we use a "bring code to data" approach, where we give vetted researchers access to CAIDA compute resources and the 60-most-recent-day window of raw telescope traffic traces, but do not allow downloading of the data. We reduce potential security and privacy risks of this access by applying CAIDA's Privacy-Sensitive Sharing (PS2) framework [23]. We also enable sharing the near-real-time data via DHS IMPACT project [36] which vets researchers and provides legal support for cybersecurity data sharing activities (§3.5).

3 Value to the Community

3.1 CISE sub-disciplines that have benefited from the infrastructure

The UCSD-NT mainly serves CISE communities in the field of Computer and Network Systems, with emphasis on network and systems security, Internet reliability and performance, and Internet censorship. However, studies using UCSD-NT data also involve researchers from other CISE subdisciplines, since the phenomena revealed by this data and the problems associated with studying them require application of sophisticated (and sometimes development of new) machine-learning methods, visualization techniques, and efficient data processing approaches. In addition, since 2014 we have collaborated with HPC researchers at SDSC to develop and test approaches that leverage SDSC's HPC infrastructure to efficiently process darknet traffic. Finally, last year we began providing data to political science researchers interested in cyberwarfare and use of technology for political repression and protests (e.g., Internet filtering, outages, or denial-of-service attacks).

3.2 Prior CAIDA research with the UCSD-NT

Our prior research contributions enabled by data from UCSD-NT have included studies of denial-of-service (DoS) attacks [37, 38], Internet worms [39] and their victims, e.g., Code-Red [5], Slammer [40], and Witty [3] worms. Data sets curated from telescope observations of these events became a foundation for modeling the top speed of flash worms [2], the "worst-case scenario" economic damages from such a worm [41], and the pathways of their spread and potential means of defense [42]. Recently, we observed and analyzed horizontal scans targeting the entire IPv4 address space carried out by large botnets [43, 44], in one case revealing sophisticated covert scanning strategies previously undocumented in literature. Our findings and the published papers are used in graduate-level courses [45, 46]. We also investigated the aftermath of the large covert scan we discovered, identifying, in collaboration with researchers from ETH Zurich, a large number of hosts compromised in the Swiss national research network [8]. This work shed light on the modus operandi of a large botnet in escalating from scanning to massive compromise and allowed us to derive conclusions about the risks associated with scanning activity.

Since 2011, CAIDA – in collaboration with RIPE NCC and University Roma Tre – published several works that showed, for the first time, that darknet traffic analysis could provide insights into causes of large connectivity disruption events [47, 11, 10, 9]. These studies posed the foundations for an NSF-funded project to operationalize our methodologies and monitor the Internet

24/7 to detect and characterize large-scale Internet blackouts caused by network failures, natural disasters, censorship, etc. [17].

Detection of Internet blackouts was the first of a broad class of inferences we discovered that were unrelated to the actual phenomena responsible for generating unsolicited traffic. In 2014, in collaboration with multiple universities in Europe and in the U.S., we demonstrated the potential of darknet traffic measurements in complementing active probing techniques to reveal trends in IPv4 address space usage [13, 12]. Finally, in 2015 we proposed a reference framework, with use-case studies, to investigate the utility of telescope traffic to support inference of a range of properties of networks across the global Internet (e.g., host uptime, NAT usage, path changes, BitTorrent client popularity) [14]. Our framework and findings provide guidance to researchers interested in using Internet Background Radiation for their investigations.

3.3 Prior research without co-authors from CAIDA

CAIDA asks researchers to notify us when they publish their work that used UCSD-NT data. We also periodically check search engines looking for publications for which we did not receive notification. Despite our best efforts, we often discover publications years later, so we recognize that our list of papers *without CAIDA co-authors* at [19] represents a lower bound estimate: since 2005, more than 100 papers and PhD theses that used UCSD-NT data have been published. Figure 1 shows respectively the most recurring words in publication titles (left image) and the year of publication (right chart).

A large body of this literature studies **denial-of-service attacks**, **computer worms** such as Conficker, malicious **botnet** activities, and traffic models for **network intrusion detection**. However, we have been impressed with the reach of the data to other IT discplines, including development of new **machine-learning** methods, **visualization** techniques, and **big data processing** approaches. For example, in 2014, Fowler et al. presented at the *IEEE Symposium on Visualization for Cyber Security (VizSec)* a novel visualization that "enables the detection of security threats by visualizing a large volume of dynamic network data" [48].

Datasets derived from UCSD-NT traffic typically offer a *global* view of macroscopic phenomena (given the statistically significant fraction of IPv4 address space monitored), constituting a rare opportunity in fields with scarcity of large-scale empirical data. Several studies have crossed the borders of computer science and adjacent disciplines: Zhang et al. presented a study on hybrid (i.e., spreading both locally and globally) **epidemics** in which, by examining several datasets on disease as well as computer virus epidemics (using UCSD-NT data during worm spreading events) they developed a mathematical framework for studying hybrid epidemics [49] (this work appeared in *Nature - Scientific Reports*).

After we started offering researchers access to near-realtime UCSD-NT traffic in 2011, we began to see papers based on **live processing of traffic data** and in some cases proposing **on-line anomaly detection** techniques. For example, in [50], Khan et al. developed *"an online, adaptive measurement platform, which utilizes real-time traffic analysis results to refine subsequent traffic measurements"*. Reviriego et al. used the real-time data to improve the energy efficiency of traffic flow identification in routers and switches based on Cuckoo hashing [51].

The quality and the heterogeneity of the venues and journals where these works have appeared are remarkable: from highly-recognized networking conferences and journals (*IEEE/ACM Transactions on Networking, IEEE Infocom, IEEE Globecom, ACM Internet Measurement Conference*) to prestigious computer security communities (*IEEE Transactions on Information Forensics and Security, Usenix Security Symposium, Visualization for Cyber Security (VizSec), Journal of Digital Crime and Forensics*), and well-known journals in other fields (*Journal of Applied Statistics, Database and Expert Systems Applications, Simulation Modelling Practice and Theory, Social Computing*).

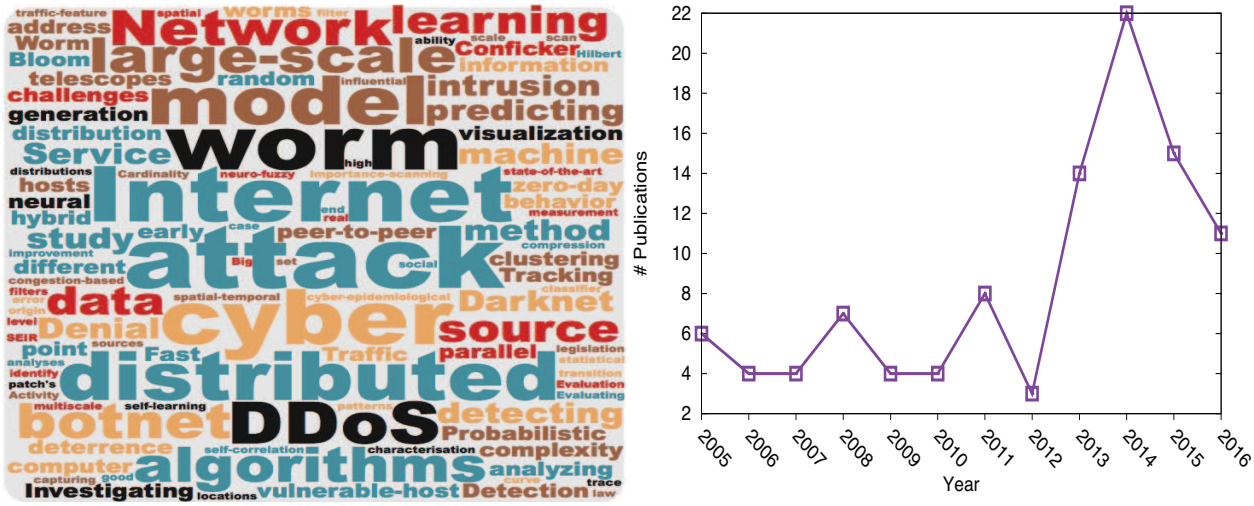

Figure 1: **Publications without co-authors from CAIDA**. The left figure shows the most recurring words in the titles of more than 100 publications authored by non-CAIDA researchers. The size of each word is proportional to its occurrence. Besides the top recurring words, this *wordcloud* highlights research involving visualization, artificial intelligence, statistical analysis, etc. The plot on the right shows the number of studies across the last decade; the large jump in 2013 followed our introduction of the near-real-time data sharing, which inspired new and expanded community attention to the potential of this data resource. (Note we are still in the process of searching for recent publications, so the 2016 count is incomplete.)

3.4 Education opportunities enabled

At least **six PhD theses** have used UCSD-NT traffic data [15, 19]. Of these, three are centered around darknet traffic and make intense use of UCSD-NT data [52, 53, 54] (also see letter of collaboration (LoC) from Snoeren, and LoC Xu). In particular, PI Dainotti **co-mentored PhD student** Karyn Benson (LoC Snoeren), whose dissertation thesis introduced several new classes of studies of properties of Internet hosts and networks that can be carried out through analysis of darknet traffic.

In 2014, to interest and train future researchers in performing analyses with telescope data, we developed and released, in collaboration with the University of Vienna, **two educational data kits** [55] – one based on the Egyptian country-level outage described in [11], and one used to analyze the effects of Microsoft Patch-Tuesday observed in darknet traffic [56]. These data kits combine curated snapshots of telescope traffic, tools, and procedures developed by CAIDA in a format suitable for use as teaching aids, both in out and of the classroom. The kits are currently used in networking classes at the Vienna University of Technology (LoC Zseby) [57]. Continuing this collaboration, we recently published in *IEEE Transactions on Education* a paper presenting a **network security laboratory project for teaching network traffic anomaly detection methods** to electrical engineering students. The Vienna University of Technology first implemented this laboratory during the Summer semester 2014, with a class of 41 students. All exercises and IP darkspace data are publicly available. The capabilities we propose to develop in STARDUST will make it possible to augment the lab activities carried out at the Vienna University of Technology (LoC Zseby) and extend them to classes in other universities (e.g., LoC Beverly).

Finally, CAIDA director Dr. Claffy lectures in networking and security classes at UC San Diego, a channel through which CAIDA attracts many undergraduate and graduate computer science students interested in studying "the real Internet".

3.5 Other government-funded projects enabled

The UCSD-NT infrastructure provides data to different U.S. government-funded projects. Since 2007 CAIDA is an active participant in *DHS's Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT)* project [16, 36] which aims to publicize and provide datasets for cyber-security research. We regularly index telescope data into the IMPACT metadata repository. This DHS project provides partial support for annotating and indexing UCSD-NT data, which enables us to leverage NSF infrastructure funds to add synergy and cross-agency momentum to the STARDUST project.

The UCSD-NT also represents an indispensable source of data for the NSF-funded project called *Internet Outage Detection and Analysis (IODA)* (Section **??**) [17, 58]. The goal of IODA is the development, testing, and deployment of an operational capability to detect, monitor, and characterize large-scale Internet infrastructure outages. Our approach relies on combining three main types of measurement data to infer network outages: responses to active probing, BGP routing data, and telescope traffic. IODA spurred several collaborations with other researchers and government agencies and received additional funding from industry (Comcast and Cisco).

CAIDA's DHS-funded *Spoofer* project seeks to minimize Internet's susceptibility to spoofed DDoS attacks. The project focuses on development and deployment of open-source software tools to assess and report on the deployment of source address validation (SAV) best anti-spoofing practices. Within Spoofer, the UCSD-NT provides backscatter traffic data from victims of randomly-spoofed denial-of-service attacks that we use to cross-validate inferences from other measurement tools developed for this project, and develop reports about attack trends.

3.6 Community satisfaction

The data collected at the UCSD-NT continues to attract new researchers. The trend in publications shown in Figure 1 (right chart) highlights that since we started offering access to near-realtime UCSD-NT traffic, the number of publications per year significantly increased[2].

We collected feedback about the availability of UCSD-NT data in several occasions and in particular we received positive feedback and ideas for improvement during the DUST workshop in 2012. In Section 5, we describe our plan to host two more workshops of the DUST series in Year 1 and 3 of our project, which will constitute opportunities to collect feedback to guide our planned infrastructure enhancements. In general, several researchers are interested in the ability to ascribe different portions of traffic to the network or to the geographic area that generated it. In Section 4.3, we describe our plan to label traffic data at flow-level granularity with IP geolocation and topological information in order to simplify these analyses. Similarly, to support these studies, we will add labels to identify portions of traffic forged to appear as originating from a different address, i.e., *spoofed* – since spoofed traffic invalidates any geographical or topological inference about its source (see LoC Mirkovic). In addition, some researchers have specific interest in studying spoofed traffic (LoC Beverly).

4 Plan for Achieving Community Sustainability

We organize our scope of work into three inter-related tasks. First, we will upgrade and modernize the current hardware (network communication hardware and storage) infrastructure to stabilize operations (Task 1). Second, we will transition the data analysis computing infrastructure to a sustainable model based on virtualization, leveraging NSF-funded HPC resources at SDSC (Task

[2]Data for 2016 should be considered incomplete, since at time of writing (early Jan. 2017) not all papers published in 2016 appear on search engines.

2). This task will include three connected sub-tasks: deploying cloud-compute support using new virtualization features of the Comet environment; redesigning the software pipeline to take advantage of this new capability; and collaborating with HPC researchers at SDSC to develop tools to support dynamic provisioning of Spark and Hadoop clusters as needed. Finally, we will introduce meta-data semantics that simplify many tasks researchers typically want to do with UCSD-NT data, leaving them more time to focus on their specific scientific questions.

We estimate that after accomplishing the proposed tasks, the cost of maintaining the telescope infrastructure operations will be about $85k per year. These costs can be covered as part of our research projects using the telescope data or with discretionary funds.

4.1 Task 1: Continuing operations

In this task, we will perform long overdue **upgrades and reconfiguration of hardware** in order to **handle modern network rates and improve the stability** of the UCSD-NT infrastructure. The top diagram in Figure 2 illustrates our current packet capture infrastructure. The UCSD-NT observes traffic reaching the unused portion of a /8 IPv4 address block (i.e., ≈16M IPv4 addresses) operated by a non-profit organization for experimental use. The telescope /8 address block is announced to the Internet through BGP by a UC San Diego router, which forwards all the traffic for the /8 to the non-profit organization's router (NP-router) through a 1 Gbps link. The upstream switch mirrors all traffic on this link to the UCSD-NT capture server, which filters away traffic to utilized addresses and then captures and compresses the remainder (i.e., traffic to all unassigned addresses in the /8 subnet) to files on disk. Every hour these files are transferred to a storage server that holds a sliding window of the last two months of raw pcap data, after which the files are transferred to an off-site tape archive. This server also performs processing to generate FlowTuple [27] data. Both the raw pcap data and the FlowTuple data are served via NFS to a research compute server providing a secure environment for guest researchers to analyze the data.

First, we will upgrade the traffic capture infrastructure components to sustain current data rates as well as to accommodate short-term traffic bursts and long-term traffic growth. Telescope traffic rates are highly variable and bursts of incoming packets can overload the capture infrastructure, resulting in **packet loss** (currently up to 50% during peaks). Besides the potential loss of data, packet loss impedes certain analyses, e.g., inferring patterns in scanning traffic. Another problem with the current hardware is **inaccurate packet timestamping**, which prevents correlation of telescope traffic with other data sources. To address these and other data quality issues, we will upgrade the capture network interface card from 1 Gbps commodity network card to a high-performance 10 Gbps capture card with accurate timestamping (e.g., Endace DAG [59]). To support replacement of the 1 Gbps capture interface we will upgrade all connected device interfaces (NP-router, storage server) to 10 Gbps and we will install an optical splitter (Figure 2 bottom). This configuration will allow data transfer from the capture infrastructure components to the storage server to keep up with the incoming traffic rates in order to support near-realtime traffic analysis.

We will also purchase and deploy an additional storage server and an attached disk array, with approximately 200TB of capacity. The current storage server has reached capacity due to ongoing archival of FlowTuple data (77 TB as of January 2017) and recent increases in telescope traffic rates. Recently we had to decrease our 2-months moving window of retained traffic data to only 15 days; this upgrade will allow us to revert to the previous most-recent 60-day window of UCSD-NT traffic.

Based on the trends observed in the last decade, we foresee that these upgrades will render the capture and storage components of the UCSD-NT infrastructure capable of sustaining current and increasing rates for many years. These components are relatively inexpensive compared to the

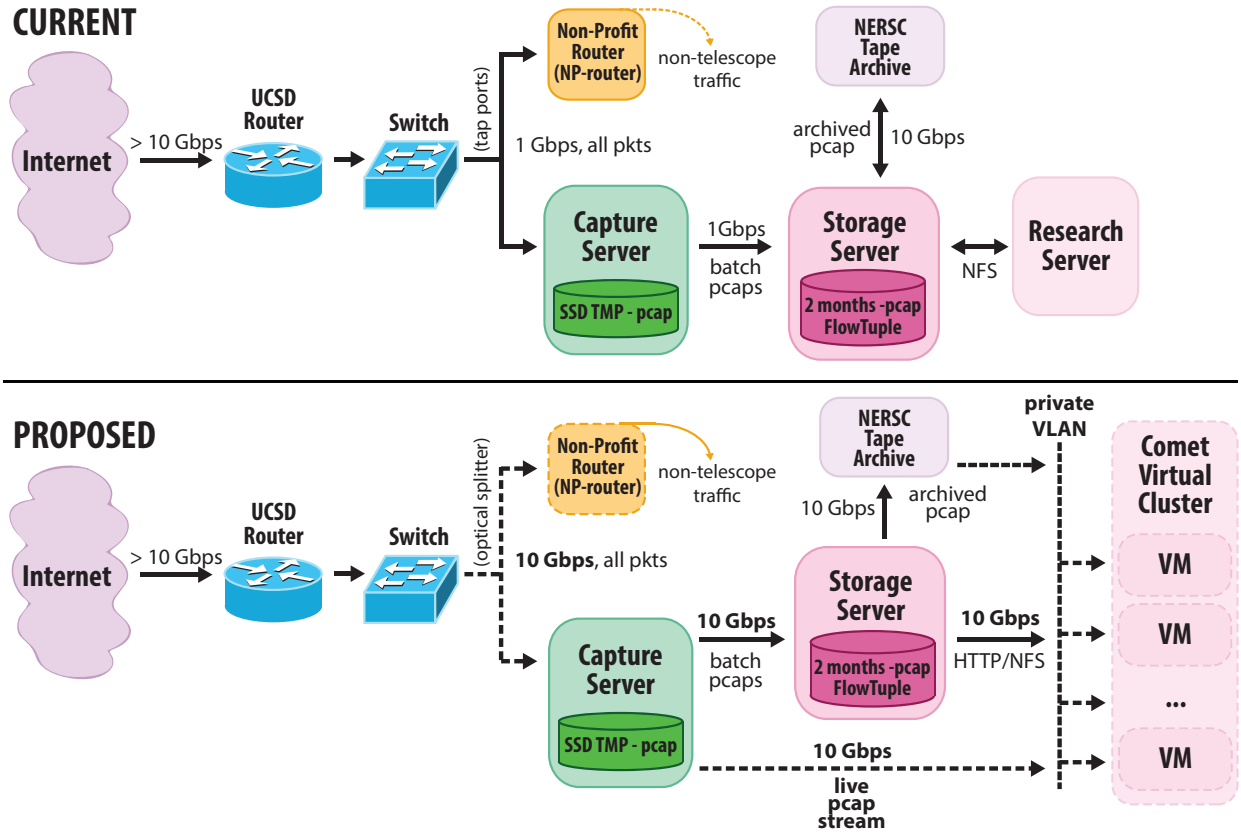

Figure 2: Current (top) and proposed (bottom) UCSD-NT packet capture and analysis infrastructure. Three notable changes between the current and proposed architectures are (highlighted with dashed lines): (i) upgrade of traffic capture interface and all other network interconnects from 1 Gbps to 10 Gbps; (ii) deployment of a real-time packet capture and distribution system ("live pcap stream" and "private VLAN"); (iii) transition from a single analysis server ("Research Server") to a scalable cloud-based cluster ("Comet Virtual Cluster").

computing infrastructure required to support data analysis by several researchers. Most importantly, these components do not need to scale with the number of users and their computational requirements. If in the future we need to upgrade these components again, we imagine that the few largest projects using the platform can fund the upgrades. The bigger challenge, which we discuss next, is to support the growing community's expanding set of research activities that use this infrastructure.

4.2 Task 2: Transition the data analysis infrastructure to a sustainable model based on NSF HPC resources

As the telescope traffic grows in velocity and volume and more researchers are interested in studying this traffic, we need more flexible, efficient, and **scalable resource allocation requiring less system administration overhead**. We also need to be able to **consistently obtain access to sufficient computing resources**. CAIDA is part of the San Diego Supercomputer Center (SDSC), which is a partner of XSEDE (eXtreme Science and Engineering Discovery Environment) [60], an NSF program that comprises the most advanced collection of integrated digital resources and services in the world. A key resource of XSEDE is the SDSC-hosted Comet supercomputer [61]

which has been specifically configured to meet the needs of researchers in domains that have not traditionally relied on supercomputers to help solve problems. "Comet is configured to provide a solution for emerging research requirements often referred to as the long tail of science, which describes the idea that the large number of modest-sized, computationally-based research projects still represents, in aggregate, a tremendous amount of research and resulting scientific impact and advance." [61] The XSEDE review committee, which evaluates requests for allocation of compute, visualization, and/or storage resources, welcomes and prioritizes projects serving a broad research community (LoC Norman). We already received an XSEDE *startup* allocation, which allowed us to test, in collaboration with Comet's HPC scientists (LoC Strande), some of the ideas proposed in this task. We will apply for a full Research Allocation on Comet through XSEDE to implement STARDUST. In addition, SDSC has a discretionary fund of Comet resources available for allocation (LoC Norman).

This task consists of the following three sub-tasks that coherently leverage the NSF-funded Comet infrastructure to create a scalable environment to support research using UCSD-NT data. First, we will use Comet's virtual clusters (VC) [62] technology to scale the number of simultaneous users of the system. Second, we will design and deploy a system for rapidly distributing live streams of telescope traffic to these virtual nodes, Third, we will build on an existing collaboration at SDSC to create a reference Apache Spark environment and toolkit that dynamically provisions HPC cluster resources as needed, which will dramatically improve the ability of researchers to scale data analysis needs over time (duration of traffic traces) and space (larger subsets of traffic).

Task 2.1. Provision and deploy a cloud-compute environment on a Comet Virtual Cluster

In modern HPC environments, projects often provide resources to external researchers by way of "Science Gateways", which are sets of tools, applications and data that are integrated through a custom interface (e.g., web portal). This approach limits the types of analyses that can be performed to those supported by the gateway interface. To overcome this limitation, **we will deploy a cloud-computing environment that uses the new "Virtual Cluster" (VC) feature provided by Comet** whereby projects may have unrestricted access to a set of Virtual Machines (VM) running on compute nodes, inter-connected with a customized network topology (which is key for implementing the live traffic distribution system we propose in Task 2.2). These VCs can be expanded and contracted dynamically, allowing resources to be scaled according to demand. Using a VC will also allow us to provide each researcher access to their own dedicated VM, onto which they may install a pre-configured OS image we will develop and tailor for telescope data analysis, or alternatively, any OS they prefer.

Researchers will also receive "root" access to their VM, allowing them to easily install required software packages – thus reducing the system administration overhead of the project. Another advantage of using VMs for analysis is that, unlike in our current shared-resource environment, heavy resource usage by one researcher cannot negatively impact analyses conducted by other researchers (another source of additional system-administration effort).

Additionally, once analysis has been completed, we can use the VC management interface to export a snapshot of a researcher's VM that they can archive, thus eliminating the incremental accumulation of researcher-specific data. Our transition to a cloud-compute environment introduces the **flexibility to migrate VMs to different underlying computing infrastructure based on future availability (e.g., new NSF-funded resources or even a commercial cloud)**. It will also enable resource accounting on a per-user basis, which would allow us to explore user-pays models as an alternative to bulk infrastructure funding.

Task 2.2. Develop and deploy live packet capture and distribution software

In this sub-task, we will implement a redesigned software pipeline to **distribute capture traffic to the VMs in real-time**. We currently use a customized version of the WDcap packet capture software [25] to perform full capture of the telescope traffic, and write it to disk in gzip-compressed pcap format. The resulting files are rotated hourly, and transferred from the capture machine to the storage server. In this configuration, the latency between when a given packet is captured and when it is available on the storage server for analysis is, on average, approximately 60 minutes. This delay is too long for certain applications, e.g., triggering active measurements in response to traffic observed at the telescope.

We will customize and extend the WDcap tool to forward captured traffic over a 10 Gbps management network interface to a CAIDA server where it will be buffered and then forwarded to a dedicated private VLAN. VMs running in the Virtual Cluster environment will be able to attach a virtual network interface and receive a real-time stream of captured packets. We will customize and extend the libtrace "RT" format [25] for encapsulation and distribution of captured traffic. This will allow researchers to analyze the real-time stream by writing analysis plugins for the Corsaro telescope data analysis framework we developed in our previously funded NSF CRI project [21], or by writing analysis software using the libtrace packet processing API [63].

Task 2.3. Dynamically provisioned specialized Big Data environments

In this task, we will develop software infrastructure to significantly **increase scalability of processing for longitudinal telescope data analysis** (i.e., very large datasets). Due to the overwhelming size of the historical telescope data archive (currently approaching 1 Petabyte of compressed pcap, and increasing at ≈36TB per month), longitudinal analysis is onerous and time-consuming. However, longitudinal analyses of telescope data typically consists of an initial stage of pre-processing hourly data files – either the raw pcap, or aggregated data such as FlowTuple – independently of one another to extract aggregate information that is further distilled in later stages. For example, a longitudinal study of Conficker may first extract only those packets matching the malware fingerprint, then subsequent stages would further process the (now much smaller) Conficker-only dataset. This type of process is perfectly suited to massive parallel architectures, and the multi-stage approach matches the processing paradigms of big data frameworks such as Apache Spark and Apache Hadoop.

To facilitate such analyses we will build on work that SDSC has undertaken to allow dynamic provisioning of Apache Spark (and Apache Hadoop) clusters on HPC compute resources [64]. (See LoC Strande.) These tools use the regular batch-scheduler to request time on a set of compute nodes, and then automatically configure and start all the processes needed for a Spark (or Hadoop) cluster (i.e., a master node and many slave nodes). Once the cluster has started, users may submit jobs as in a normal Spark cluster. Based on these tools, we will develop and deploy an interface that allows researchers to request and provision such a cluster for processing historical telescope data.

Since we store all the historical pcap files at an off-site tape archive, we will also develop helper routines/APIs for Spark and Hadoop that allow researchers to retrieve historical data directly from the archive during processing, eliminating the current bottleneck of requiring system administrator intervention as well as the need to occupy large amounts of local temporary storage. To further lower the barrier to entry for researchers, we will also develop sample analysis scripts and documentation that will provide a starting point for implementing longitudinal analyses.

4.3 Task 3: Reduce processing complexity and simplify data analysis

Telescope traffic can be *"unwieldy (huge) and messy, requiring a steep learning curve to make effective use of the data in empirical research efforts"* (LoC Snoeren) and requiring several pre-processing stages. Based on our experience in collaborating with and supporting other researchers in their analysis of telescope traffic, we have identified three meta-data types associated with network traffic that are commonly used. These meta-data types are all associated with the source IP address appearing in packets.

- IP geo-location: several studies need to isolate telescope traffic originating from a given country or region (e.g., studies related to Internet outages or censorship), or are interested in learning and visualizing the geographic distribution of traffic (e.g., studying botnet activities). To associate IP addresses with geographic locations, we use commercial geo-location databases updated weekly.
- Originating ISP (Internet Service Provider, identified with Autonomous System Number (ASN)): similarly, it can be necessary to extract traffic from a single AS (e.g., outages, path changes, NAT usage) or aggregate traffic with a given pattern (e.g., in order to rank malicious ASes propagating malware). We obtain IP-to-AS information by processing public BGP data made available by the RouteViews and RIPE RIS projects [65, 66].
- Spoofed source IP addresses: in a previous study [13] we have shown that the telescope receives large amounts of packets with a forged source IP address. On one hand, taking this data into account can yield wrong inferences, for example: when looking at IP-geolocation or AS lookup information as described in the previous two points; researchers interested in understanding the liveness of the IPv4 address space are also highly interested in filtering out these packets (LoC Mirkovic). On the other hand, understanding the extent and the characteristics of large IP address spoofing phenomena is a topic of research of its own (LoC Beverly). We infer spoofed packets using our heuristics based on packet header analysis as we describe in a recent paper [13].

In this task, we will extend the FlowTuple information extracted by our current infrastructure to tag each flow with this meta-data in order to (i) **reduce the computational cost for researchers analyzing telescope traffic, and (ii) simplify research tasks** by removing the need to perform meta-data tagging – which requires specific expertise – for each experiment. In addition, in the case of spoofing meta-data, this information can only be derived from raw pcap traces, which would prevent researchers from leveraging the light-weight FlowTuple data.

We will extend the FlowTuple format to include geo-location, origin-AS, and spoofed-source tags that we will generate using the Corsaro [27] software suite for performing large-scale analysis of trace data, which we developed in our previous NSF CRI project [21]. We will use the cloud compute environment described in Task 2.1, along with the real-time traffic stream described in Task 2.2 to deploy several "operational" analysis VMs to process the telescope traffic and derive our multi-level aggregated datasets. We will also explore efficient indexing of FlowTuple records, in order to dramatically reduce the volume of data to be processed when analyzing traffic with only certain meta-data characteristics (e.g., a given country or AS, or only spoofed packets).

Finally, in addition to creating hourly FlowTuple data files, we will provide real-time streaming access to Flowtuple data using Apache Kafka. Kafka is an open-source stream processing platform that provides high-throughput, low-latency, real-time data feeds. We will publish minute-granularity FlowTuple data, in JSON format, to a Kafka stream. In this way researchers can write high-level (e.g., Python/R/Node.js) code to consume live data from the Kafka stream rather than parsing the raw pcap or FlowTuple data. By leveraging our meta-data tags, we will create streams containing subsets of the overall traffic. For example, we will use the source IP address geo-

location tag to create one stream per country, reducing the processing complexity for researchers interested in traffic from specific countries.

5 Community Outreach

CAIDA regularly organizes international workshops that attract researchers both from academia and industry as well as program directors of funding agencies [67]. In particular, in 2012 CAIDA organized the 1st International Workshop on Darkspace and UnSolicited Traffic Analysis (DUST) [68], a two-day workshop that helped to publicize among the research community the availability of near-realtime UCSD-NT traffic data. We also organized two workshops – in 2014 and 2016 – on Internet Measurement and Political Science (IMAPS) [69], in which we presented our work on leveraging UCSD-NT data for studying Internet phenomena often linked to political protest and censorship, such as denial-of-service attacks and Internet filtering/blackouts. Interest of political scientists in this source of data has grown thanks to these workshops and allowed us to establish new collaborations that involve researchers and graduate students from other disciplines and universities.

In the second half of Year 1 of the project **we propose to host another DUST workshop**, focused on STARDUST and targeting existing and potential collaborators interested in using our telescope data and tools and improving telescopes as scientific instrumentation. We also plan to organize **a workshop during the third year** of the project to collect feedback and experience from early STARDUST users, and to present the new capabilities to a broader community of researchers.

We will open a new UCSD-NT public project website highlighting the new capabilities available, while an internal wiki will provide orientation material and documentation for all the tools and datasets available in STARDUST. We also plan to create a mailing list of STARDUST users to facilitate circulation of ideas and promote the creation of a community. This channel for information exchange will be especially useful if hands-on experience with real-time data analysis will prompt researchers to contribute to improving available tools for monitoring, analysis, and data visualization of the telescope data.

References

[1] "UCSD Network Telescope," 2010. http://www.caida.org/projects/network_telescope/.

[2] S. Staniford, D. Moore, V. Paxson, and N. Weaver, "The top speed of flash worms," in *ACM Workshop on Rapid Malcode (WORM)*, pp. 33–42, 2004.

[3] D. Moore and C. Shannon, "The Spread of the Witty Worm," *IEEE Security and Privacy*, vol. 2, no. 4, pp. 46–50, 2005.

[4] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," *IEEE Security and Privacy*, vol. 1, no. 4, pp. 33–39, 2003.

[5] D. Moore, C. Shannon, and J. Brown, "Code-Red: a case study on the spread and victims of an Internet worm," in *ACM Internet Measurement Workshop 2002*, Nov 2002.

[6] D. Moore, G. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," in *Usenix Security Symposium*, (Washington, D.C.), Aug 2001. **[Best Paper Award]**. http://www.caida.org/publications/papers/2001/BackScatter/.

[7] A. Dainotti, A. King, K. Claffy, F. Papale, and A. Pescapé, "Analysis of a "/0" stealth scan from a botnet," *IEEE/ACM Trans. Netw.*, vol. 23, pp. 341–354, Apr. 2015.

[8] E. Raftopoulos, E. Glatz, X. Dimitropoulos, and A. Dainotti, "How Dangerous Is Internet Scanning? A Measurement Study of the Aftermath of an Internet-Wide Scan," in *Traffic Monitoring and Analysis Workshop (TMA)*, vol. 9053, pp. 158–172, Apr 2015.

[9] A. Dainotti, R. Amman, E. Aben, and K. C. Claffy, "Extracting benefit from harm: using malware pollution to analyze the impact of political and geophysical events on the internet," *SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 1, pp. 31–39.

[10] K. Benson, A. Dainotti, k. Claffy, and E. Aben, "Gaining insight into AS-level outages through analysis of internet background radiation," in *Proceedings of the 2012 ACM conference on CoNEXT student workshop*, CoNEXT Student '12, (New York, NY, USA), pp. 63–64, ACM, 2012.

[11] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescapé, "Analysis of country-wide internet outages caused by censorship," *Accepted for publication in IEEE/ACM Transactions on Networking*.

[12] A. Dainotti, K. Benson, A. King, B. Huffaker, E. Glatz, X. Dimitropoulos, P. Richter, A. Finamore, and A. Snoeren, "Lost in Space: Improving Inference of IPv4 Address Space Utilization," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 34, pp. 1862–1876, Jun 2016.

[13] A. Dainotti, K. Benson, A. King, k. claffy, M. Kallitsis, E. Glatz, and X. Dimitropoulos, "Estimating internet address space usage through passive measurements," *Accepted for publication in SIGCOMM Comput. Commun. Rev.*

[14] K. Benson, A. Dainotti, k. claffy, A. Snoeren, and M. Kallitsis, "Leveraging Internet Background Radiation for Opportunistic Network Analysis," in *Internet Measurement Conference (IMC)*, Oct 2015.

[15] CAIDA, "CAIDA Papers." http://www.caida.org/publications/papers/?keywordslistings=networktelescope. Accessed: 2017-1-17.

[16] CAIDA, "The IMPACT Project." https://www.caida.org/projects/impact/. Accessed: 2017-1-17.

[17] CAIDA, "Internet Outage Detection and Analysis (IODA)." http://www.caida.org/projects/ioda/, 2014.

[18] CAIDA, "Spoofer." http://www.caida.org/projects/spoofer/.

[19] CAIDA, "Non-CAIDA Publications using CAIDA Data: UCSD Network Telescope." https://www.caida.org/data/publications/bydataset/index.xml#UCSDNetworkTelescope. Accessed: 2017-1-17.
[20] UCSD Network Telescope – Near-Real-Time Network Telescope Dataset. http://www.caida.org/data/passive/telescope-near-real-time_dataset.xml.
[21] CAIDA, "A Real-time Lens into Dark Address Space of the Internet." http://www.caida.org/funding/cri-telescope/.
[22] N. Brownlee, "One-way traffic monitoring with iatmon," in *PAM* (N. Taft and F. Ricciato, eds.), vol. 7192 of *Lecture Notes in Computer Science*, pp. 179–188, Springer, 2012.
[23] E. Kenneally and K. Claffy, "Dialing Privacy and Utility: A Proposed Data-sharing Framework to Advance Internet Research," *IEEE Security and Privacy (S&P)*, July 2010. http://www.caida.org/publications/papers/2009/dialing_privacy_utility/.
[24] "Apache Spark." http://spark.apache.org/, 2015.
[25] "WDcap." http://research.wand.net.nz/software/wdcap.php/.
[26] "tcpdump/libpcap." http://www.tcpdump.org/.
[27] A. King, "Corsaro," 2012. http://www.caida.org/tools/measurement/corsaro/.
[28] CAIDA Data - Overview of Datasets, Monitors, and Reports. http://www.caida.org/data/overview/.
[29] CAIDA, "Backscatter 2008 data." http://www.caida.org/data/passive/backscatter_2008_dataset.xml.
[30] CAIDA, "Witty data." http://www.caida.org/data/passive/witty_worm_dataset.xml.
[31] CAIDA, "Code red data." http://www.caida.org/data/passive/codered_worms_dataset.xml.
[32] "UCSD Network Telescope – Three Days of Conficker Dataset," September 2009. http://www.caida.org/data/passive/telescope-3days-conficker_dataset.xml.
[33] UCSD Network Telescope Dataset on the Sipscan. http://www.caida.org/data/passive/sipscan_dataset.xml.
[34] "UCSD Network Telescope – Two Days in November 2008 Dataset," June 2009. http://www.caida.org/data/passive/telescope-2days-2008_dataset.xml.
[35] UCSD Network Telescope Dataset – Patch Tuesday. http://www.caida.org/data/passive/telescope-patch-tuesday_dataset.xml.
[36] DHS Science and Technology Directorate, "Information Marketplace for Policy and Analysis of Cyber-risk and Trust (IMPACT)." https://www.impactcybertrust.org/.
[37] D. Moore, G. M. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," *Usenix Security Symposium*, 2001.
[38] D. Moore, C. Shannon, D. Brown, G. M. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," *ACM Transactions on Computer Systems*, 2004.
[39] Dainotti, A. and Pescapé, A. and Ventre, G., "Worm Traffic Analysis and Characterization," in *IEEE International Conference on Communications*, June 2007.
[40] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the Slammer Worm," *IEEE Security and Privacy*, vol. 1, no. 4, pp. 33–39, 2003.
[41] N. Weaver and V. Paxson, "A worst-case worm," *Workshop on Economics and Information Security (WEIS)*, June 2004. http://dtc.umn.edu/weis2004/weaver.pdf.
[42] D. Moore, C. Shannon, G. Voelker, and S. Savage, "Internet Quarantine: Requirements for Containing Self-Propagating Code," in *INFOCOM03*, 2003. http://www.caida.org/publications/papers/2003/quarantine/.

[43] A. Dainotti, A. King, "CAIDA Blog: Carna botnet scans confirmed." http://blog.caida.org/best_available_data/2013/05/13/carna-botnet-scans/.

[44] A. Dainotti, A. King, k. Claffy, F. Papale, and A. Pescapè, "Analysis of a "/0" stealth scan from a botnet," in *Proceedings of the 2012 ACM conference on Internet measurement conference*, IMC '12, (New York, NY, USA), pp. 1–14, ACM, 2012.

[45] A. Kuzmanovic, "Northwestern University - EECS 440: Advanced Networking." http://networks.cs.northwestern.edu/EECS440-f13/schedule.html, 2013.

[46] M. Gunes, "University of Nevada, Reno - CS 765: Complex Networks." http://www.cse.unr.edu/~mgunes/cs765/cs765sp13/, 2013.

[47] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescapé, "Analysis of country-wide internet outages caused by censorship," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, IMC '11, (New York, NY, USA), pp. 1–18, ACM, 2011.

[48] J. J. Fowler, T. Johnson, P. Simonetto, M. Schneider, C. Acedo, S. Kobourov, and L. Lazos, "Imap: Visualizing network activity over internet maps," in *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*, VizSec '14, (New York, NY, USA), pp. 80–87, ACM, 2014.

[49] C. Zhang, S. Zhou, J. C. Miller, I. J. Cox, and B. M. Chain, "Optimizing hybrid spreading in metapopulations," *Scientific Reports*, vol. 5, pp. 9924 EP –, 04 2015.

[50] F. Khan, N. Hosein, S. Ghiasi, C. N. Chuah, and P. Sharma, "Streaming solutions for fine-grained network traffic measurements and analysis," *IEEE/ACM Transactions on Networking*, vol. 22, pp. 377–390, April 2014.

[51] P. Reviriego, S. Pontarelli, and J. A. Maestro, "Energy efficient exact matching for flow identification with cuckoo affinity hashing," *IEEE Communications Letters*, vol. 18, pp. 885–888, May 2014.

[52] K. Benson, "Leveraging internet background radiation for opportunistic network analysis," 2016.

[53] C. Fachkha, "Darknet as a source of cyber threat intelligence: Investigating distributed and reflection denial of service attacks." December 2015.

[54] Z. Zhan, "A statistical framework for analyzing cyber attacks." 2014.

[55] CAIDA, "UCSD Network Telescope Educational Dataset: Analysis of Unidirectional IP Traffic to Darkspace." http://www.caida.org/data/passive/telescope-educational_dataset.xml, 2014.

[56] T. Zseby, A. King, N. Brownlee, and k. claffy, "The Day After Patch Tuesday: Effects Observable in IP Darkspace Traffic," in *Passive and Active Network Measurement Workshop (PAM)*, PAM 2013, Mar 2013.

[57] T. Zseby, "University of Vienna - 389.160 Network Security, Advanced Topics." https://tiss.tuwien.ac.at/course/courseDetails.xhtml?windowId=563&courseNr=389160&semester=2013W, 2013.

[58] CAIDA, "Detection and analysis of large-scale Internet infrastructure outages (IODA)." http://www.caida.org/funding/ioda/, 2014.

[59] Endace, "Capture Network Packet Device - Network Packet Sniffing Software - Deep Packet Sniffing Cards." https://www.endace.com/endace-dag-high-speed-packet-capture-cards.html. Accessed: 2017-1-17.

[60] J. Towns, T. Cockerill, M. Dahan, I. Foster, K. Gaither, A. Grimshaw, V. Hazlewood, S. Lathrop, D. Lifka, G. D. Peterson, R. Roskies, J. R. Scott, and N. Wilkins-Diehr, "Xsede: Accelerating scientific discovery," *Computing in Science Engineering*, vol. 16, pp. 62–74, Sept 2014.

[61] SDSC, "SDSC HPC Systems: Comet." http://www.sdsc.edu/services/hpc/hpc_systems.html#comet. Accessed: 2017-1-17.
[62] SDSC, "Comet User Guide: Virtual Clusters." http://www.sdsc.edu/support/user_guides/comet.html#clusters. Accessed: 2017-1-17.
[63] University of Waikato WAND Network Research Group, "*libtrace*: library for trace processing," 2005. http://research.wand.net.nz/software/libtrace.php.
[64] S. Krishnan, M. Tatineni, and C. Baru, "myHadoop - Hadoop-on-Demand on Traditional HPC Resources," in *Proceedings of the 2011 TeraGrid Conference: Extreme Digital Discovery*, Jul 2011.
[65] D. Meyer, "University of Oregon Route Views Project." http://www.routeviews.org/.
[66] RIPE, "Routing information service (ris)," 2008. http://www.ripe.net/ris/.
[67] CAIDA, "CAIDA Workshops." http://www.caida.org/workshops/. Accessed: 2017-1-18.
[68] T. Zseby and k. claffy, "DUST 2012 Workshop Report," *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 42, pp. 49–53, Oct 2012.
[69] CAIDA, "IMAPS - Internet Measurement And Political Science (IMAPS) Workshops." http://www.caida.org/workshops/imaps/. Accessed: 2017-1-18.