UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

itee PhD
information technology
electrical engineering

PhD student: Antonia Affinito

Analyzing malicious and large-scale phenomena over the Internet through the lens of the Domain Name System

Tutor: Prof. Alessio Botta

Cycle: XXXV

Year: Third

itee PhD
information technology
electrical engineering

Background information

- MSc degree: Computer Engineering
- Research group/laboratory: COMICS/ARCLAB
- PhD start date – end date: Nov. 2019 – Jan. 2023
- Scholarship type: Università “Federico II”
- Periods abroad: Apr. 2021 - Apr. 2022 at University of Twente, Enschede (the Netherlands)

Summary of study activities (1/2)

- Ad hoc courses:
  - “Scientific Programming and Visualization with Python”
  - “Virtualization Technologies and their Applications”
  - “Machine Learning”

- PhD schools:
  - “SSIE 2021 – IEEE Italy Section Summer School. Machine Learning Theory”
  - ”TMA PhD School 2022”

- MSc courses:
  - “Big Data Analytics and Business Intelligence”
  - “Intelligenza Artificiale”
  - “Data Management”

Summary of study activities (2/2)

- Conferences attended:
  - IFIP Networking Conference 2022, Catania (Italy), June 13-16 2022. Presentation of the paper "Local and Public Resolver: do you trade off performance against security?"
  - Network Traffic Measurement and Analysis Conference 2022, TMA 2022, Enschede (the Netherlands), June 27-30 2022. Presentation of the paper "Domain Name Lifetimes: Baseline and Threats"
  - Internet Measurement Conference 2022, IMC 2022, Nice (France), October 25-27 2022
  - International Conference on Emerging Networking Experiments and Technologies, CoNEXT 2022, Rome (Italy), December 6-9 2022

PhD Year	Courses	Seminars	Research	Tutoring
Year 1	31.9	6.6	36.1	0
Year 2	11	6.8	43.5	6
Year 3	0	2.65	61	0

Research areas

- Computer Networks and Internet
  - Activities of large interest occurring on the Internet
  - Impact of malicious and real-life events over the Internet
  - Domain Name System

Research results

- Development of a system for scanning activities detection in high-speed networks using Big Data techniques
- Empirical analysis of the performance of DNS resolvers
- Inference of lifetimes of domain names from 10 of the largest Top-Level Domains (TLDs), considering malicious short-lived domain names and take-down efforts
- Study of the impact of COVID-19 pandemic and Russia-Ukraine conflict on the Internet

Research products

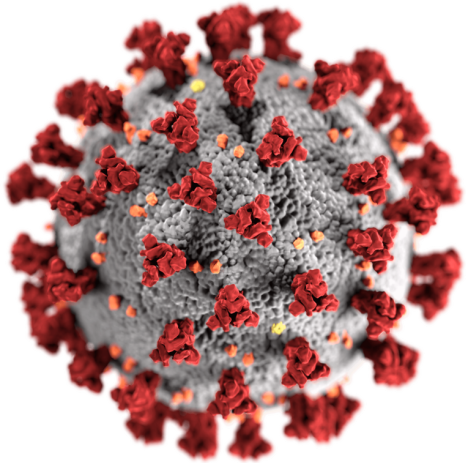
[P1]	A. Affinito, A. Botta, L. Gallo, M. Garofalo, G. Ventre, *Spark-based port and net scan detection,* Proceedings of the 35th Annual ACM Symposium on Applied computing (SAC '20), Virtual Conference, March 2020, pp. 1172-1179, Association for Computing Machinery (ACM)
[P2]	A. Affinito, A. Botta, G. Ventre, *The impact of covid on network utilization: an analysis on domain popularity*, IEEE International Workshop on Computer-Aided Modeling, Analysis, and Design of Communication Links and Networks, CAMAD, Virtual Conference, Sept 2020, pp. 1-6, IEEE
[P3]	A. Affinito, A. Botta, G. Ventre, *Local and Public DNS Resolvers: do you trade off performance against security?*, IFIP Networking Conference, Catania, Italy, June 2022, pp. 1-9, IEEE
[P4]	A. Affinito, R. Sommese, G. Akiwate, S. Savage, K. Claffy, G. M. Voelker, A. Botta, M. Jonker, *Domain Name Lifetimes: Baseline and Threats*, Proceedings on the 6th edition of the Network Traffic Measurement and Analysis Conference (TMA Conference) Enschede, the Netherlands, June 2022 ,IFIP
[P5]	M. Jonker, G. Akiwate, A. Affinito, KC Claffy, A. Botta, G. M. Voelker, R. van Rijswijk-Deij, S. Savage, *Where .Ru? Assessing the Impact of Conflict on Russian Domain Infrastructure*, Proceedings of the 22nd ACM Internet Measurement Conference, Nice, France, October 2022, pp. 159-165, Association for Computing Machinery

Research awards

- Receipt of the travel grant at ACM CoNEXT 2022
- Receipt of the travel grant at ACM IMC 2022
- Receipt of the travel grant at TMA PhD School 2022

PhD thesis overview

- Problem statement
  - Cyber threats and global societal phenomena are increasingly impacting the Internet, but current methodologies and tools are inadequate in effectively analyzing these events

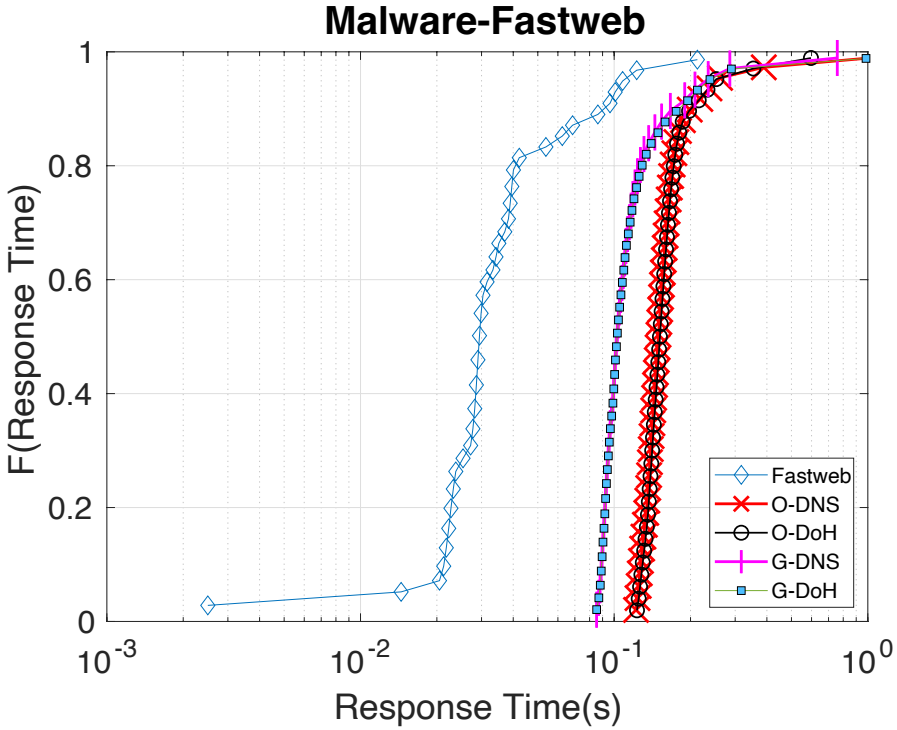


PhD thesis overview

- Objective
  - Development of methodologies and tools to shed light on current threats and global societal events, allowing better understanding and optimal operation of the Internet
- Methodology
  - Big Data analysis technologies to cope with data from high-speed networks
  - Small Data from Domain Name System (DNS) infrastructure and features to understand a large fraction of Internet phenomena
    - Active and passive measurements, TLD configuration files

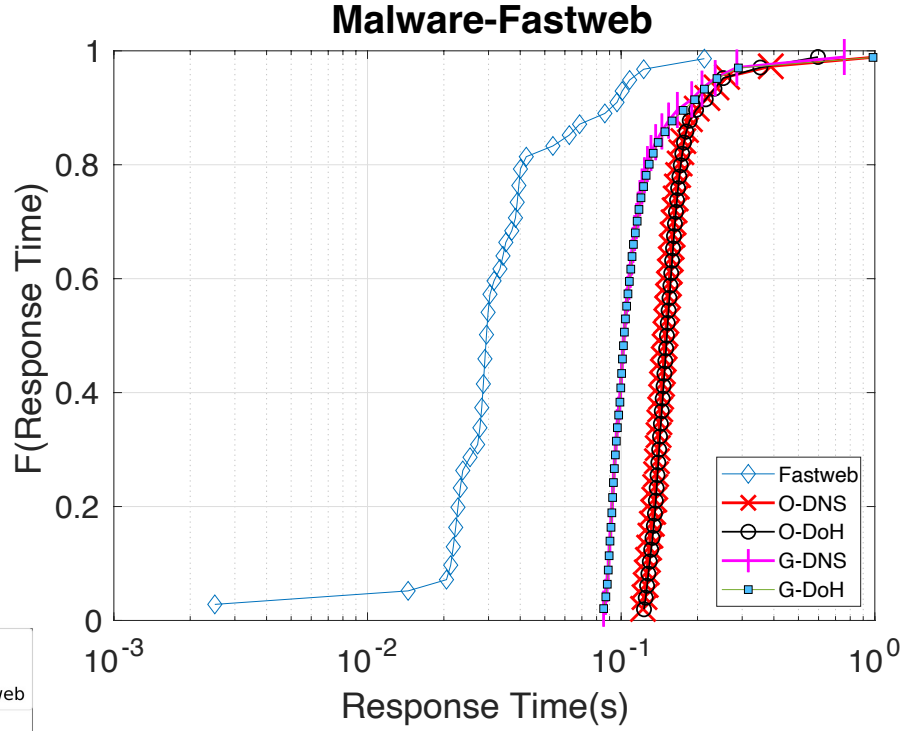
PhD thesis (1/4)

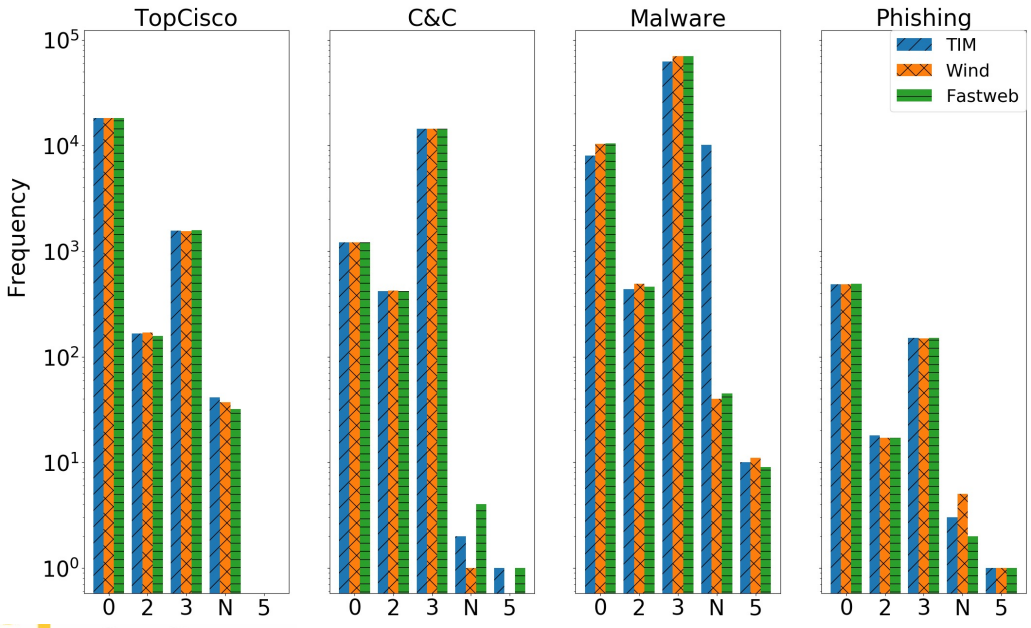
- Explore local DNS resolvers - **three main Italian ISPs** - and contrast them with **open, public** ones - Google and OpenDNS
- Analyze **timing performance**: time spent to perform a DNS query and obtain a response



PhD thesis (1/4)

- Explore local DNS resolvers - **three main Italian ISPs** - and contrast them with **open, public** ones - Google and OpenDNS
- Analyze **timing performance**: time spent to perform a DNS query and obtain a response





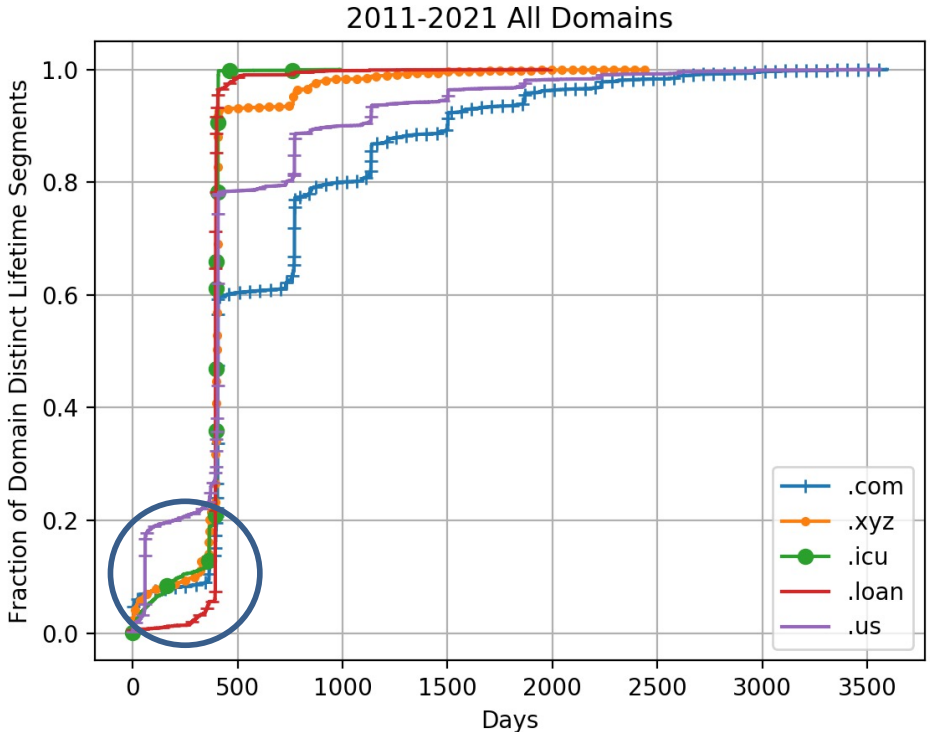
- Analysis of **malicious-domain detection performance**: capability to recognize domains associated with malicious activities, blocking related requests to protect users

PhD thesis (2/4)

- A non negligible number of domain **lifetimes** is shorter than one year, the minimum registration term. These domains are also referred to as **short-lived**
- Malicious names — especially short-lived — are taken down, quickly under some TLDs, never under others

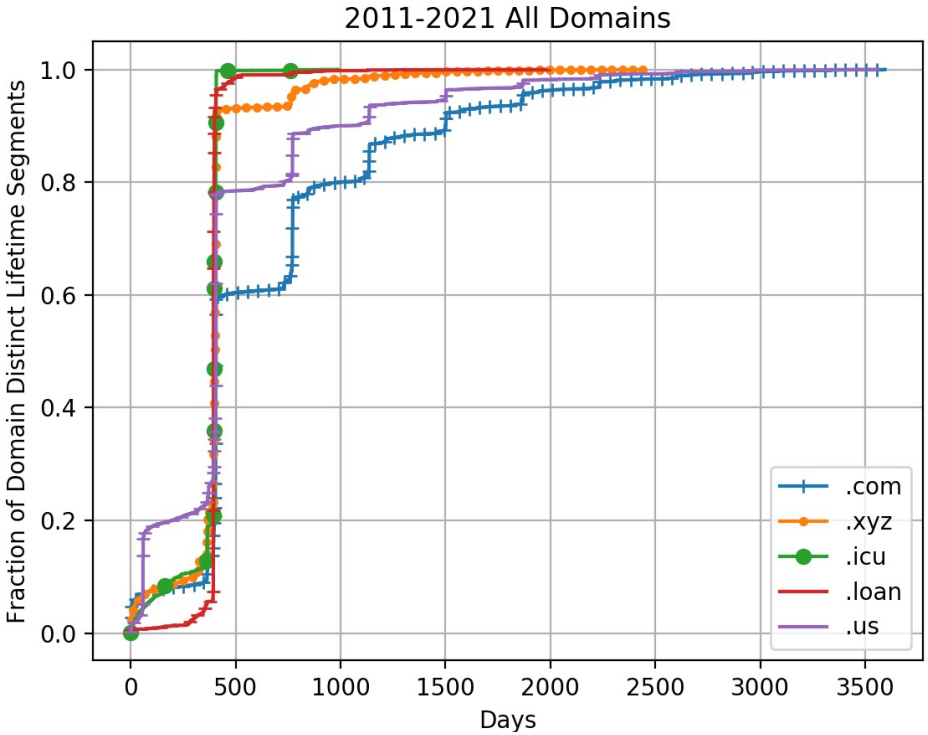
PhD thesis (2/4)

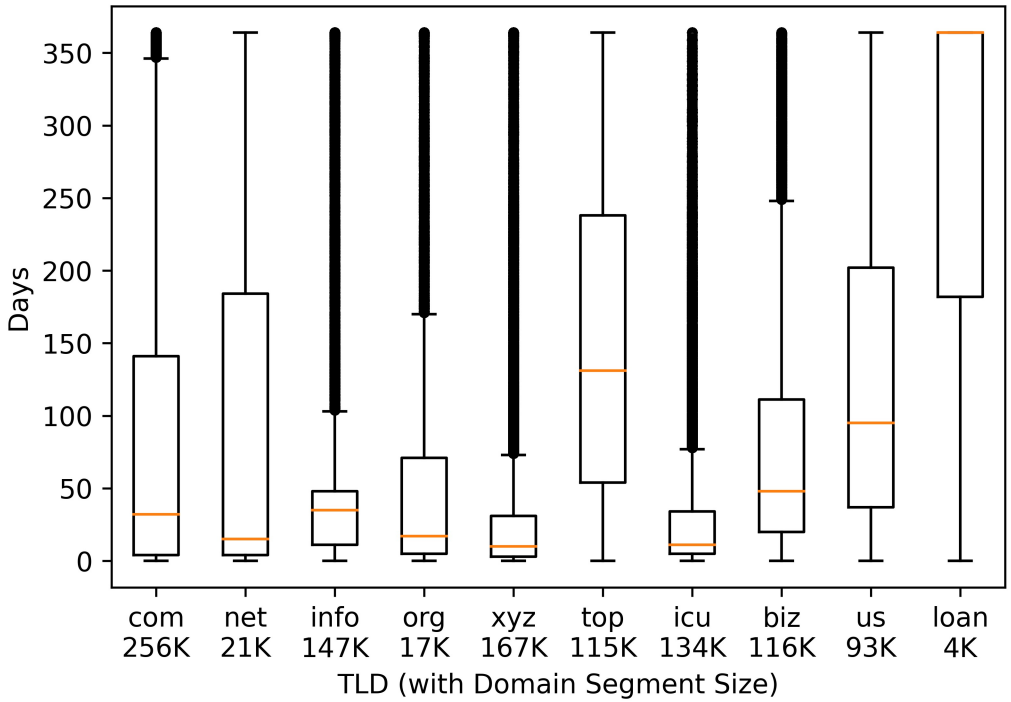
- A non negligible number of domain **lifetimes** is shorter than one year, the minimum registration term. These domains are also referred to as **short-lived**
- Malicious names — especially short-lived — are taken down, quickly under some TLDs, never under others



PhD thesis (2/4)

- A non negligible number of domain **lifetimes** is shorter than one year, the minimum registration term. These domains are also referred to as **short-lived**
- Malicious names — especially short-lived — are taken down, quickly under some TLDs, never under others





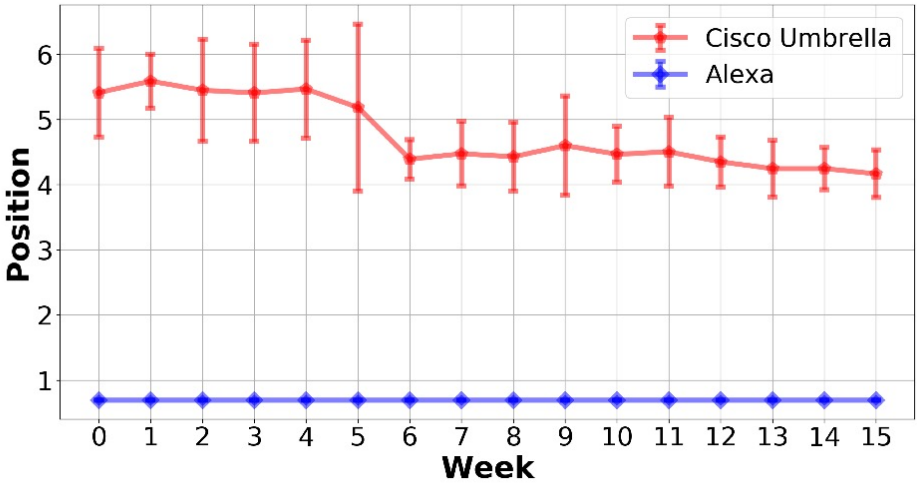
PhD thesis (3/4)

- Impact of **COVID-19** pandemic restrictions on different categories of **Internet applications**
- Analysis of two top 1 million domain lists
  - **Cisco Umbrella** -> most queried domains based on passive DNS
  - **Alexa** -> most popular sites visited using Alexa's browser extensions

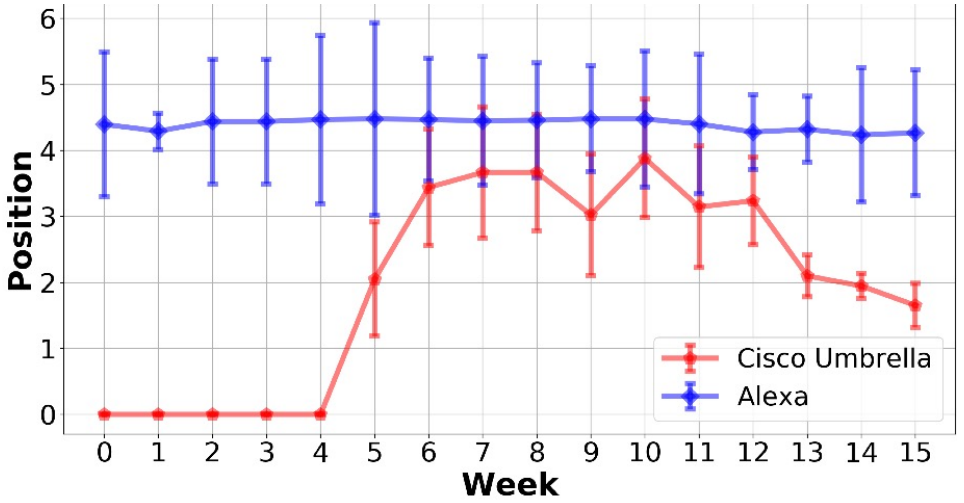
PhD thesis (3/4)

- Impact of **COVID-19** pandemic restrictions on different categories of **Internet applications**
- Analysis of two top 1 million domain lists
  - **Cisco Umbrella** -> most queried domains based on passive DNS
  - **Alexa** -> most popular sites visited using Alexa's browser extensions

youtube.com



netflix.com



PhD thesis (4/4)

- In November 2019, Russian governement introduced new regulations for centralized state management of the internet within Russia's borders
  - The implementation of a Russian national Domain Name System (DNS)

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»

Принят Государственной Думой 16 апреля 2019 года

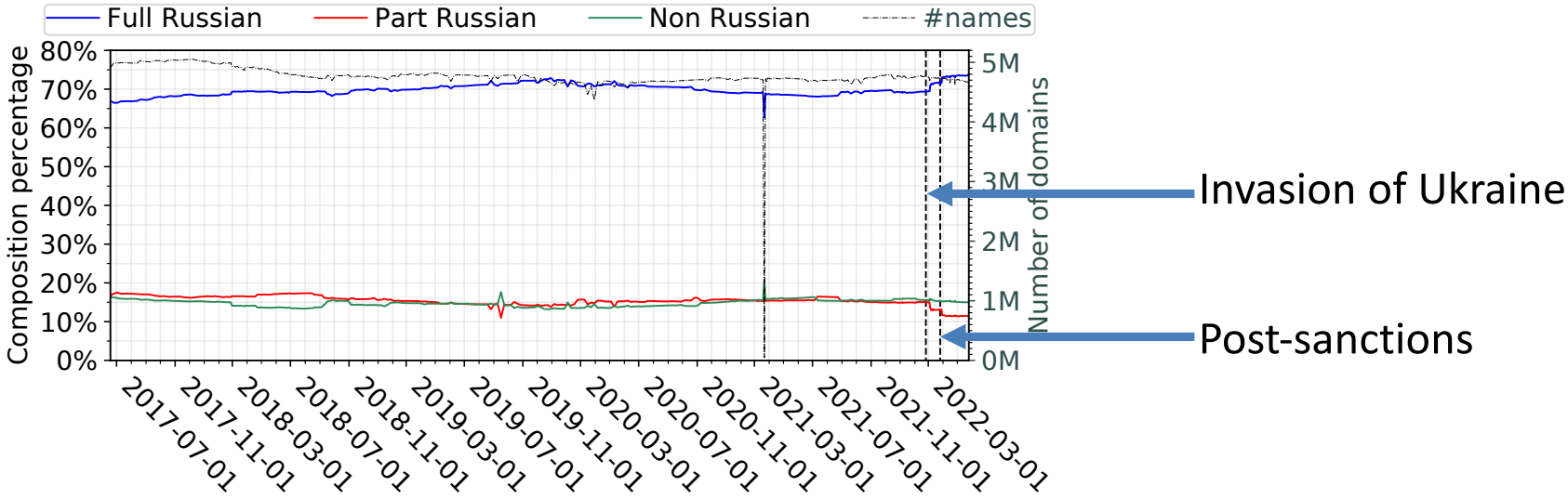
Одобрен Советом Федерации 22 апреля 2019 года

PhD thesis (4/4)

- Investigation of **longitudinal changes** in the infrastructure used by **Russian sites** — notably DNS, hosting, and TLS certificate issuance — before and after the **invasion of Ukraine**
- The analysis combines five years of daily **.ru** and **.рф** zone data, and **historic certificate** issuance data

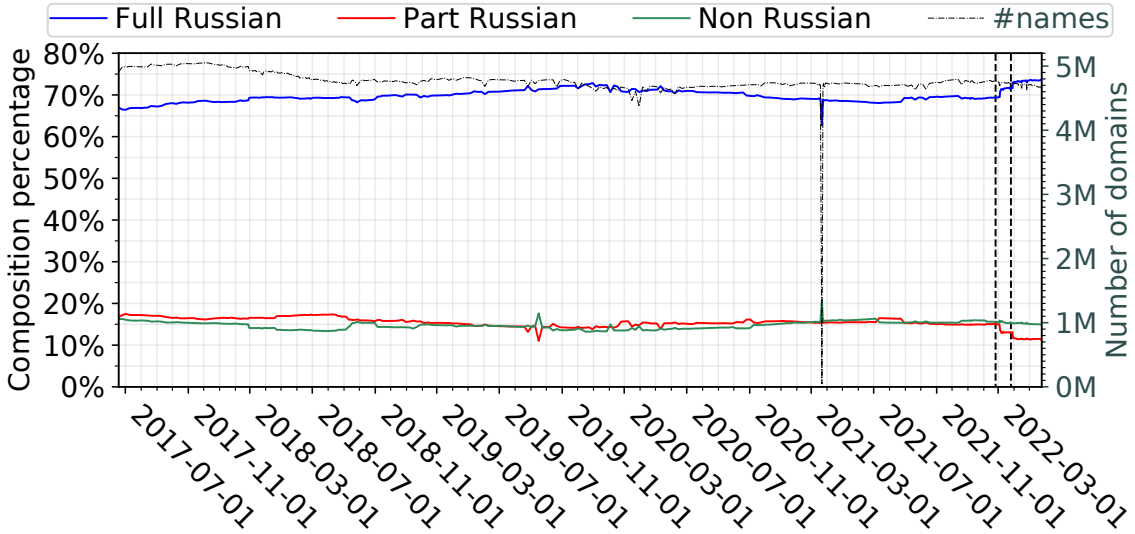
PhD thesis (4/4)

- Investigation of **longitudinal changes** in the infrastructure used by **Russian sites** — notably DNS, hosting, and TLS certificate issuance — before and after the **invasion of Ukraine**
- The analysis combines five years of daily **.ru** and **.рф** zone data, and **historic certificate** issuance data



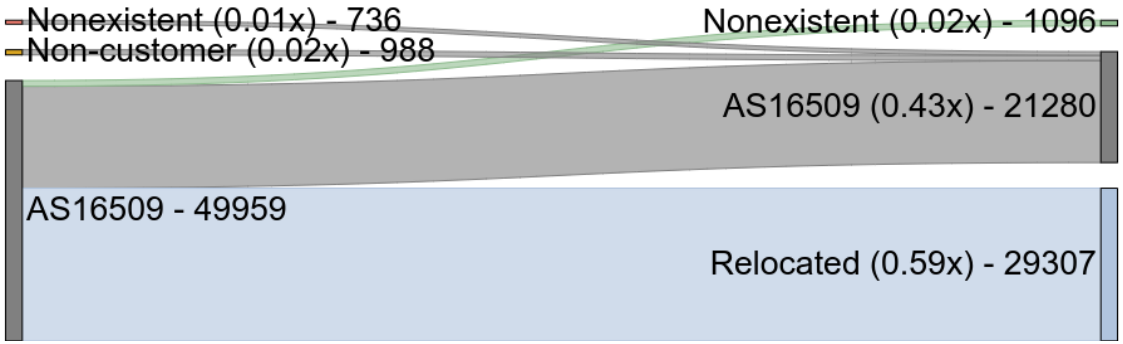
PhD thesis (4/4)

- Investigation of **longitudinal changes** in the infrastructure used by **Russian sites** — notably DNS, hosting, and TLS certificate issuance — before and after the **invasion of Ukraine**
- The analysis combines five years of daily **.ru** and **.рф** zone data, and **historic certificate** issuance data



Country composition of DNS infrastructure of **.ru and .рф domain names**

Russian domain name movement in **Amazon**'s AS16509



itee PhD
information technology
electrical engineering

CONCLUSIONS

- Protection level of local resolvers is largely comparable with the one of public resolvers. Response times of local resolver are shorter than the ones of public resolvers

- Domains are subject to take down efforts. In some TLDs this takes place quickly after domains have appeared on a blocklist

- During the first COVID-19 lockdown, the most used Internet applications were Youtube, Netflix, Whatsapp, and Skype

- After the start of the Ukrainian conflict and the bans from both governments, some Russian companies still use foreign Internet services, and some US companies still sell such services to Russian ones

THANKS FOR YOUR ATTENTION!