Where .ru? Assessing the Impact of Conflict on Russian Domain Infrastructure

MAPRG | IETF 115 London
November 10, 2022

Mattijs Jonker,[1] **Gautam Akiwate,**[2] Antonia Affinito,[3] kc Claffy,[4] Alesso Botta,[3]
Geoffrey M. Voelker,[2] Roland van Rijswijk-Deij,[1] Stefan Savage[2]

UNIVERSITY OF TWENTE.

UC San Diego
JACOBS SCHOOL OF ENGINEERING

caida

Context — Conflict [1/3]

- On February 24, 2022, Russia invaded Ukraine
- Produced strong global response
- Western countries imposed broad economic sanctions
- Independent of gov't actions, private sector companies restricted or exited the Russian market [1]

- [1] *"Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain," Yale Chief Executive Leadership Institute (CELI), 2022*

Context — Sanctions [2/3]

- The Internet has not escaped this conflict
- For example: corporate Russian websites on US OFAC SDN list
- Western Internet service companies independently disengaged from Russian market
  - … moral principle, reputational risk, economic volatility

Context — Internet Sovereignty [3/3]

- Actions reinforced Russia's long-held concerns about "Internet Sovereignty"
- Russian authorities mandated that all state-owned websites switch to domestic providers (March 2022)
- Ministry of Digital Development announced new Russian Root CA
  - … to be trusted by Russian browsers (VK Atom, Yandex.Browser)

Our goal

- Internal repatriation pressures combined with risk of further sanctions
  - → unprecedented environment for operators + customers
- Stands to reason that Russian sites rapidly decouple from non-Russian infrastructure
- We attempt to put this on **empirical footing**
- We studied longitudinal changes in infrastructure of Russian sites
  - DNS Infrastructure – Auth NS Infra
  - Hosting
  - Certificate issuance

Data — DNS [1/3]

- Active DNS measurement of Russian Federation domain names
  - all names under **.ru** and **.рф**
- Notably includes resource records: **NS**, **NS→A**, **@→A**
- Data covers almost five-year period (1803 days)
  - Extends years before invasion (2017-06-18)
  - … and 90 days into the war (2022-05-25)

- Some stats:
  - 11.7M unique names in total (~5M active)
  - 13.3k/9.5k unique ASNs for @/NS hosting

Data — TLS [2/3]

- Longitudinal certificate data for Russian Federation domain names
- Historic CT logs, active scan data (TLS, CRL, OCSP status)
  - From Censys (provided in bulk; thank you!)

- Some stats: ~115-130k certs issued/day (avg)

Data — Complementary [3/3]

- IP2Location to infer physical hosting (auth. NS, website)
- Sanctioned domain names (~110x)
  - US OFAC SDN & UK Sanctions list

Definitions

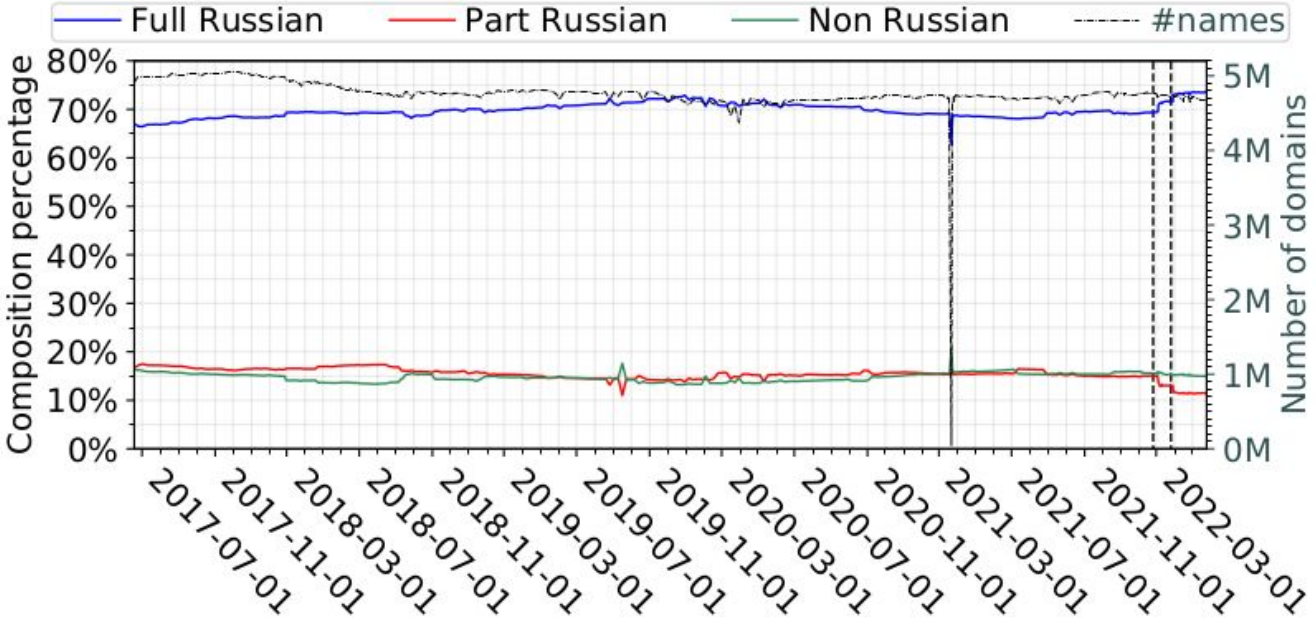
- **Three periods**
  - Pre-conflict — before February 24
  - Post-sanctions — after March 26
  - Pre-sanctions — the period in between
- **Hosting "composition"**
  - *Fully* Russian — all @ A records in Russia
  - *Non* Russian — none of the @ A records in Russia
  - *Part* Russian — some in Russia some not
- **DNS infrastructure "composition"**
  - Similar, but for A records of authoritative NS

Hosting — Historical Context [1/2]

- Historically, fraction of names hosted in Russia fluctuates only mildly
- June 18, 2017:
  - *Fully* Russian: 71%
  - *Partial:* 0.2%
  - *Not:* 28.8%
- Shows slight increase (Full and Partial) after the invasion
- Lots is already Russian
  - Could be manifestation of decade-long efforts
  - uncertain if significant change occurred pre 2017-06

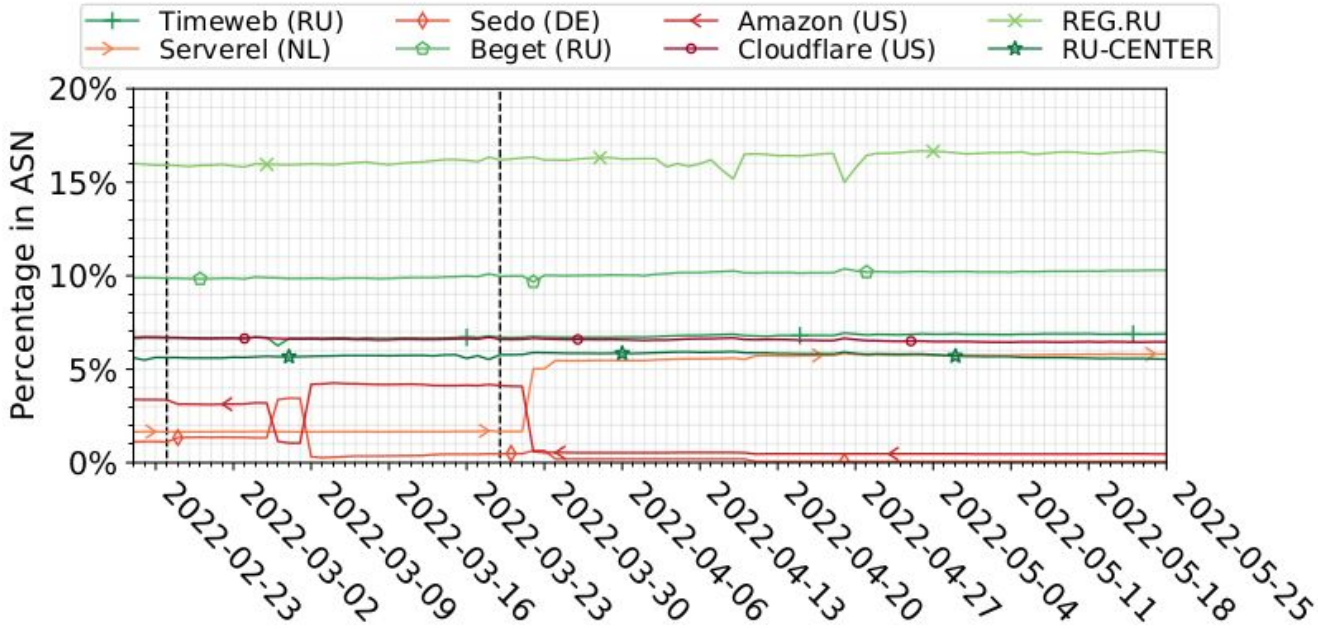
Hosting — Historical Context [2/2]

- Similar for NS infra, but more pronounced change after the Invasion
- Relatively stable over time, suggesting that internal pressures had limited effects
- Apparent changes in Feb. 2022, with *Partial* moving to *Full*
  - → Minor in historical context (6.9% change over five years)



Hosting — Recent Activity [1/2]

- Post-conflict, Russian domains experienced more movement in hosting networks
  - … almost entirely outside of Russia
- Russian ASNs have stable and consistent customer bases over time (38% of names)
- Networks that do experience movement involve Western providers
  - e.g., Amazon/Sedo flip-flop → Serverel (NL)

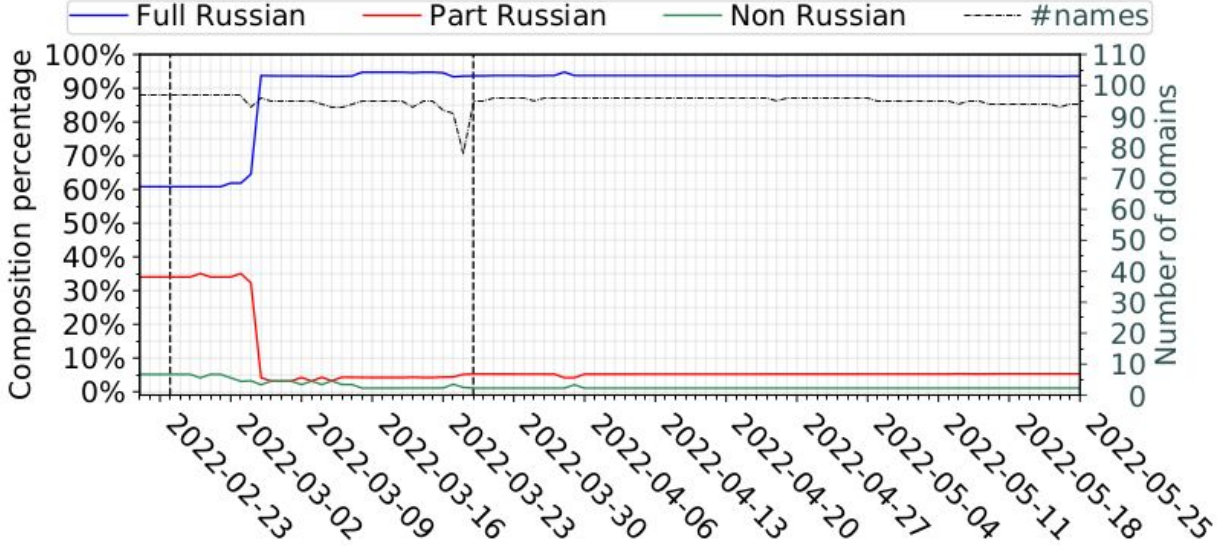


Hosting — Recent Activity [2/2]

- Russian domains also experienced movement in DNS infra hosting
- A significant change involved Netnod, a Swedish DNS provider, and RU-CENTER, a large Russian domain name registrar (March 3)
- One non-Russian network that sees use of DNS infra for a substantial no. of Russian domains is Cloudflare (seen little change)

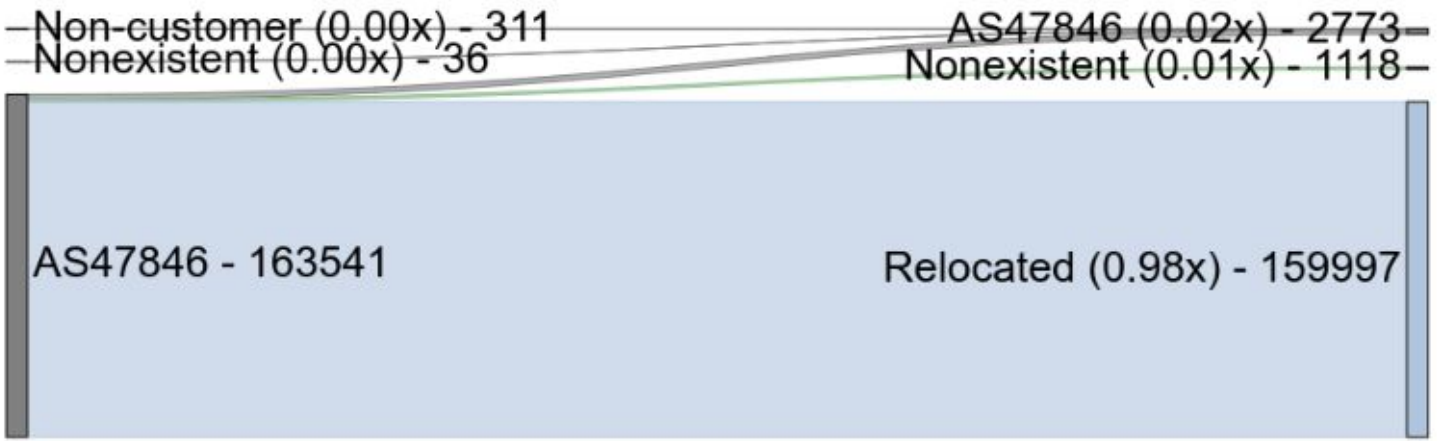
Hosting — Sanctioned Domain Names

- Names specifically tied to sanctioned Russian entities (US OFAC/UK lists)
- Significant movement for auth. NS hosting
  - Feb 24: 34% *Partial*, 5.2% *Non*
  - Mar 4: 93.8% *Full* (largely by the Netnod change)
- Potential for hosting (@) slight: 94.4% already *Fully* Russian before the conflict



Hosting — Actions Taken by Providers

- On Mar 9, Sedo was reportedly “pulling the plug”



- They followed through: by May 25, 98% of domains had relocated
- Other cases in paper (Amazon, Cloudflare, Google)

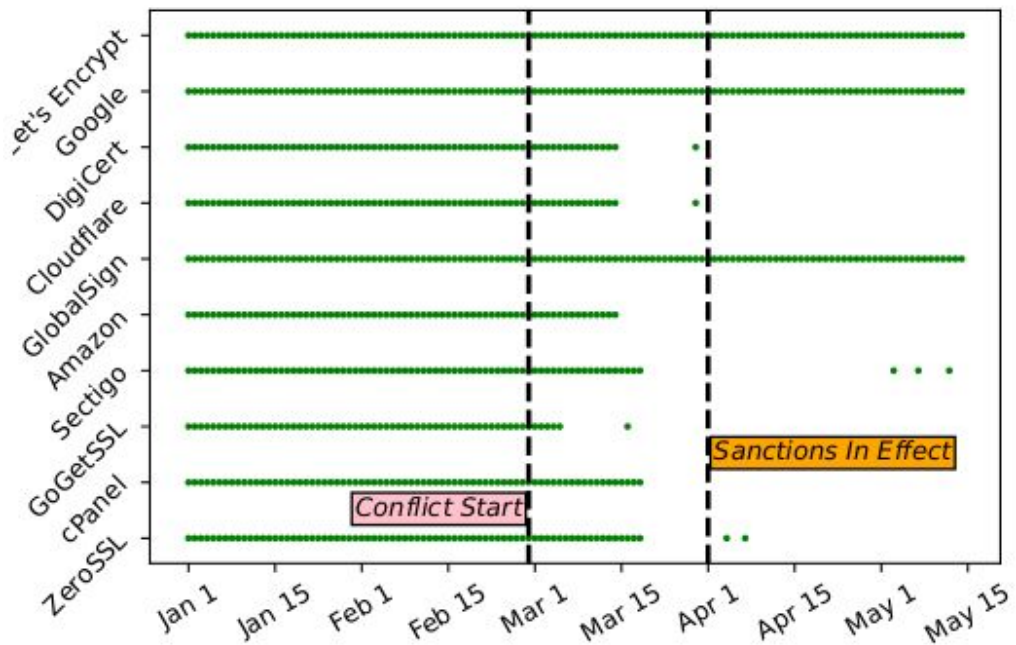
Web PKI — Certificate Issuance [1/3]

- Pre-conflict: long tail of CAs issue certs (~130k/day avg)
- Post-sanctions: only three CAs effectively participate
- Let's Encrypt already dominated pre-conflict (92%)
  - → Further increased post-sanctions (99%)

Pre-Conflict			Pre-Sanctions			Post-Sanctions		
Issuer Org.	**# Certs**	**(%)**	**Issuer Org.**	**# Certs**	**(%)**	**Issuer Org.**	**# Certs**	**(%)**
Let's Encrypt	6,586k	91.58%	Let's Encrypt	3,285k	98.06%	Let's Encrypt	5,458k	99.23%
DigiCert	244k	3.40%	GlobalSign	25k	0.76%	GlobalSign	28k	0.52%
cPanel	153k	2.13%	cPanel	11k	0.34%	Google	13k	0.24%
Other CAs	207k	2.89%	Other CAs	28k	0.84%	Other CAs	422	0.01%

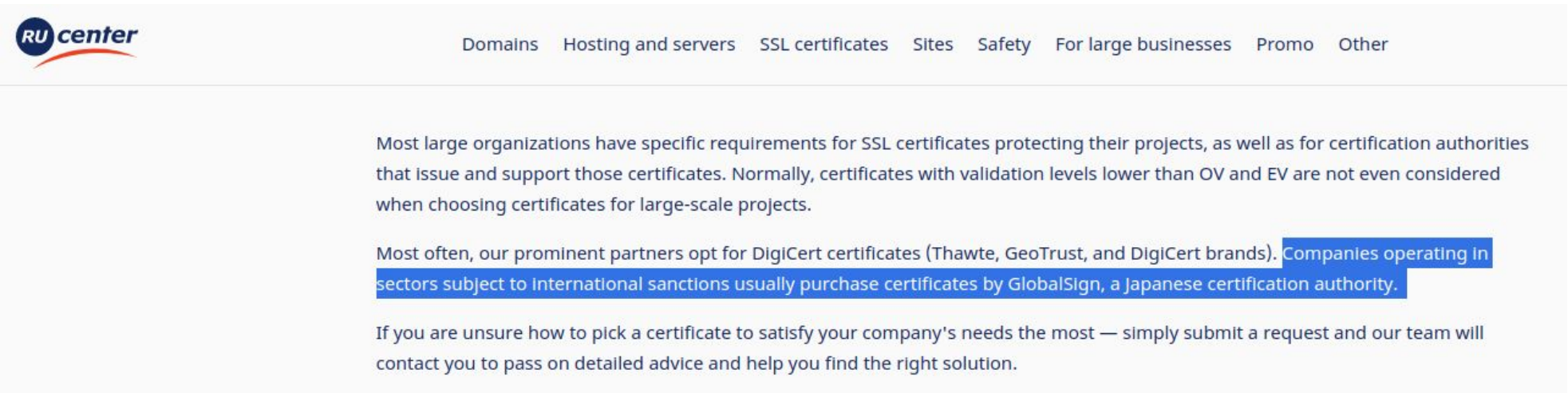
Web PKI — Certificate Issuance [2/3]

- Nearly all CAs stop issuing certificates a few weeks after conflict starts



Web PKI — Certificate Issuance [3/3]

- GlobalSign jumps into the Top 3 issuing CAs post-sanctions
  - Primarily serves sanctioned domains



Web PKI — Revocation

- Use CRLs and OCSP status (from Censys) to tally revocations after Feb 25th
- Both DigiCert and Sectigo revoked certs for all sanctioned domains
- We have no insight into policy decisions, but note all CAs have significantly higher revocation rates for sanctioned vs. all

	.ru and .рф Domains		Sanctioned Domains	
Issuer	**Issued**	**Revoked**	**Issued**	**Revoked**
Let's Encrypt	15M	10k (0.06%)	16k	196 (1.19%)
DigiCert	247k	2.1k (0.80%)	308	308 (100%)
GlobalSign	95k	1.6k (1.68%)	905	23 (2.54%)
Sectigo	96k	5.1k (5.15%)	164	164 (100%)
ZeroSSL	56k	165 (0.30%)	82	2 (2.43%)

Web PKI — Russian Trusted Root CA

- Created by Russia's Ministry of Digital Development (Mar 1, '22)
- Does not record in CT logs
- Using Censys (CUIDS) scan data, identify certs with this Russian CA
- Two trends:
  - Few domains secured by this CA (170; lower bound)
  - All certs secure Russia-related entities
    - 130/170 are Russian Federation (.ru and .рф), others affiliated with
    - 36/170 secure sanctioned domains
- Highlights low uptake, especially compared to Let's Encrypt dominance.

Discussion

- Russia long understood that the Internet could become a pressure point
- We have clear empirical evidence of this
  - Many thousands of Russian sites losing access to Western providers
- However, far from existential threat
  - First, pre-existing domestic provisioning (e.g., 70% *Fully* at conflict start)
  - Second, many providers continue to service Russian customers
- We note that cert issuance represents one area of significant exposure
  - The near-complete domination of LE is startling (99%)
  - LE has a public interest mission, but is also a US entity
  - Russia appears to not have anticipated this (e.g., by establishing domestic CAs with similar capabilities and trust relationships with major browsers)