Censored Planet

TSPU: Russia's Decentralized Censorship System

Diwen Xue
University of Michigan

Benjamin Mixon-Baca
ASU/Breakpointing Bad

ValdikSS
Independent

Anna Ablove
University of Michigan

Beau Kujath
ASU/Breakpointing Bad

Jedidiah R. Crandall
ASU/Breakpointing Bad

Roya Ensafi
University of Michigan

ABSTRACT

Russia's Sovereign RuNet was designed to build a Russian national firewall. Previous anecdotes and isolated events in the past two years reflected centrally coordinated censorship behaviors across multiple ISPs, suggesting the deployment of "special equipment" in networks, colloquially known as "TSPU". Despite the TSPU comprising a critical part of the technical stack of RuNet, very little is known about its design, its capabilities, or the extent of its deployment.

In this paper, we develop novel techniques and run in-country and remote measurements to discover the *how, what,* and *where* of TSPU's interference with users' Internet traffic. We identify different types of blocking mechanisms triggered by SNI, IP, and QUIC, and we find the TSPU to be in-path and stateful, and possesses unique state-management characteristics. Using fragmentation be-

1 INTRODUCTION

Since 201 h legal
and techı ıs [17].
In May 2 ıg tele-
com ope ıuially
known a is pro-
vides the ıtrally
and unil nds of
privately ıl was
establish ı from
the rest ɔreign
threats [
Previc of the
TSPU. Ir / with
its conte hreats

Throttling Twitter: An Emerging Censorship Technique in Russia

Diwen Xue
University of Michigan

Reethika Ramesh
University of Michigan

ValdikSS
Independent

Leonid Evdokimov
Independent

Andrey Viktorov
Independent

Arham Jain
University of Michigan

Eric Wustrow
University of Colorado Boulder

Simone Basso
OONI

Roya Ensafi
University of Michigan

ABSTRACT

In March 2021, the Russian government started to throttle Twitter on a national level, marking the first ever use of large-scale, targeted throttling for censorship purposes. The slowdown was intended to pressure Twitter to comply with content removal requests from the Russian government.

In this paper, we take a first look at this emerging censorship technique. We work with local activists in Russia to detect and measure the throttling and reverse engineer the throttler from in-country vantage points. We find that the throttling is triggered by Twitter domains in the TLS SNI extension, and the throttling limits both upstream and downstream traffic to a value between 130 kbps and 150 kbps by dropping packets that exceed this rate. We also find that the throttling devices appear to be located close to end-users, and that the throttling behaviors are consistent across different ISPs suggesting that they are centrally coordinated. Notably, this deployment marks a departure from Russia's previously

1 INTRODUCTION

Traditional Internet censorship relies on targeted blocking of con-
tent work
traffi key-
word n ex-
trem com-
plete ɔd ac-
cess
W been
obse: rship.
In co ı to a
servi This
offer: lt for
user: vn to
cens work
cong
In vitter

Network Responses to Russia's Invasion of Ukraine in 2022: A Cautionary Tale for Internet Freedom

Reethika Ramesh[†*] Ram Sundara Raman[†*] Apurva Virkud[†] Alexandra Dirksen[△]
Armin Huremagic[†] David Fifield Dirk Rodenburg[‡] Rod Hynes[‡] Doug Madory[◇] Roya Ensafi[†]

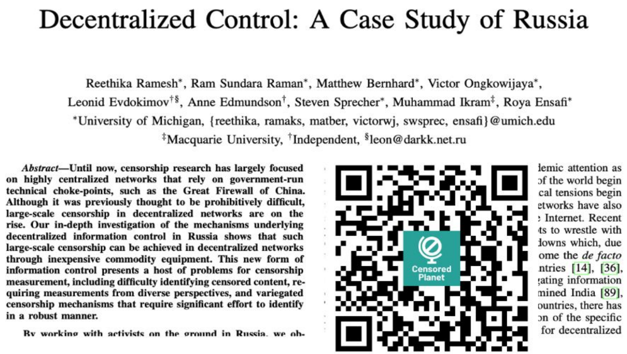
[†]*University of Michigan* [△]*TU Braunschweig* [‡]*Psiphon* [◇]*Kentik*

Abstract

Russia's invasion of Ukraine in February 2022 was followed by sanctions and restrictions: by Russia against its citizens, by Russia against the world, and by foreign actors against Russia. Reports suggested a torrent of increased censorship, geoblocking, and network events affecting Internet freedom.

This paper is an investigation into the network changes that occurred in the weeks following this escalation of hostili-

was ; ɔns, busi-
ness the state
of in ɩ's desire
to cc increase
cens ınd limit
the u reased in
both ing made
unav ities out-
side k access



Decentralized Control: A Case Study of Russia

Reethika Ramesh*, Ram Sundara Raman*, Matthew Bernhard*, Victor Ongkowijaya*,
Leonid Evdokimov[†§], Anne Edmundson[†], Steven Sprecher*, Muhammad Ikram[‡], Roya Ensafi*
*University of Michigan, {reethika, ramaks, matber, victorwj, swsprec, ensafi}@umich.edu
[‡]Macquarie University, [†]Independent, [§]leon@darkk.net.ru

***Abstract*—Until now, censorship research has largely focused on highly centralized networks that rely on government-run technical choke-points, such as the Great Firewall of China. Although it was previously thought to be prohibitively difficult, large-scale censorship in decentralized networks are on the rise. Our in-depth investigation of the mechanisms underlying decentralized information control in Russia shows that such large-scale censorship can be achieved in decentralized networks through inexpensive commodity equipment. This new form of information control presents a host of problems for censorship measurement, including difficulty identifying censored content, requiring measurements from diverse perspectives, and variegated censorship mechanisms that require significant effort to identify in a robust manner.**

By working with activists on the ground in Russia, we ob-

ɗemic attention as
ɔf the world begin
cal tensions begin
etworks have also
: Internet. Recent
ɩts to wrestle with
ɗowns which, due
ome the *de facto*
ntries [14], [36],
ɡating information
mined India [89],
ountries, there has
ɔn of the specific
for decentralized