Appendix 1: Description of the methodology used for the technical assessment of the sanctions' implementation.

In this section we provide a high-level overview of our experiments, measurement methodologies, and collected data. Our aim is to understand how access to select Russian resources may have been affected due to sanctions enforcement. We focus on connectivity and access to Russian media organisations from vantage points in Europe unless otherwise noted. We do not examine nor collect any traffic except that which is generated or required by own active measurements through the platforms RIPE Atlas, EduVPN, Dataplane.org and NLNOG RING or provided by OONI. All active measurements, including those originating from within Ukraine are designed to be low-impact and nonrecurring. For our RIPE Atlas measurements, we send 12 DNS queries per domain name spread over a period of three hours. OONI data is retrieved from the public s3 bucket and the raw data is reprocessed using the OONI Data tool[1]. OONI measurements are collected through their global network of volunteers who have gone through an informed consent procedure where they are informed of the risks associated with participating in this active measurement collection[2]. EduVPN, Dataplane.org, and NLNOG RING measurements are manual non- recurring and each vantage point (VP) is accessed sequentially with each measurement run in serial to prevent measurement traffic synchronisation toward targets.

1) Sanctioned resource selection

Block lists of domain names, IP addresses, URLs, or routing information are commonly used to enforce network operator policies. In early 2022 we considered two technical proposals that use block list techniques to enforce internet sanctions against Russia. One is an ambitious, community cooperative project focused on transparency[3]. Another is a DNS-based firewall approach that blocks access to IP addresses geo-located to any country under sanction by the US government[4]. We found no evidence that either approach has been widely deployed, nor consensus on how they should be deployed.

We then evaluated US and European economic sanction lists published by national and regional government agencies. One of the best known and most influential is from The Office of Foreign Assets Control (OFAC) in the US Department of Treasury (USDOT). OFAC maintains and enforces economic sanctions targeting various entities around the globe, but it is primarily a list of foreign agencies, commercial organisations, and individuals[5]. This list data is populated with names, aliases, and known physical addresses, but may also include associated internet resources such as URLs, email addresses, or cryptocurrency wallet identifiers. However, we often found the internet-specific attributes in OFAC data to be incomplete, inconsistent, or inaccurate.

1 OONI Data Kraken. [n. d.]. https://github.com/ooni/data.

2 Open Observatory of Network Interference (OONI). [n. d.]. https://ooni.org/about/risks.

3 We, The Undersigned. 2022. Multistakeholder Imposition of Internet Sanctions. https://wiki.sanctions.net/index.php/The_Open_Letter.

4 MacFarlane, Druce. 2022. Infoblox Response to Ukraine Crisis. https://blogs.infoblox.com/security/infoblox-response-to-ukraine-crisis.

5 Office of Foregin Assets Control, U.S. Department of the Treasury. [n. d.]. https://ofac.treasury.gov/ofac-sanctions-lists.

Furthermore, we could find no evidence that the OFAC list was being widely used for internet sanctions enforcement. EU-based sanctions regulations were more scattered. In many of these sanctions data sets, we found similar issues that would make transforming them into internet block list solutions difficult.

Despite the apparent consistency and specificity challenges with existing economic sanctions data, multilateral internet sanctions against Russia began to take shape immediately following the February 24, 2022 attacks on Kyiv. Implementation details from network providers were few and far between with some ISPs grudgingly left to work out the details for themselves[6]. We decided to construct our own list drawn from multiple authoritative sources. See Table 1. The focus on Russian media in our study reflects the focus of sanctions from official European governing bodies, but we also include two well-known Russian banks and a branch of the Russian government that have been sanctioned by the US. In most of our experiments we also utilise two control web sites that are not covered by any known sanctions. One is a static, benign website on a U.S. academic network. The other is the icanhazip IP address test site run by Cloudflare[7].

2) Experiments and measurements

Internet sanctions enforcement may occur at a variety of points in the communications path or at different layers in a protocol stack. To evaluate enforcement we examine access across four broad dimensions: reachability, Domain Name System (DNS) response, Transport Layer Security (TLS) handshake, and Hypertext Transfer Protocol (HTTP) connection.

IP and transport reachability. We issue a series of ICMP, TCP, and UDP traceroute probes to our sanctions list to identify when enforcement occurs at the IP or transport layers. Traceroute access failures typically indicate network-layer enforcement mechanisms such as a packet filter on a firewall or via a firewalls or black hole route announcement. Where applicable, failures above the IP layer by experiments described below are also recorded.

DNS query response behaviour. For each domain in our sanctions list we perform both A and AAAA DNS queries over UDP transport. Few names have associated AAAA (IPv6) address map- pings and we are limited by each vantage point's local network configuration whether we can conduct experiments over both IPv4 and IPv6. Unless otherwise indicated, all results are based on IPv4 transport. When necessary, we perform identification queries to detect the resolver configuration if it is not directly available to us. We identify block-attempts by relying on fingerprints published by OONI [8]. Additionally, we manually examine if IP addresses point towards websites. If the website contains information about blocking efforts, we classify the response as a block-attempt. Finally, we classify DNS responses containing errors or non-routable IP addresses (like 127.0.0.1) as block-attempts.

6 UK sanctions law, A&A, and Domain blocking. [n. d.]. https://www.aa.net.uk/etc/news/uk-sanctions-law-aa-and-domain-blocking/.

7 Major Hayden. 2021. A new future for icanhazip. https://major.io/2021/06/06/a-new-future-for-icanhazip.

8 OONI blocking-fingerprints [Online]. [n. d.]. https://github.com/ooni/blocking-fingerprints/blob/main/fingerprints_dns.csv.

TLS handshake. We perform a TLS handshake to the IP addresses associated with port 443 on the targets and perform TLS certificate verification. We can detect TLS MiTM attempts by evaluating whether the server X.509 certificate returned is valid given the SNI and destination IP address in our requests when validated against the Mozilla root certificate list[9].

HTTPS request. Once a TLS session has been established, we attempt to retrieve the content of the homepage by issuing a HTTP GET request for the / resource. We issue requests over both HTTP (80) and HTTPS (443) where applicable. For each session we record all relevant HTTP response metadata (e.g., headers and response status code) as well as body content.

3) Network measurement platforms

For our study, we rely on a variety of network measurement platforms. Combined, these platforms allow us to run and evaluate a variety of network experiments from in-country vantage points. The OONI and RIPE Atlas platforms are widely used, well understood, and described elsewhere[10][11]. In OONI most URLs were already part of the testing lists, and those missing were added in April 2023[12]. EduVPN, Dataplane.org, and the NLNOG RING may be less familiar to readers so we briefly summarise them below.

EduVPN is a federated VPN project coordinated by SURFnet, the National Research & Education Network (NREN) for the Netherlands[13]. Participating organisations can provide two types of access: Institute Access and Secure Internet. The former grants access to the internal resources of the host institution. The latter, which we use, only grants access to the public internet through a trusted server. Our motivation for using EduVPN is to assess the enforcement of sanctions in academic and research networks. We set up individual VPN connections at each EduVPN server to appear as a local client on the host network. DNS resolution configuration varies by institution. We had access to 11 academic networks, of which four were within the EU.

Dataplane.org is a non-profit network observation and measurement platform that operates over 300 dedicated and virtual Linux server systems[14]. The majority of vantage points are in hosting provider data centers around the globe. While these systems may not reflect end-user experiences, they help provide additional insight into sanctions enforcement seen in hosting environments or at the country-level. Almost all vantage points on this platform utilise Google Public DNS[15].

9 Mozilla. [n. d.]. https://wiki.mozilla.org/CA.

10 Arturo Filastò and Jacob Appelbaum. 2012. OONI: Open Observatory of Network Interference. In 2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI 12). USENIX Association, Bellevue, WA. https://www.usenix.org/conference/foci12/workshop-program/presentation/Filast{ò}

11 RIPE Ncc Staff. 2015. Ripe atlas: A global internet measurement network. Internet Protocol Journal 18, 3 (2015), 2–26.

12 Russian media github pull request. [n. d.]. https://github.com/citizenlab/test-lists/pull/1271

13 EduVPN. [n. d.]. https://www.eduvpn.org.

14 Dataplane.org. [n. d.]. https://dataplane.org.

15 Google Public DNS. [n. d.]. https://developers.google.com/speed/public-dns/.

NLNOG RING is a project administered by the non-profit Netherlands Network Operator Group (NLNOG)[16]. This platform is a collaborative troubleshooting network consisting of over 600 Linux-based virtual machines (VMs) in many distinct autonomous systems around the world. Participating networks contribute VMs and in return are granted access to all others in the network. The platform is widely used by network operators to troubleshoot and debug network-related issues using common Unix-based tools. All vantage points use a locally installed DNS resolver.

4) Detailed Measurement Findings

For a more in-depth description of the methods, findings, and measurements we refer to the video presentation on this research: https://archive.org/download/foci2024-1/video-01-kristoff.mkv and the technical conference paper we wrote about this: https://www.petsymposium.org/foci/2024/foci-2024-0001.php

16 NLNOG RING. [n. d.]. https://ring.nlnog.net.