Doug Madory, Kentik





- Initial months of invasion (Feb-Mar 2022)
 - Impacts in Ukraine
 - Impacts in Russia
- Conflict shifts east and south (Summer 2022)
- Ukraine counteroffensive, Russian retaliation



- Initial months of invasion (Feb-Mar 2022)
 - Impacts in Ukraine
 - Impacts in Russia
- Conflict shifts east and south (Summer 2022)
- Ukraine counteroffensive, Russian retaliation



As NANOG 84 was winding down in Austin, TX in Feb...

- Russian troops amassed on Ukraine's border. Then the DDoS attacks began.
- Initial targets included (15 Feb)
 - Mirohost (AS28907), hosts the Ukraine Army website...
 - Privatbank (AS15742), one of Ukraine's largest bank supported bits/s
 - Oschadbank (AS60173), state savings bank of Ukraine.

≡ Menu					Feedback	Q A •
♦ CORE > Data Explorer			HI Full width	G Refresh	 Actions 	\Xi Query
Top Dest AS Number by Avera	age bits/s Inter	net Traffic to Uk	traine			
Pada	DDoS attacks a	gainst Mirohost (A	AS28907)		·	



H Full width 😘 Refresh 💌 Actions 💌 😇 Que

Internet Traffic to PrivatBank (AS15742

https://twitter.com/DougMadory/status/1493680334965297159

Ukraine became a frequent target of DDoS attacks

- DDoS attacks continued and shifted to Ukrainian government targets.
- On 23 February, the targets included Ukraine's:
 - Parliament (Rada), foreign ministry (MFA), and executive cabinet (KMU)
 - Attacks weren't novel or record-breaking in size, but did disrupt access.



Russia invades Ukraine on early on 24 February

European satellite operator disrupted by cyberattack

- 24 Feb: Beginning at ~4:20 UTC, AS29286 experienced a large drop in traffic & responses to active probes.
- 28 Feb: SentinelOne reported satcom modems were commanded by compromised support servers to run destructive malware
- "It was a really huge loss in communications in the very beginning of war," Viktor Zhora, a senior official at Ukraine's cybersecurity agency





Outages in Ukraine following the invasion

25 Feb: largest initial outage was national broadband operator Triolan (AS13188).

Triolan would later go down twice more as a result of "cyberattacks" against their network.





Outages in Ukraine following the invasion

Ukrainian incumbent Ukrtelecom (AS6849) also experienced multiple outages.

Only the 7th most popular traffic destination in Ukraine, but incumbents are often only option for service to rural areas.





Ukrtelecom also suffered an outage on 28 March due to a "cyberattack" - note the slow decline in connectivity over ~5hrs. \rightarrow

Few details about the attack emerged...



the potential implication that the employee was physically coerced.

11:49 AM · Apr 5, 2022 · Twitter Web App

94 Retweets 25 Ouote Tweets 205 Likes



Not only outages, transit in Ukraine was also affected

HOME > NEWS > TELECOMS & 5G

Vodafone suspends partnership with Russian telco MTS

Russia's invasion of Ukraine convinces Vodafone to drop MTS

March 03, 2022 By: Sebastian Moss 🔘 Comment



Vodafone has suspended its 14-year partnership with Russian telecoms company MTS due to the invasion of Ukraine.

The move comes after US stock exchanges <u>halted trading of MTS</u>, along with other Russian firms, and the <u>West levies sanctions</u> against Russia.

"Vodafone confirms that it has suspended its partner market agreement with MTS," the



Internet transit for AS21497 (Vodafone Ukraine)



Vodafone Ukraine (AS21497) lost transit from MTS (AS8359) on February 28, 2022.

https://www.datacenterdynamics.com/en/news/vodafone-suspends-partnership-with-russian-telco-mts/

Not only outages, transit in Ukraine was also affected

Internet transit for AS3326 (Datagroup)



Loss of transit from AS20764 (Rascom, Russia)

Internet transit for AS25229 (Volia)



Transit instability during initial phase of conflict.

- Initial months of invasion (Feb-Mar 2022)
 - Impacts in Ukraine
 - Impacts in Russia
- Conflict shifts east and south (Summer 2022)
- Ukraine counteroffensive, Russian retaliation



Ukraine calls for help on the Internet

26 Feb: Ukraine's Minister for Digital Transformation called for the formation of a volunteer "IT army" of hackers to target 31 important Russian websites.



https://twitter.com/FedorovMykhailo/status/1497642156076511233

IT ARMY of Ukraine

@ 68.5K 10:12 AM For all IT specialists from other countries, we translated

Task #1 We encourage you to use any vectors of cyber and DDoS attacks on these resources.

Business corporations

tasks in English.

Gazprom - https://www.gazprom.ru/ Lukoil - https://lukoil.ru Magnet - https://magnit.ru/ Norilsk Nickel - https://www.nornickel.com/ Surgetneftegas - https://www.surgutneftegas.ru/ Tatneft - https://www.tatneft.ru/ Evraz - https://www.evraz.com/ru/ NLMK - https://nlmk.com/ Sibur Holing - https://www.sibur.ru/ Severstal - https://www.severstal.com/ Metalloinvest - https://www.metalloinvest.com/ NNC - https://nangs.org/ Russian Copper Company - https://rmk-group.ru/ru/ TMK - https://www.tmk-group.ru/ Yandex - https://ya.ru/ Polymetal International - https:// www.polymetalinternational.com/ru/ Uralkali - https://www.uralkali.com/ru/ Eurosibenergo - https://www.eurosib.ru/ OMK - https://omk.ru/

Banks

Sberbank - https://www.sberbank.ru VTB - https://www.vtb.ru/ Gazprombank - https://www.gazprombank.ru/

The state

Public services - https://www.gosuslugi.ru/ Moscow State Services - https://www.mos.ru/uslugi/ President of the Russian Federation - http://kremlin.ru/ Government of the Russian Federation - http://

government.ru/

Ministry of Defense - https://mil.ru/ Tax - https://www.nalog.gov.ru/ Customs - https://customs.gov.ru/ Pension Fund - https://pfr.gov.ru/ Roskomnadzor - https://rkn.gov.ru/

Russian Internet become a target of DDoS attacks

- Even before Federov's call to action, RU DDoS targets included http:// kremlin.ru hosted by AS8291 (Russia State Internet Network).
- Sberbank (AS35257) and Alfabank (AS15632) were targeted in consecutive DDoS attacks on 24 Feb.



https://twitter.com/DougMadory/status/1496961857638309893

Russian Internet become a target of DDoS attacks

Rostelecom stopped announcing the BGP routes of Russia's e-government platform (AS196747) outside the country on 26-Feb. It hosts one of the 31 sites on Ukraine's hitlist.

				lormalized Va		_	
100%	, Feb 26 - 16:45 P (#Visible /24s): 100	1%		Toggle Pai	n/Zoom 🏢	2004	Reset Zoo
80%							
4.02							
00%							
40%							
40%							

Test Timestamp: 2022-02-24 23:51 UTC

e				
	Agent A	Status Code	Response Size	
n	Amsterdam, Netherlands IBM Cloud (SoftLayer),US (36351)	418		
	Ashburn, VA, United States Amazon,US (14618)	418		
	Chicago, IL, United States Microsoft,US (8075)	418		
	EXOSCALE,CH (61098)	418		
	C London, United Kingdom Akamai (Linode),US (63949)	418		
	Coogle, US (15169)	418		
	Contraction Moscow, Russia Tencent,CN (132203)	200	808 KB	
	Colo, Norway Microsoft,US (8075)	418		
	Amazon,US (16509)	418		
	Sydney, Australia Alibaba,CN (45102)	418		
	Taipei, Taiwan Google,US (15169)	418		
Mil.ru	was restricted to Rus	sian IPs	s only.	
Outsid	lers received the 418	"I'm a t	eapot" e	erro
	 Akamai (Linode), US (63949) 			
used t	o let users know they	are be	ing bloc	кеа

Ukraine request that Russia be disconnected

- 28 Feb: Ukraine's Minister for Digital Transformation requests Internet orgs work to disconnect the Russia.
- For ICANN
 - Shut down DNS root servers in Russia
 - Revoke Russian TLDs (.ru, .pф, .su)
- For RIPE
 - Withdraw the right to use all IPv4 and IPv6 addresses by all Russian members.
 - Block DNS root servers that it is operating.
- ICANN and RIPE refuse.



MIHICTEPCTBOMINISTRYЦИФРОВОЇ ТРАНСФОРМАЦІЇOF DIGITAL TRANSFORMATION OFУКРАЇНИUKRAINEвул. Ділова, 24, м. Київ, 03150
тел. 207-17-3024, Dilova str., Kyiv, 03150, Ukraine
Tel: +38 (044) 207-13-30Е-mail: hello@thedigital.gov.ua
Web: http://www.thedigital.gov.ua
Koд згідно 3 €ДРПОУ 43220851E-mail: hello@thedigital.gov.ua
Web: http://www.thedigital.gov.ua

№ <u>1/03 - 1-1948 від 28.02 2022</u>р.

Goran Marby President and Chief Executive Officer, ICANN

Dear Mr. President and Chief Executive Officer,

I am sending you this letter on behalf of the People of Ukraine to ask you to address an urgent need to introduce strict sanctions against the Russian Federation in the field of DNS regulation in response to its acts of aggression towards Ukraine and its citizens.

Ukraine request led to a controversial idea...

The Internet Sanctions Project

Use Internet governance model to facilitate discussion of resources should be blocked to affect sanctions against violators of international and human rights law.

- Produce real-time BGP and RPZ data feeds of network resources (IP addresses, ASNs, and domain names) associated with sanctioned entities.
- Block without impinging upon civilians' access to information and communications.
- Neither pro-sanction nor anti-sanction but it exists to facilitate public/private-sector coordination while ensuring that the human rights of civilians are protected.

Russia begins blocking international news, social media

- Blocking of independent Russian news & foreign news sites
- Centralized throttling of Twitter
- Decentralized censorship using multiple techniques.

See OONI's excellent report: https://ooni.org/post/2022-russia-blocks-amid-ruua-conflict/

Blocking of news media websites in Russia (February - March 2022)

| Value | 1,0
0.0 | 100%
 | 100% | 100% | 100% | 100%

 | 100% | 100% | 100% | 100% | 100% | 100%
 | 100% | 100%
 | 100% | 100%
 | 100% | 100% | 91%
 | 74% |
|-------|---
--
---|---|--|--
--
--|--|--|--|---|--
--
--|--
--
--
--|--|--
--|--|
| Value | 1,0 | 100%
 | 100% | 100% | 100% | 100%

 | 100% | 100% | 100% | 100% | 100% | 100%
 | 100% | 100%
 | 100% | 99%
 | 100% | 100% | 91%
 | 65% |
| | 1,0 | 98%
 | 100% | 99% | 98% | 99%

 | 100% | 98% | 99% | 100% | 98% | 99%
 | 100% | 100%
 | 98% | 100%
 | 99% | 99% | 98%
 | <mark>57%</mark>
43% |
| | 1,0 | 99%
 | 100% | 97% | 97% | 98%

 | 100% | 97% | 98% | 100% | 99% | 96%
 | 97% | 98%
 | 90% | 87%
 | 76% | 77% | 87%
 | |
| | 1,0 | 99%
 | 99% | 98% | 98% | 97%

 | 99% | 97% | 98% | 100% | 100% | 99%
 | 100% | 100%
 | 87% | 74%
 | 70% | 78% | 81%
 | 84% |
| | 1,0 | 99%
 | 99% | 96% | 98% | 98%

 | 97% | 98% | 98% | 100% | 99% | 99%
 | 100% | 100%
 | 100% | 99%
 | 100% | 99% | 98%
 | <mark>48%</mark>
52% |
| | 1,0 | 98%
 | 99% | 97% | 97% | 98%

 | 100% | 98% | 98% | 100% | 98% | 97%
 | 100% | 100%
 | 100% | 99%
 | 99% | 100% | 98%
 | 72% |
| | 1,0 | 98%
 | 100% | 97% | 95% | 97%

 | 98% | 97% | 97% | 96% | 100% | 98%
 | 99% | 99%
 | 100% | 99%
 | 99% | 100% | 87%
 | 71% |
| | 1,0 | 99%
 | 98% | 97% | 98% | 99%

 | 100% | 95% | 95% | 96% | 100% | 96%
 | 100% | 99%
 | 100% | 98%
 | 100% | 99% | 86%
 | 67% |
| | 1,0 | 98%
 | 100% | 98% | 98% | 99%

 | 98% | 98% | 97% | 100% | 98% | 97%
 | 100% | 100%
 | 99% | 100%
 | 99% | 99% | 92%
 | 60% |
| | 1,0 | 98%
 | 98% | 98% | 96% | 98%

 | 100% | 98% | 97% | 100% | 96% | 95%
 | 100% | 100%
 | 100% | 100%
 | 99% | 97% | 91%
 | 67% |
| | 1,0 | 100%
 | 100% | 100% | 100% | 100%

 | 100% | 100% | 100% | 100% | 100% | 99%
 | 99% | 98%
 | 99% | 99%
 | 75% | 86% | 69%
 | 80% |
| | 1,0 | 99%
 | 100% | 98% | 96% | 98%

 | 100% | 98% | 98% | 99% | 100% | 99%
 | 100% | 100%
 | 100% | 100%
 | 100% | 97% | 90%
 | 84% |
| | 1,0 |
 | | | |

 | | | | | |
 | |
 | |
 | | |
 | 86% |
| | 1,0 | 100%
 | 100% | 100% | 100% | 100%

 | 100% | 100% | 100% | 100% | 100% | 100%
 | 100% | 57%
 | 92% | 94%
 | 65% | 100% | 88%
 | 71% |
| | |
 | | | |

 | | | | | |
 | |
 | |
 | | |
 | |
| Value | 1,0
0,0 | 99%
 | 100% | 98% | 98% | 98%

 | 100% | 98% | 96% | 100% | 100% | 98%
 | 100% | 100%
 | 100% | 100%
 | 100% | 97% | 90%
 | 92% |
| | Value | Agine Agine <th< td=""><td>International system International system International system antipy 0,0 100% 98% antipy 0,0 98% 98% antipy 0,0 99% 99% antipy 0,0 98% 98% antipy 0,0 98% 98%</td><td>I)IPA 0.0 100% 100% anilex 0.0 </td><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>IDDE IDDE <th< td=""><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>TOX 100%</td><td>TYDA 100% <th< td=""><td>Interview 100%<</td><td>100% <th< td=""><td>100% <th< td=""><td>100% <th< td=""><td>TOP 100%</td><td>TOP 100%
 100% 100%</td><td>TODA 100% <th< td=""><td>TODA 100%</td></th<></td></th<></td></th<></td></th<></td></th<></td></th<></td></th<> | International system International system International system antipy 0,0 100% 98% antipy 0,0 98% 98% antipy 0,0 99% 99% antipy 0,0 98% 98% antipy 0,0 98% 98% | I)IPA 0.0 100% 100% anilex 0.0 | $\begin{array}{c c c c c c c c c c c c c c c c c c c $ | IDDE IDDE <th< td=""><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>TOX 100%</td><td>TYDA 100% <th< td=""><td>Interview 100%<</td><td>100% <th< td=""><td>100% <th< td=""><td>100% 100%
100% <th< td=""><td>TOP 100%</td><td>TOP 100%</td><td>TODA 100% <th< td=""><td>TODA 100%</td></th<></td></th<></td></th<></td></th<></td></th<></td></th<> | $\begin{array}{c c c c c c c c c c c c c c c c c c c $ | $\begin{array}{c c c c c c c c c c c c c c c c c c c $ | $\begin{array}{c c c c c c c c c c c c c c c c c c c $ | $ \begin{array}{c c c c c c c c c c c c c c c c c c c $ | TOX 100% | TYDA 100% <th< td=""><td>Interview 100%<</td><td>100% 100%
 100% <th< td=""><td>100% <th< td=""><td>100% <th< td=""><td>TOP 100%</td><td>TOP 100%</td><td>TODA 100% <th< td=""><td>TODA 100%</td></th<></td></th<></td></th<></td></th<></td></th<> | Interview 100%< | 100% 100% <th< td=""><td>100% 100% 100% 100%
100% <th< td=""><td>100% <th< td=""><td>TOP 100%</td><td>TOP 100%</td><td>TODA 100% <th< td=""><td>TODA 100%</td></th<></td></th<></td></th<></td></th<> | 100% 100% <th< td=""><td>100% <th< td=""><td>TOP 100%
 100% 100%</td><td>TOP 100%</td><td>TODA 100% <th< td=""><td>TODA 100%</td></th<></td></th<></td></th<> | 100% 100% <th< td=""><td>TOP 100%</td><td>TOP 100%</td><td>TODA 100% <th< td=""><td>TODA 100%
 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100% 100%</td></th<></td></th<> | TOP 100% | TOP 100% | TODA 100% <th< td=""><td>TODA 100%</td></th<> | TODA 100% |

Russia begins blocking international news, social media

- Inadvertent global BGP hijack of Twitter on 28 March.
- From 12:05-12:50 UTC, Russian telecom RTComm (AS8342) hijacked 104.244.42.0/24 belonging to Twitter.
- Same prefix was hijacked during the military coup in Myanmar last year, however...
- It fared much better this time due to an RPKI ROA which enabled other networks to simply drop the erroneous Russian announcement.

OP MONITOR										
	ck of Twit	ter							Time Range (UT Mar 28 12:00 to	C) 13:00
2.00	12:06	12:10	12:15	12:20	12:25 12:30 12:35	12:40	12.45	12:50	12:55	13
					2022-03-28 UTC (1 minute increments)					
Show Reacha	ibility / Visibility	~ 104.244.42.0/5	24 ~						- Hø	e Timeline
ercentage of 10% 0% 15 15 15 10	Kentik's BGP vantag	12:10	12:16	By Origin ASN: N • Twitter, US (134 • RTCerrm, RU (1 12/20	4# 28, 12.2.7 154: 98.3%	12-40	12,45	12:50	12:55	18
Show AS Path	h Visualization	×						Hide ASN	Name 📄 Hide P	withs Gray
	sualization h showing all key AS (paths associated w	ith the monitored prefix	es. Hover over any AS ති AS1103 SURFNet (N etwo	node or link to see more information	ති AS8342 RTCorm,RU				4.42.02

Cogent and Lumen curtail operations in Russia

• 3 March 2022: Cogent notified customers in Russia that service was being

discontinued: In light of the unwarranted and unprovoked invasion of Ukraine, Cogent is terminating all of your services effective at 5 PM GMT on March 4, 2022. The economic sanctions put in place as a result of the invasion and the increasingly uncertain security situation make it impossible for Cogent to continue to provide you with service.

- Transtelecom (TTK) and VEON were among a handful of RU networks that were disconnected from Cogent.
 - VEON was re-connected the following week.
 - Other RU customers (including Rostelecom) were never disconnected.
- Lumen issued similar statement, no practical effect.
- RU continues tothe well connected to global connects from russia/ Internet.



- Initial months of invasion (Feb-Mar 2022)
 - Impacts in Ukraine
 - Impacts in Russia
- Conflict shifts east and south (Summer 2022)
- Ukraine counteroffensive, Russian retaliation



Eastern Ukraine: Donbas region (Donetsk and Luhansk)

- Russian-held areas in eastern Donbas
 - Have used RU transit almost exclusively since 2014
 - BGP/DNS hijacks of 2018 misdirected to Luhansk



- Internet partition along UA/RU lines
 - RTT latencies between areas can be >100ms
 - Approaching RTT across Pacific Ocean



Southern Ukraine: switchover to Russian transit

- March 2014: Russia annexed Crimean Peninsula from Ukraine
- Crimea Internet re-routed via Miranda Media (AS201776) in July 2014.
- Kherson Internet re-routed via AS201776 in June 2022.

How Russia Took Over Ukraine's Internet in Occupied Territories (New York Times, Aug 9)

Crimea.



All Kherson ISPs switch to Russian transit beginning June 1, 2022.

https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html https://www.kentik.com/blog/rerouting-of-kherson-follows-familiar-gameplan/

Kherson's internet

- Initial months of invasion (Feb-Mar 2022)
 - Impacts in Ukraine
 - Impacts in Russia
- Conflict shifts east and south (Summer 2022)
- Ukraine counteroffensive, Russian retaliation



Latest: Kerch bridge damaged in attack (Oct-8)







Romain Fontugne @romain_fontugne

It looks like the Kerch bridge explosion had a significant impact on UMLC routing (AS48084, an Internet provider to Crimea). Most of UMLC downstream networks are being rerouted to Miranda Media (AS201776)

...

ihr.iijlab.net/ihr/en-us/netw...



https://twitter.com/romain_fontugne/status/1578918563121090560

Russia retaliates with attacks on numerous Ukrainian cities



Internet outages due to power outages as electrical infrastructure was among targets.

- Initial months of invasion (Feb-Mar 2022)
 - Impacts in Ukraine
 - Impacts in Russia
- Conflict shifts east and south (Summer 2022)
- Ukraine counteroffensive, Russian retaliation
- Conclusion



Ukraine stayed online



≡ Menu □ Feedback Q A -人 CORE > Data Explorer H Full width G Refresh 🔻 📽 Share Actions 🔻 🖻 Query Top Dest AS Number by Average bits/s Internet traffic to Ukraine Last 30 Days 📑 163 of 163 data sources 🍸 1 Filter Expected peak traffic levels Russian invasion 02/16 02/18 02/20 02/22 02/24 02/26 02/28 03/2 03/4 03/6 03/8 03/10 03/12 03/14 2022-02-15 to 2022-03-17 UTC (60 minute intervals) Start 🛱 2/16/2022 End 🗇 3/17/2022 **Google Transparency Report** - Product traffic 80 70 Russian invasion 60 50 40 30 20 10 Feb 18, 2022 Feb 22, 2022 Feb 26, 2022 Mar 02, 2022 Mar 06, 2022 Mar 10 2022 Mar 14, 2022

Product Web Search

Country/Region Ukraine

https://twitter.com/DougMadory/status/1504904422077444101 https://labs.ripe.net/author/emileaben/the-resilience-of-the-internet-in-ukraine/

Ukraine stayed online

... the Ukrainian government to rally global support.

Critical for _____ ... news organizations to cover the war.

... Ukrainians to show the world what was happening.







Ukraine stayed online

due to the efforts of these heroes of the Internet

On-going war is largest in Europe since WWII

- What does this means in the Internet age?
 - DDoS attacks against high-profile targets in both Ukraine and Russia
 - ISP outages in Ukraine due to destroyed fiber lines, cyberattacks.
 - Heroic efforts to repair broken lines by Ukrainian technicians.
- Blowback effects in Russia
 - Social media and news blockage in Russia
 - Possibility of Internet-level sanctions
- Assimilation of occupied areas
 - Wholesale cutover of transit for an entire occupied city



Тримайте Україну на зв'язку

Support the Keep Ukraine Connected effort!

Doug Madory dmadory@kentik.com Twitter: @dougmadory

