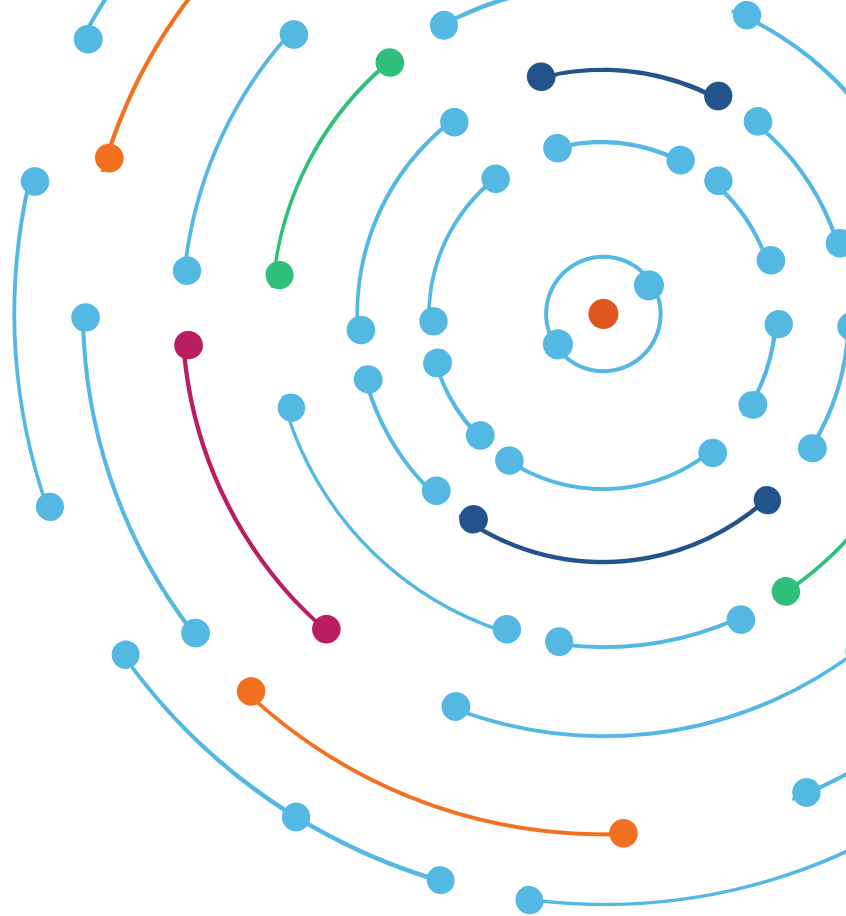


# Internet impacts due to the war in Ukraine

Doug Madory, Kentik



# Internet impacts due to the war in Ukraine

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



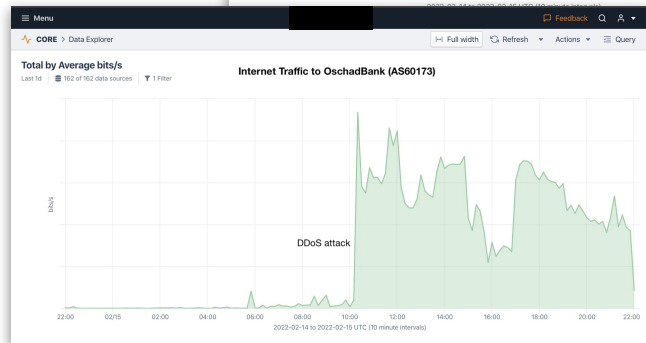
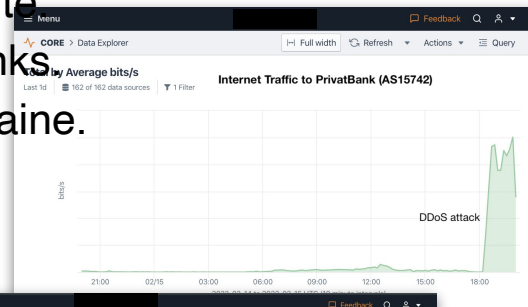
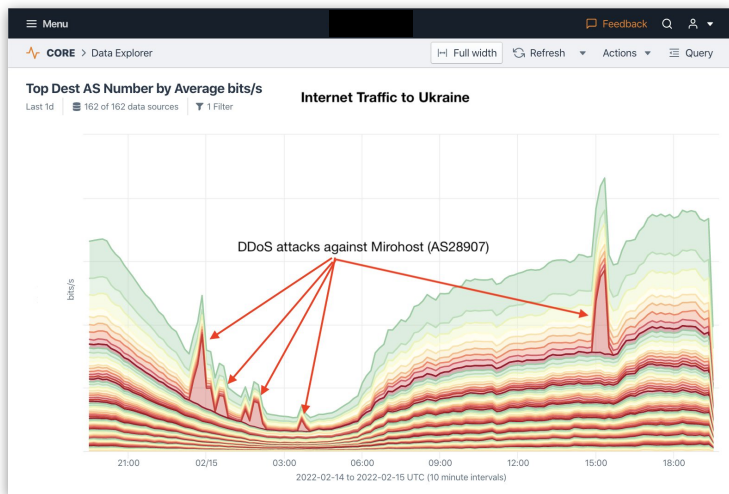
# Internet impacts due to the war in Ukraine

- 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 banks
  - Oschadbank (AS60173), state savings bank of Ukraine.

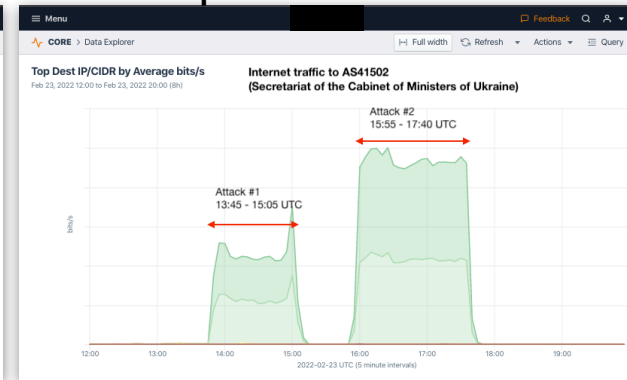
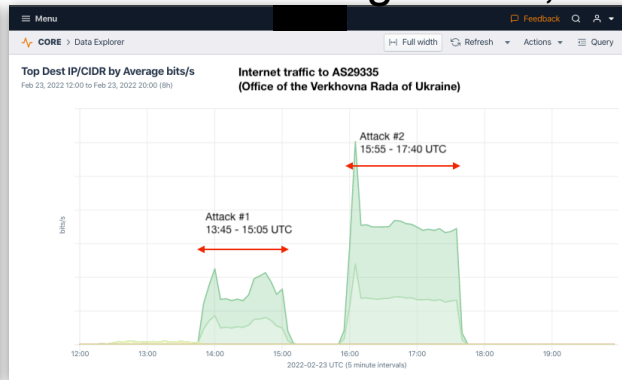
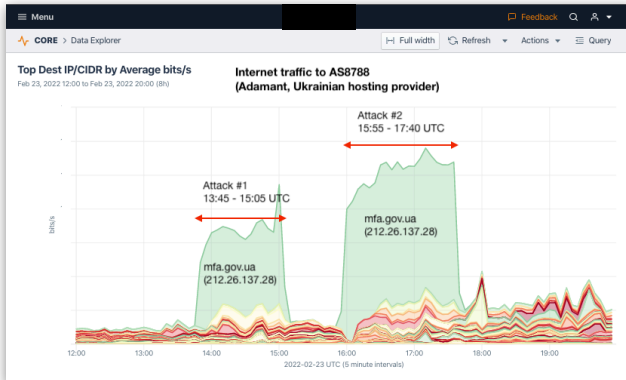


<https://twitter.com/DougMadory/status/1493680334965297159>



# 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.

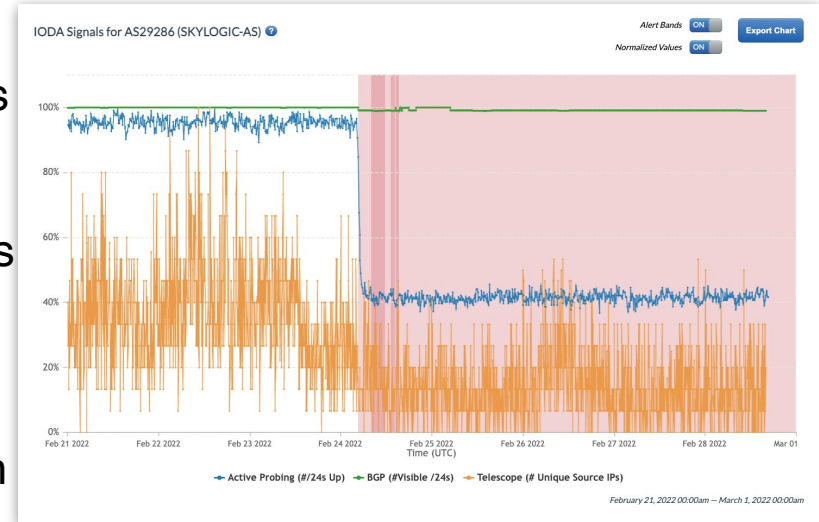


Russia invades Ukraine on early on 24 February



# 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

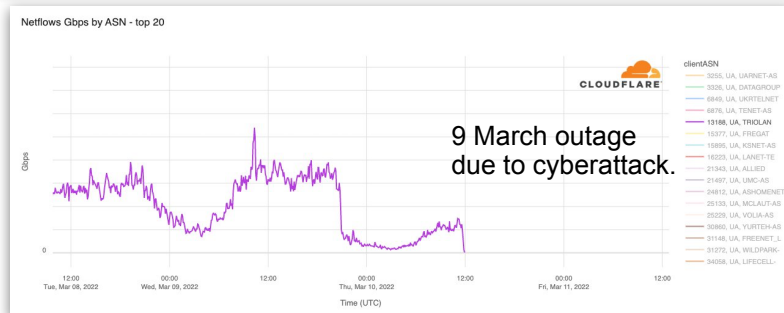
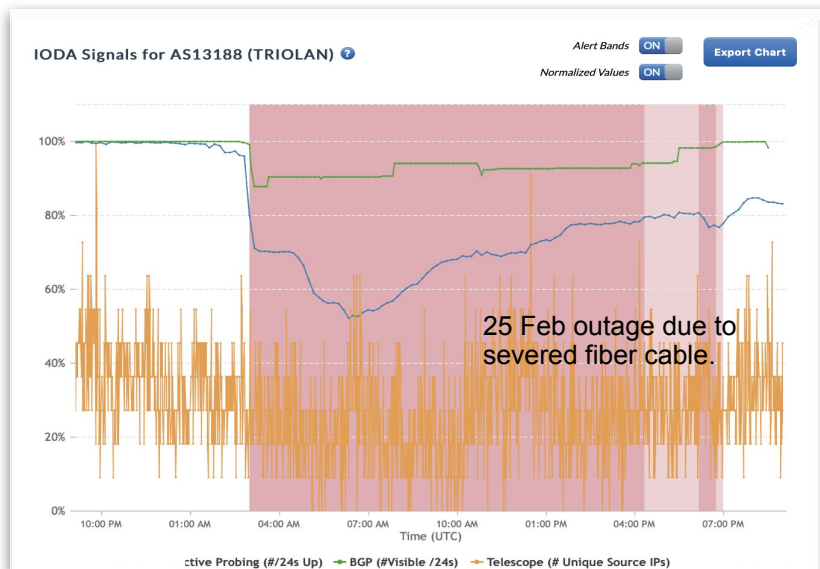
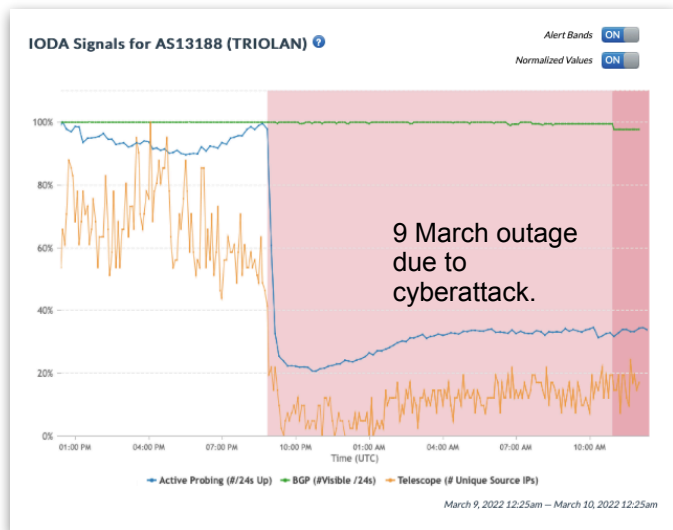


<https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/>  
[https://twitter.com/gatech\\_ioda/status/1498349622808522756](https://twitter.com/gatech_ioda/status/1498349622808522756)

# 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.

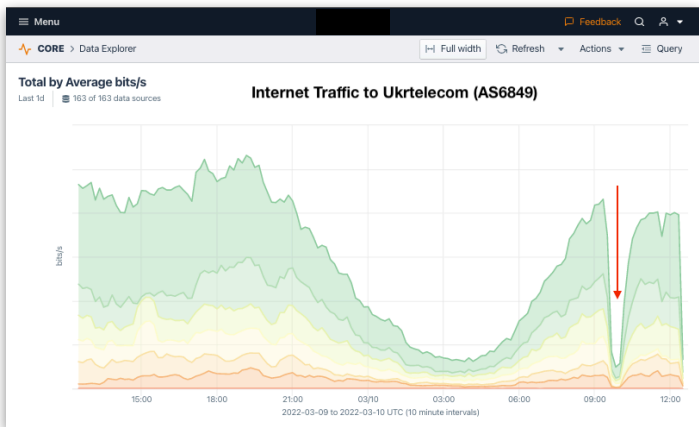
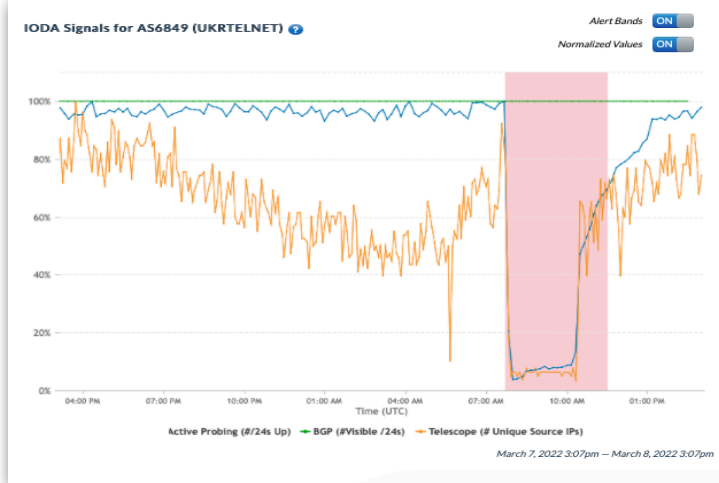
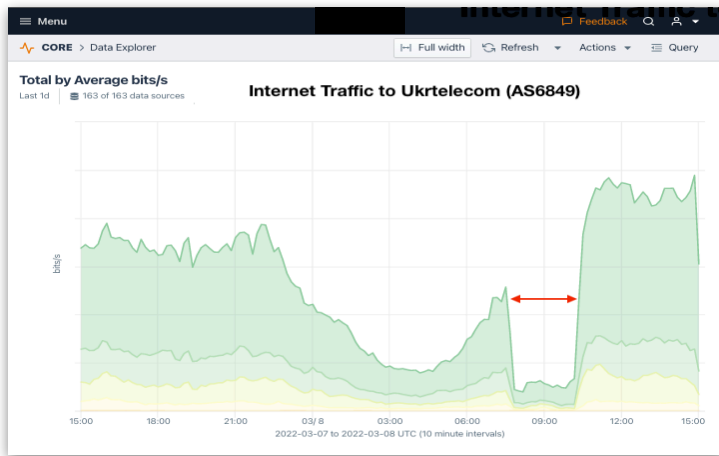




# Outages in Ukraine following the invasion

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.



Outages in Ukraine following the invasion

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

Few details about the attack emerged...

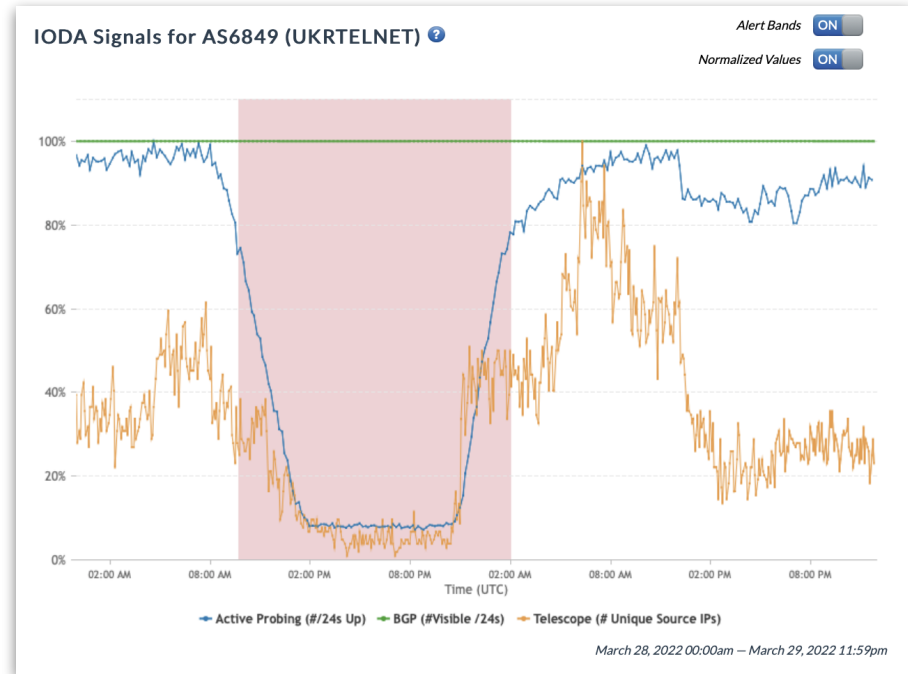


**Kevin Collier** ✓  
@kevincollier

In a Zoom presser earlier today, UKR Telecom CIO Kirill Goncharuk said the hack on his ISP started with compromised credentials from an employee in a territory Russia recently occupied. Declined to address the potential implication that the employee was physically coerced.

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

94 Retweets 25 Quote 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](#)



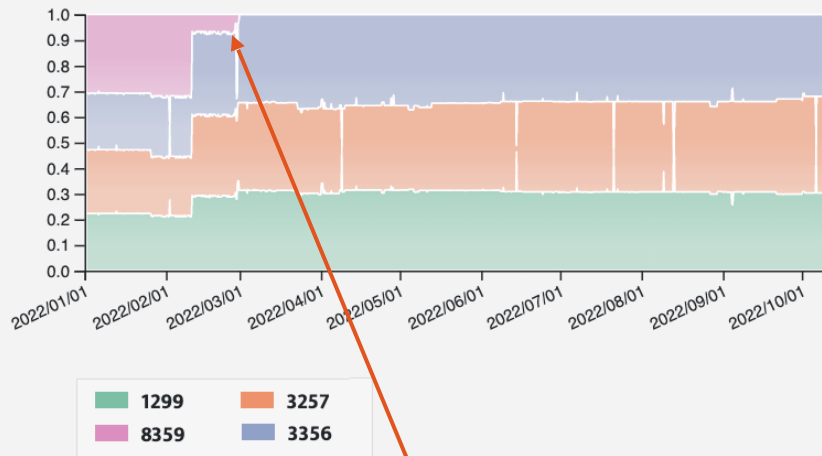
Vodafone has suspended its 14-year partnership with Russian telecoms company MTS due to the invasion of Ukraine.

The move comes after US stock exchanges [halted trading of MTS](#), along with other Russian firms, and the [West levies sanctions](#) against Russia.

"Vodafone confirms that it has suspended its partner market agreement with MTS," the company said in a short statement.



Internet transit for AS21497 (Vodafone Ukraine)

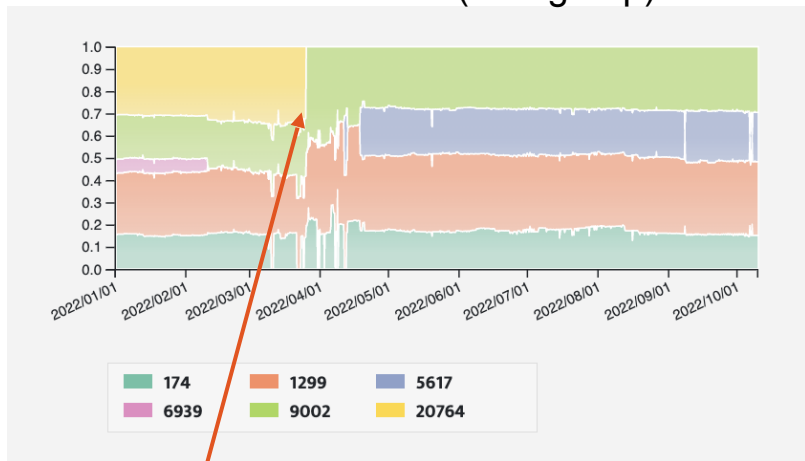


Vodafone Ukraine (AS21497) lost transit from MTS (AS8359) on February 28, 2022.

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

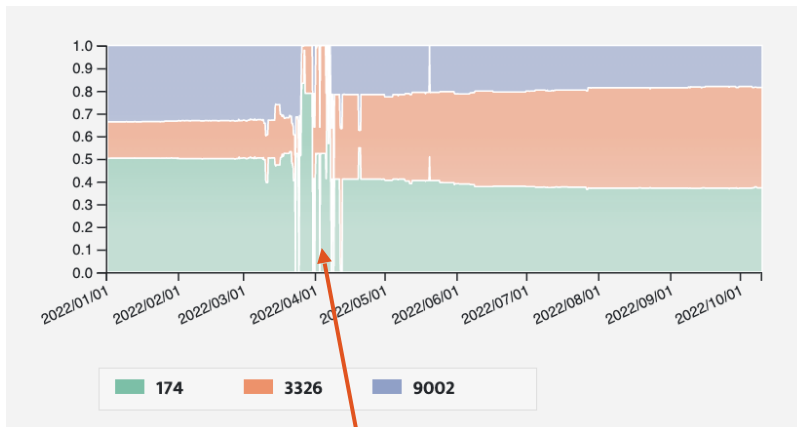
# Not only outages, transit in Ukraine was also affected

Internet transit for AS3326 (Datagroup)



Loss of transit from AS20764 (Rascom, Russia)

Internet transit for AS25229 (Volia)



Transit instability during initial phase of conflict.



# Internet impacts due to the war in Ukraine

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

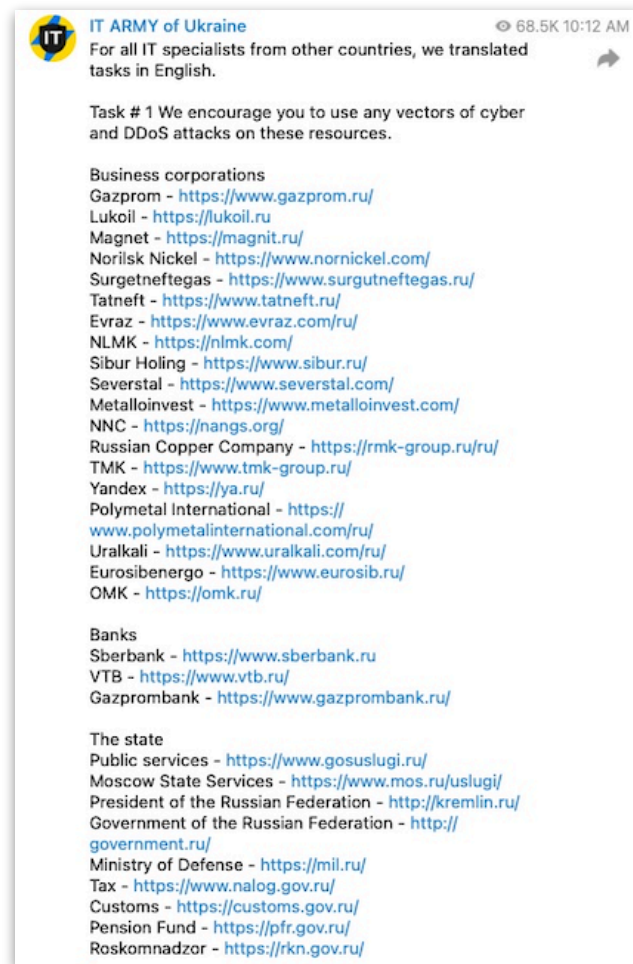


# Ukraine calls for help on the Internet

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.



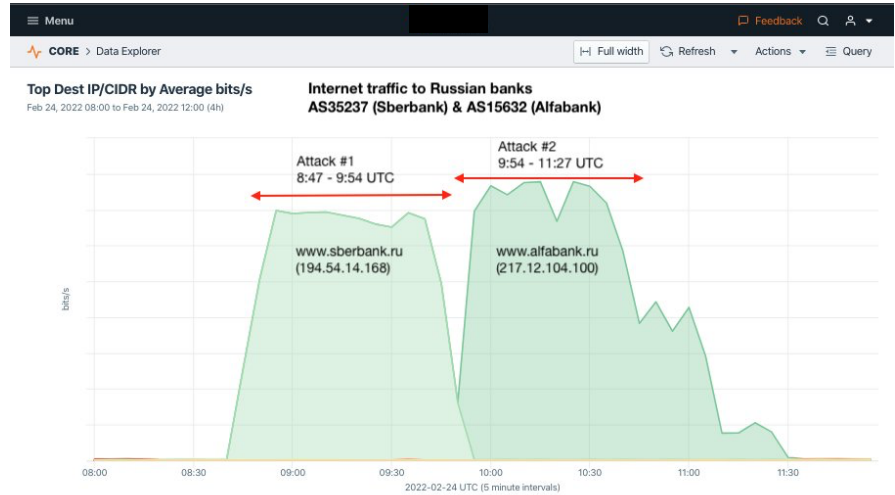
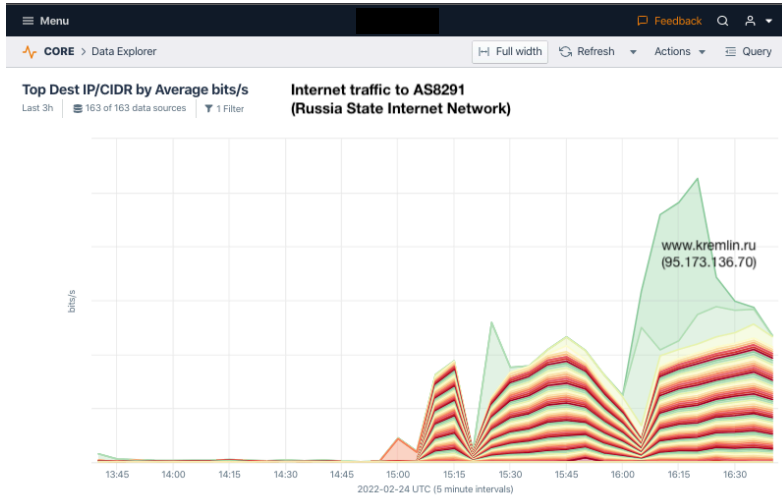
He called it world cyberwar.



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

# 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.



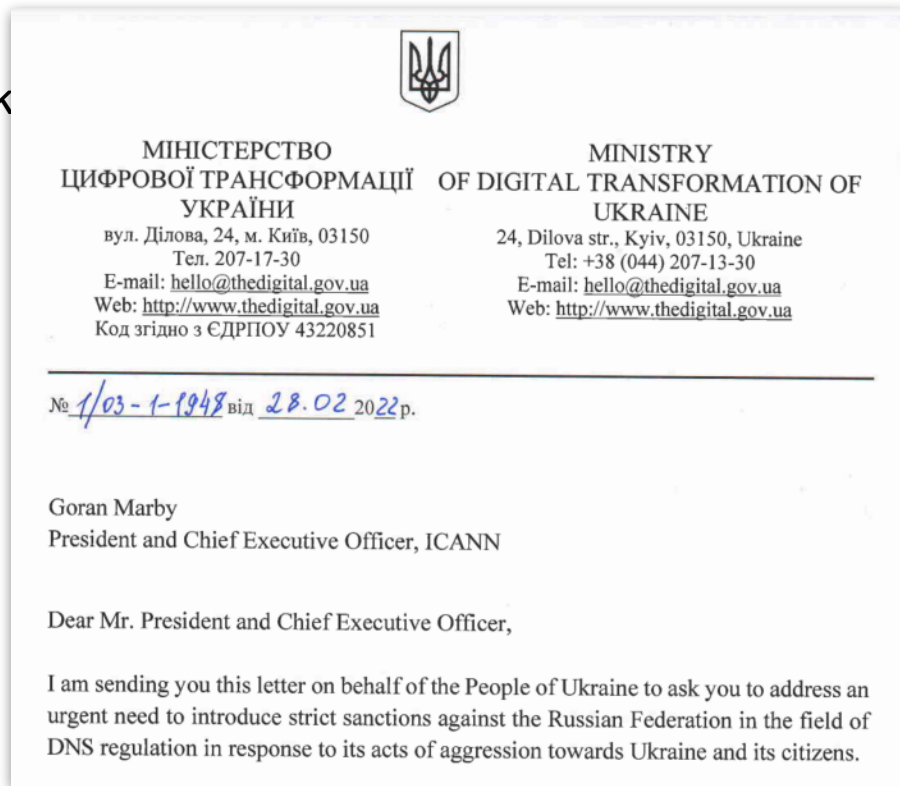
Test Timestamp: 2022-02-24 23:51 UTC

Agent ^	Status Code	Response Size
Amsterdam, Netherlands IBM Cloud (SoftLayer),US (36351)	418	---
Ashburn, VA, United States Amazon,US (14618)	418	---
Chicago, IL, United States Microsoft,US (8075)	418	---
Frankfurt, Germany EXOSCALE,CH (61098)	418	---
London, United Kingdom Akamai (Linode),US (63949)	418	---
Los Angeles, CA, United States Google,US (15169)	418	---
Moscow, Russia Tencent,CN (132203)	200	808 KB
Oslo, Norway Microsoft,US (8075)	418	---
Singapore Amazon,US (16509)	418	---
Sydney, Australia Alibaba,CN (45102)	418	---
Taipei, Taiwan Google,US (15169)	418	---
Tokyo, Japan IBM Cloud (SoftLayer),US (36351)	418	---
Wroclaw, Poland Akamai (Linode),US (63949)	418	---

Mil.ru was restricted to Russian IPs only.  
Outsiders received the 418 "I'm a teapot" error  
used to let users know they are being blocked.

# 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, .рф, .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.



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.

[https://wiki.sanctions.net/index.php/Welcome\\_to\\_the\\_Internet\\_Sanctions\\_Project](https://wiki.sanctions.net/index.php/Welcome_to_the_Internet_Sanctions_Project)

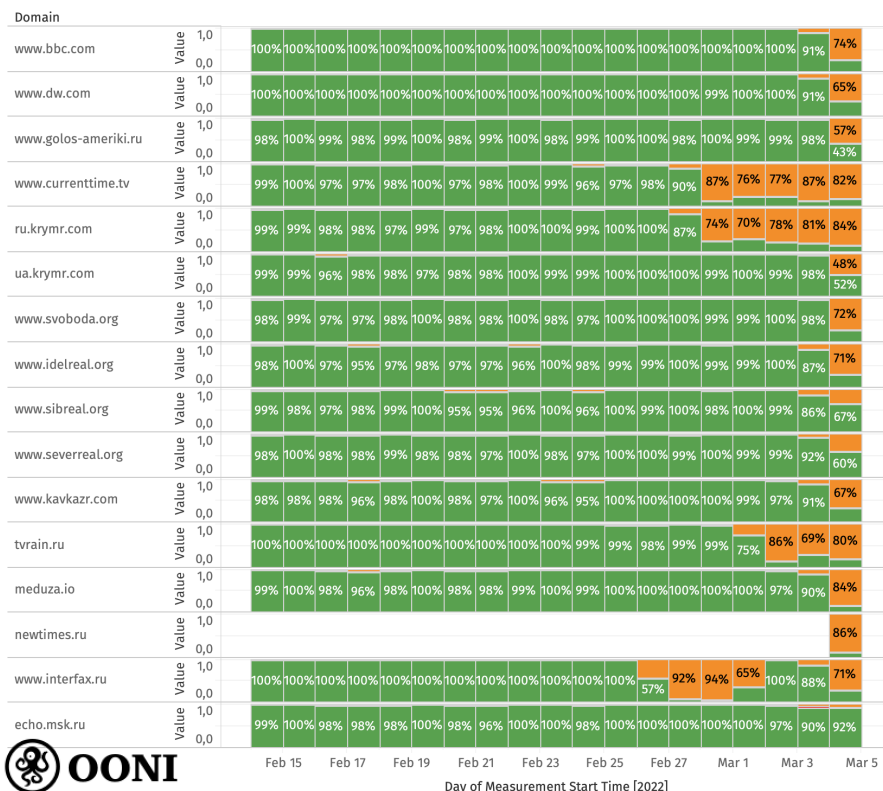
# Russia begins blocking international news, social media

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

See OONI's excellent report:

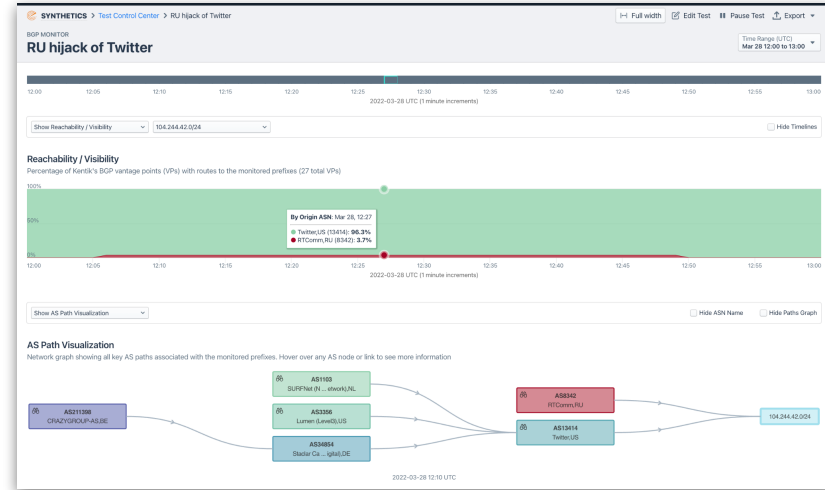
<https://ooni.org/post/2022-russia-blocks-amid-ru-ua-conflict/>

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



# 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.



<https://twitter.com/DougMadory/status/1508466367112093709>

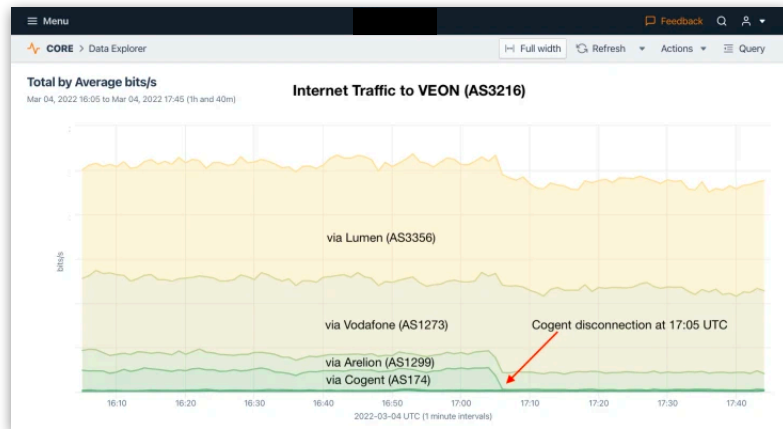


# Cogent and Lumen curtail operations in Russia

- 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 to be well connected to global Internet.



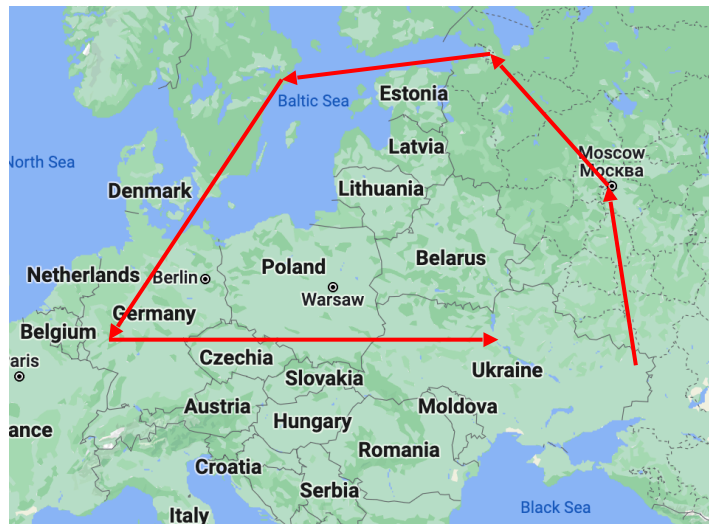
# Internet impacts due to the war in Ukraine

- 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)

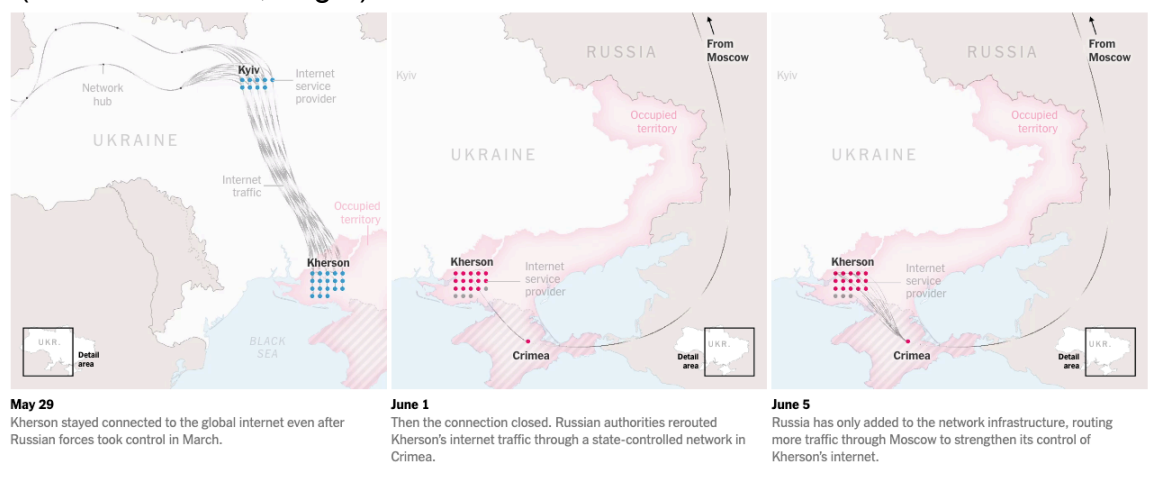
- Russian-held areas in eastern Donbas
  - Have used RU transit almost exclusively since 2014
  - BGP/DNS hijacks of 2018 misdirected to Luhansk
- Internet partition along UA/RU lines
  - RTT latencies between areas can be >100ms
  - Approaching RTT across Pacific Ocean



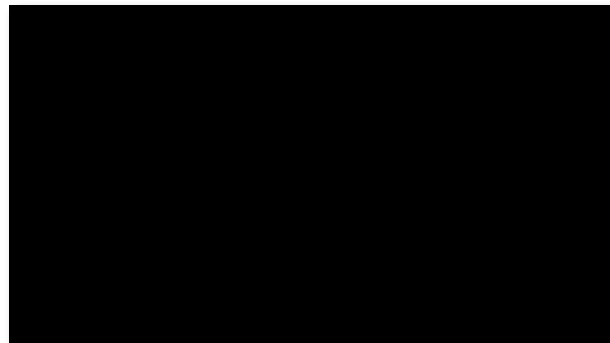
# Southern Ukraine: switchover to Russian transit

- 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)



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/>


# Internet impacts due to the war in Ukraine

- 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)

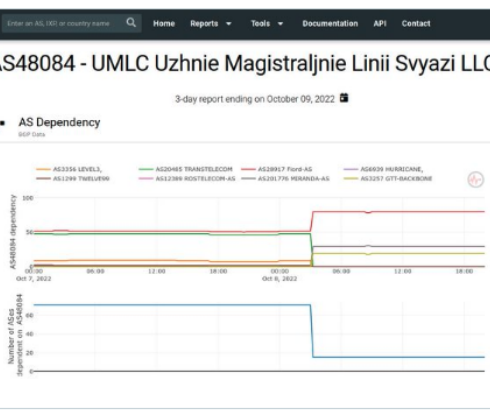




**Romain Fontugne**  
@romain\_fontugne

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...](http://ihr.iijlab.net/ihr/en-us/netw...)



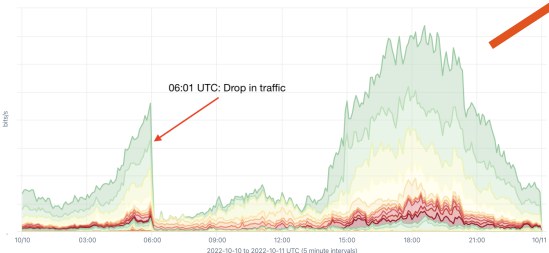
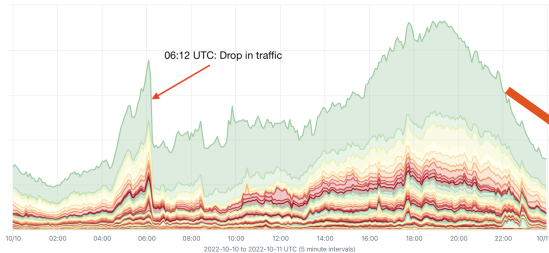
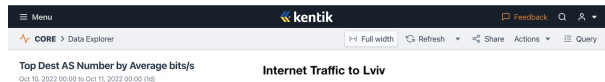
The screenshot shows the AS Dependency tool interface. The title is "AS48084 - UMLC Uzhnie Magistralnie Linii Svyazi LLC, RU". Below the title, it says "3-day report ending on October 09, 2022". The main chart is titled "AS48084 dependency" and shows the number of ASes dependent on AS48084 over time. The x-axis represents time from 00:00 on Oct 7, 2022, to 18:00 on Oct 8, 2022. The y-axis represents the "Number of ASes dependent on AS48084" from 0 to 100. A blue line shows the dependency count, which is stable at approximately 100 until 00:00 on Oct 8, 2022, where it drops sharply to approximately 20 and remains stable. A legend at the top lists several ASes: AS3356 LEVELL, AS1299 THELEVELL, AS20465 TRANSILTECOM, AS20817 FORT-AS, AS6939 HURRICANE, AS12289 KODTELECOM-AS, AS201776 MIRANDA-AS, and AS3257 GTT-BACKBONE. A small red circle highlights the sharp drop in the dependency count.

9:21 PM · Oct 8, 2022 · Twitter Web App

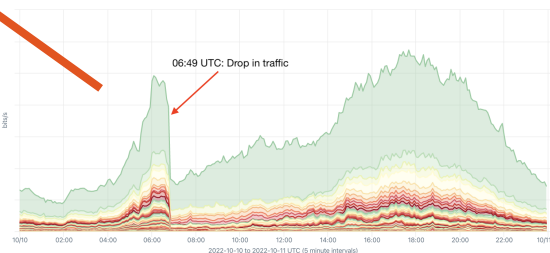
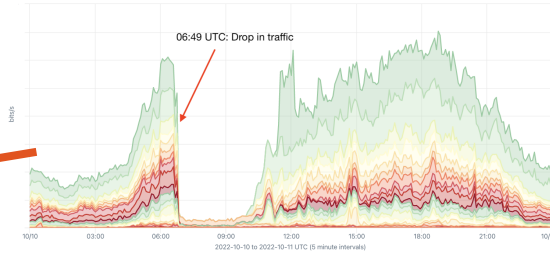
39 Retweets   6 Quote Tweets   73 Likes

[https://twitter.com/romain\\_fontugne/status/1578918563121090560](https://twitter.com/romain_fontugne/status/1578918563121090560)

# Russia retaliates with attacks on numerous Ukrainian cities



## Explosions reported near major Ukrainian cities



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

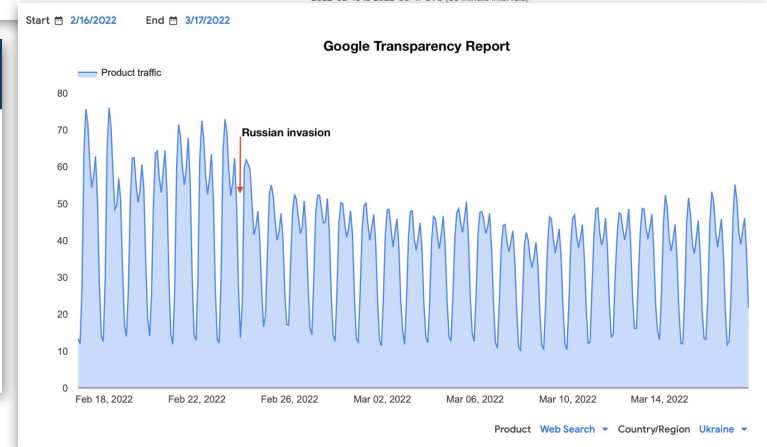
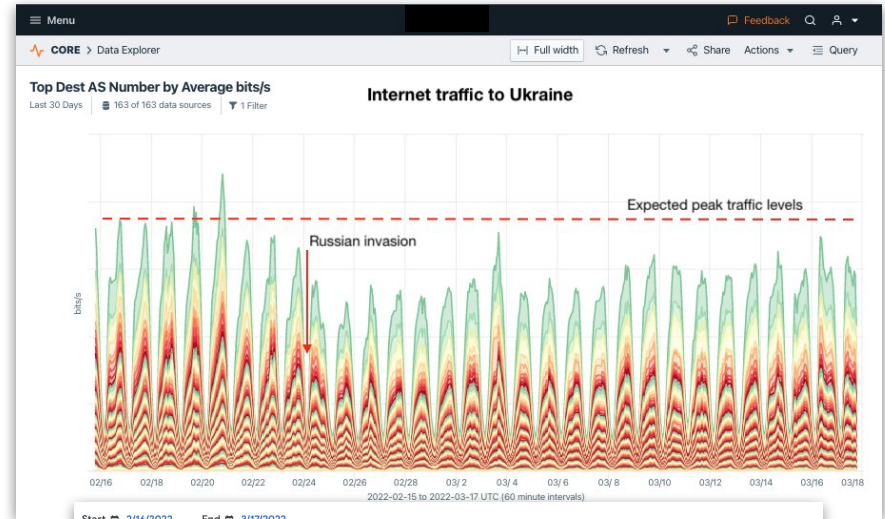
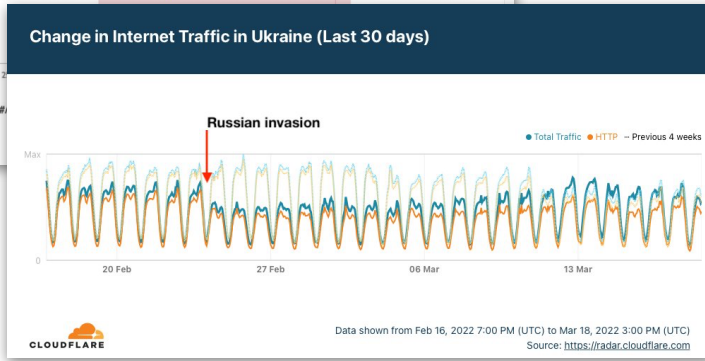
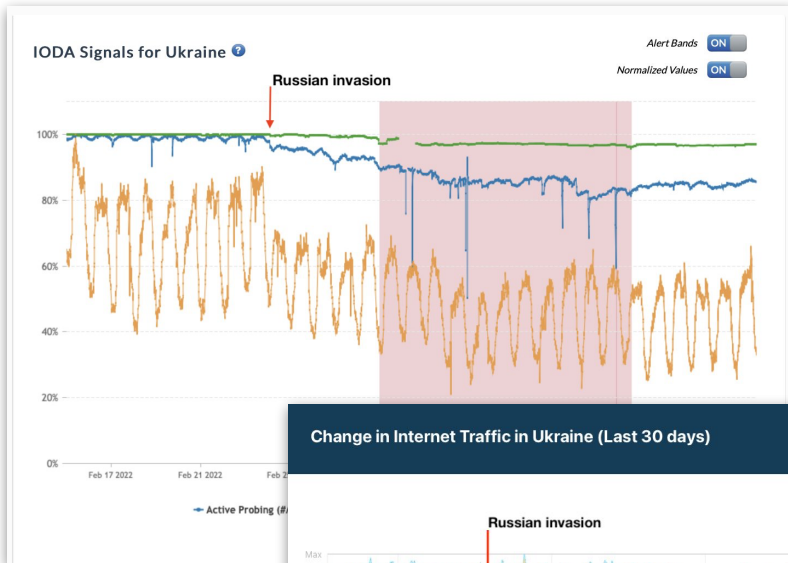
# Internet impacts due to the war in Ukraine

- 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



<https://twitter.com/DougMadory/status/1504904422077444101>

<https://labs.ripe.net/author/emileaben/the-resilience-of-the-internet-in-ukraine/>

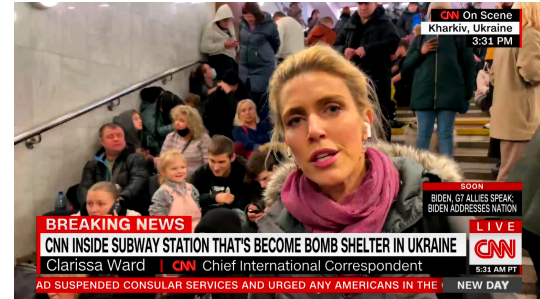
# Ukraine stayed online

...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 mean 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](mailto:dmadory@kentik.com)

Twitter: [@dougmadory](https://twitter.com/dougmadory)

