Darkbeam

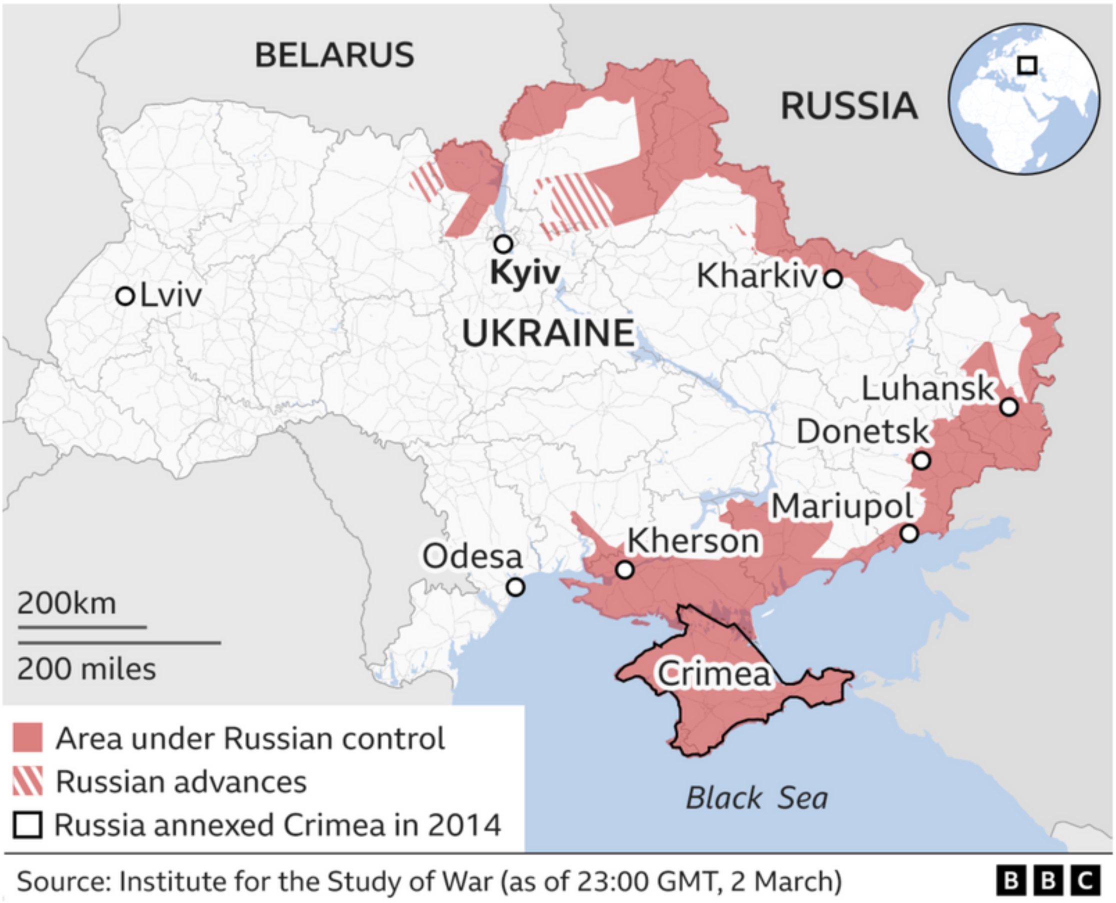
Understanding Ukraine's Infrastructural Risk

March 2022

Executive Summary

Before Ukraine, Russia invaded Georgia in 2008, highlighting the vulnerability of terrestrial internet cables in the South Caucasus. In Ukraine, internal destruction has affected internet access without causing a full national outage. Ukraine's internet infrastructure has some resilience from how it has distributed IP address space among its autonomous systems. Examining the relations between these autonomous systems identifies points of control that are responsible for 90% of a country's IP address space. Ukraine's abundance of points of control has added resilience in a way that more centralised architectures don't.

As Russian tanks roll across Ukraine, a key piece of infrastructure lies beneath them. The terrestrial internet cables that spider across Europe and connect countries internationally are vital infrastructure at a time of disinformation wars and digital reliance. Crucial internet infrastructure throughout Europe and the Caucasus could be at risk as Russian incursion continues. In order to grasp the challenges facing Russia's targets, you must examine national and international infrastructure resilience. This will dive into Russo-Georgian war, Russo-Ukrainian war, cable diplomacy, autonomous system resilience, and satellite communication safety.



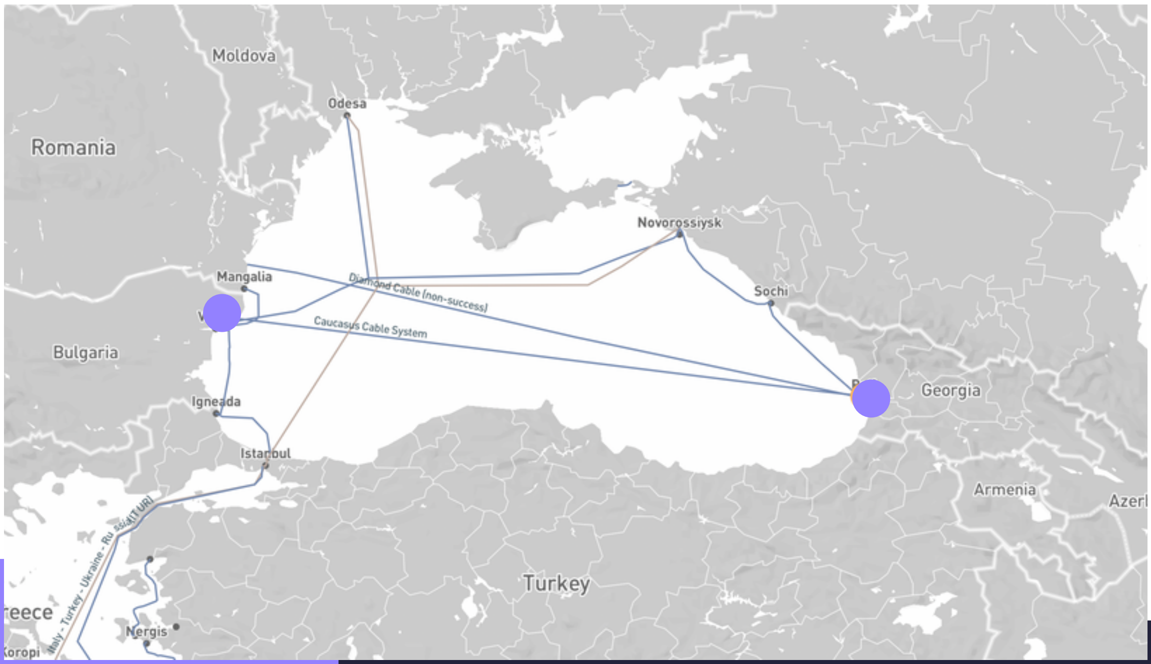
Source: Institute for the Study of War (as of 23:00 GMT, 2 March)

Before Ukraine: Georgia

In 2008, the Russo-Georgian war followed Russia’s recognition of two pro-Russian separatist states in Georgia: Abkhazia and South Ossetia. This following military action against Georgia was described by Russia as peacekeeping actions. On February 24th 2022, the Russo-Ukrainian war began following Russia’s recognition of two pro-Russia separatist states in Ukraine: Luhansk and Donetsk. The movement of Russian military forces into Ukraine was first described as a peacekeeping operation.

In the case of Georgia, the key city connecting the nation to the Caucasus cable system, Poti, was briefly occupied by Russia. Had the Caucasus Cable System connection been cut off, Russia’s ally, Armenia, would have suffered a loss of 90% of its internet connectivity. Most of Armenia’s internet traffic runs through a single trunk cable along Georgia’s East-West railway.

Instead of targeting connection to the Internet, Russia attacked individual websites of the government administration and news outlets. That said, overland cables remain a potential target for disruption and disconnection. This is especially true in the South Caucasus, where Armenia’s trunk cable through Georgia has been a prime example of why cable diplomacy doesn’t work.

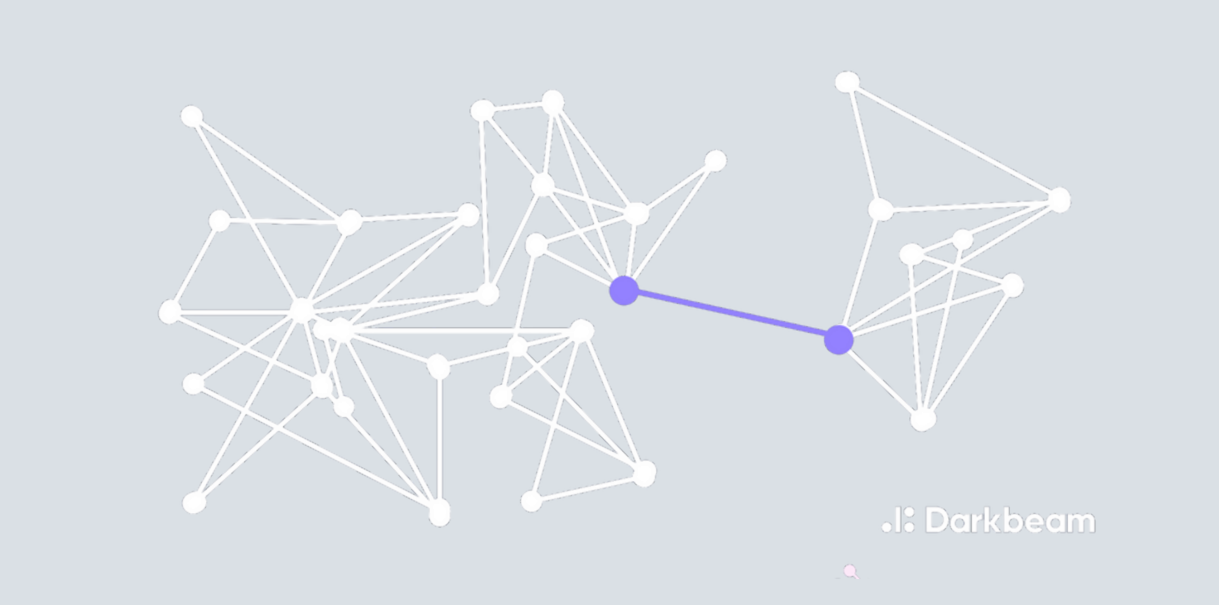


Source: https://www.infrapedia.com/app

International Cut Offs

The downstream effects of disconnection from the Caucasus Cable System have been felt by Armenia and Azerbaijan in the past. The trunk cable through Georgia is a single point of failure for most of Armenia. This has been seen in the past when an elderly Georgian woman cut the trunk cable in 2011 while scrapping for copper, leaving it once it turned out to be fibre.[i] Armenia was offline for five hours before this the cable was successfully repaired. This non-political event has been used as an example to address network political resiliency and the effects of cable diplomacy.

Cable diplomacy was used here to support an important relationship between Armenia and Georgia. Armenia needs a connection to the Caucasus Cable System and Georgia can't risk cutting off Russia's ally. This has created a system that is at odds with itself. It serves a diplomatic function so long as it never changes and traffic goes almost exclusively through Georgia. It serves an infrastructural function so long as it can change and adapt to outages using additional routing options. These cannot be achieved simultaneously and any further conflict in Georgia could collapse this agreement. This critical infrastructure is not resilient to political change and could fall apart with a single snip.



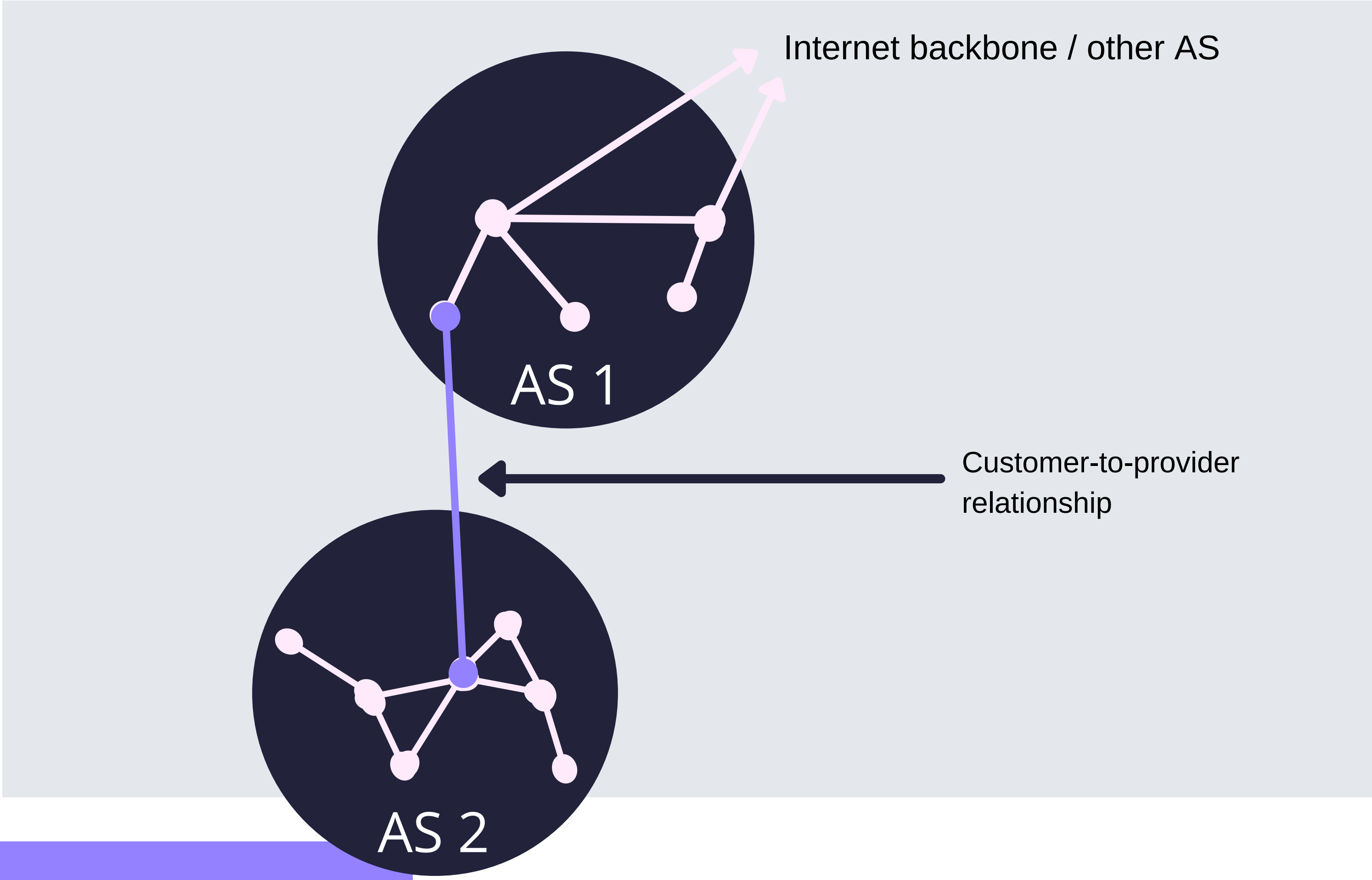
In Ukraine, however, major terrestrial cable resiliency is not the key metric being tested. Internal resilience to autonomous system outages is a key concern.

Ukraine

Intranational Network Resilience

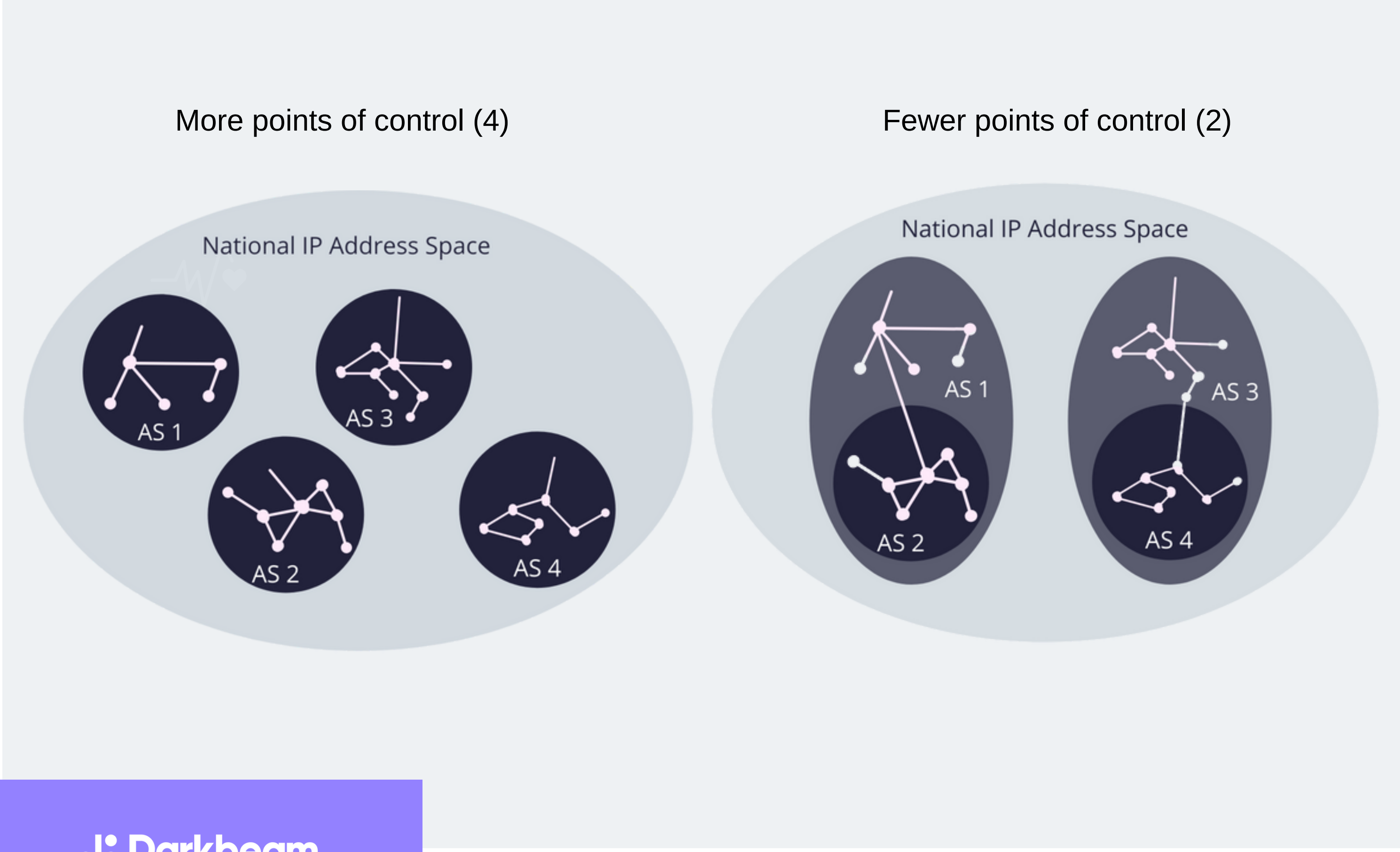
Every country's IP address space is divided among the autonomous systems (AS) within it. Resilience to destruction of autonomous system infrastructure can be defined using the relationships between the AS in a country. A strictly hierarchical set of AS could lead to choke points that can be exploited. The resilience built into Ukraine against this kind of attack can be seen by looking at the routing prefixes that announce the address space that each AS covers.

The relationships between autonomous systems can be inferred from their IP routing prefixes. For example, if one AS announces that it has an IP address range that is a subset of another AS, it can be inferred that there is a customer-to-provider relationship and that the larger AS is the target that would take more IP address space offline.


Internet backbone / other AS
AS 1
Customer-to-provider relationship
AS 2

If a country's internet space is decentralized across many AS at the same level rather than hierarchically, an attacker would need to take down far more infrastructure to have the same effect. This effectively makes the country's overall internet connectivity more resilient to the disruption or destruction of individual autonomous systems. In countries where address space is distributed among AS in a way that creates this resilience, there will still be a possibility to disrupt internet connectivity by taking enough AS offline. This raises the question: how many would it take?

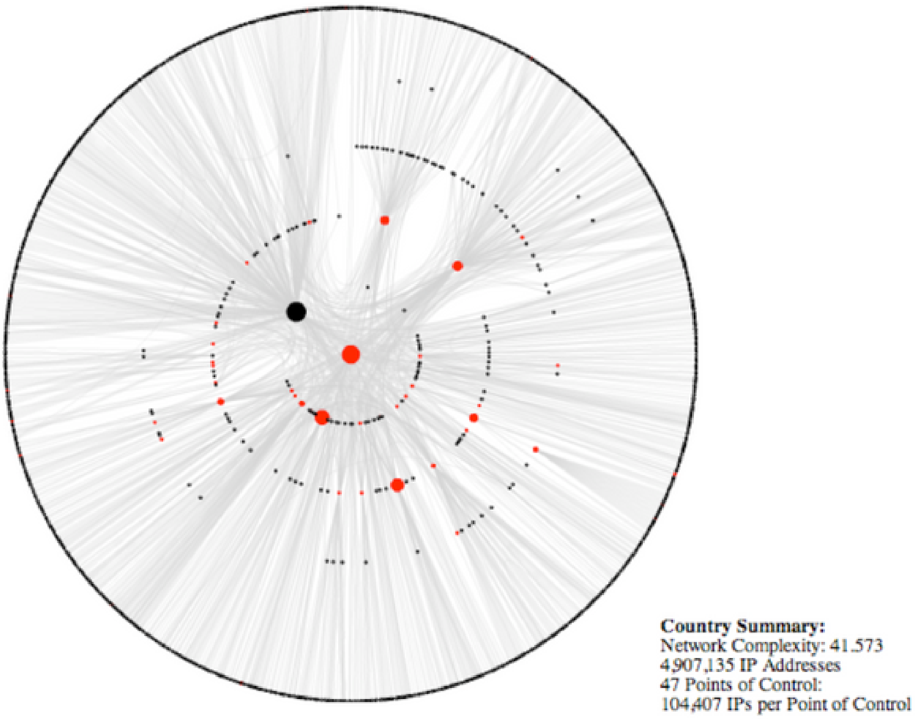
To answer this question, you need to find the most important autonomous systems and define what taking a country offline means. Points of control are "the smallest set of autonomous system nodes whose IP addresses include 90% of a country's total direct IP addresses" (Roberts et al. 2011).[i] In simple terms, these are the most influential systems that would need to be taken down together to take down almost all of a country's internet connectivity. If a system has a single point of control, it has an Achilles heel. If you have many, you can make an attacker play Whack-a-Mole without crippling your system.


More points of control (4)
National IP Address Space
AS 1
AS 3
AS 2
AS 4
Fewer points of control (2)
National IP Address Space
AS 1
AS 3
AS 2
AS 4

The point of control metric was originally developed to see how easily a country's own government could stop internet access. However, it can also be used to assess how many points an invading force would need to target internally to eliminate at least 90% of internet access. With this in mind, Ukraine's AS prefixes can be examined to see how address space is distributed and how resilient it will be to internet infrastructure disruption.

Ukraine is one of the top countries in terms on autonomous systems and points of control. In 2011, when the biggest dataset using the points of control metric was put together, Ukraine had a 48 points of control. In contrast, the UK had 13. This reflects a broader trend that Eastern European countries tend to be more decentralised, spreading address space across autonomous systems. In doing so, they create resilience against individual AS outages. Since then, Ukraine has nearly doubled its number of autonomous systems.[ii]

Autonomous System Diagram - Ukraine



Country Summary:
Network Complexity: 41.573
4,907,135 IP Addresses
47 Points of Control:
104,407 IPs per Point of Control

Source: https://cyber.harvard.edu/netmaps/mlic.pdf

At this time, Ukraine has experienced sporadic connectivity losses without a nation-scale blackout.[i] Internet service providers GigaTrans and NetBlocks have reported services being brought by significant amounts but not completely. The South and East have experienced the most disruption.

The current outlook of Ukraine’s internet availability is helped by the adoption of satellite communications. Starlink terminals have been sent to Ukraine to give more reliable connectivity. However, it should be noted that these could be a potential risk if used. Satellite signals could potentially be triangulated and used to target Ukrainians. This is how Russian aircraft reportedly found and assassinated Chechen president Dzhokhar Dudayev in 1991 while he was using a satellite phone.[ii]

Impact of Ukrainian Outage

If Ukraine was to see a major internet infrastructure disruption, this damage could affect countries relying on shared infrastructure. Ukraine is part of the Trans-Asia Europe System, the Trans-European Lines project, the Kerch Strait Cable, the Italy-Turkey-Ukraine-Russia cable, and the Europe Persia Express Gateway cable.[i] Modern infrastructure has relied on Ukraine as a gateway between East and West Europe.

In the case of the Europe Persia Express Gateway cable, one of the longest terrestrial internet cables could be cut. This 10,000 km cooperative effort between telecoms spans Germany, Poland, Ukraine, Russia, Azerbaijan, and Oman.

The Future of Internet Infrastructure Resilience

In examining past, present, and potential future Russian invasions, clear lessons can be drawn out regarding infrastructural resilience.

Key takeaways:

- Internet infrastructure is a target in modern armed conflict and can be targeted at key terrestrial cables or key autonomous systems.
- Autonomous systems are often hierarchical and inferring the relationships between them can identify key points of control. A numerous and decentralised collection of AS that have a smaller amount of IP address space relying on each can take more hits without a national blackout.
- Satellite communications can be a useful redundancy in the case of infrastructural compromise. However, in armed conflict, this raises the risk of being triangulated by the enemy using satellite signals.

References

i. A. Knapp, “Elderly Woman Shuts Down Armenian Internet,” Forbes, Apr. 09, 2011. https://www.forbes.com/sites/alexknapp/2011/04/09/elderly-woman-shuts-down-armenian-internet/

ii. H. Roberts, D. Larochelle, R. Faris, and J. Palfrey, “Mapping Local Internet Control,” 2011, p. 21. [Online]. Available: https://cyber.harvard.edu/netmaps/mlic.pdf

iii. “Regional Internet Registries Statistics - RIR Delegations - Ukraine (UA) - Autonomous System Number delegations.” https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/Delegations/ASN/UA.html

iv. J. Pearson and R. Satter, “Internet in Ukraine disrupted as Russian troops advance,” Reuters, Feb. 27, 2022. Accessed: Mar. 02, 2022. [Online]. Available: https://www.reuters.com/world/europe/internet-ukraine-disrupted-russian-troops-advance-2022-02-26/

v. E. Margolis, “Time to Set the Chechen Free,” Jan. 05, 2010. https://web.archive.org/web/20120105203129/http://www.ericmargolis.com/political_commentaries/time-to-set-the-chechen-free.aspx

vi. “Ukraine Communications 2020, CIA World Factbook.” https://theodora.com/wfbcurrent/ukraine/ukraine_communications.html (accessed Mar. 04, 2022).

Darkbeam

Dark Beam Limited
Redcliffe Way
Bristol
BS1 6NL
United Kingdom

contact@darkbeam.com
www.darkbeam.com