Governing the Internet after the Ukraine War

Pari Esfandiari

Global TechnoPolitics Forum

GOVERNING THE INTERNET AFTER THE UKRAINE WAR

PARI ESFANDIARI

Global TechnoPolitics Forum

www.TechnoPoltics.org,

ISBN: 978-1-7362034-1-5

Nov. 2022

GLOBAL TECHNOPOLITICS FORUM

The conclusions and recommendations of any Global TechnoPolitics Forum publication are solely those of its authors and do not reflect the views of the Forum, its management, board of advisors, donors, or scholars.

This report is written and published in accordance with the Global TechnoPolitics Forum Policy on Intellectual Independence.

The Global TechnoPolitics Forum is a (501C) (3) nonprofit educational organization with a mission to **shape the public debate and facilitate global coordination at the intersection of technology and geopolitics.** It achieves this mission through: convenings, research, and community building.

Acknowledgements:

Editorial credit: The author would like to thank Graham Baugh for his editorial contributions and Talia Tao for her research contributions.
Cover art credit: Composition II, by Wassily Kandinsky, 1923.
"All methods are sacred if they are internally necessary. All methods are sins if they are not justified by internal necessity."

Please direct inquiries to: Global TechnoPolitics Forum: info@technopolitics.org

TABLE OF CONTENTS

FOREWORD

The brutal Russian invasion of Ukraine drove home, tragically, the intersection that drives the mission of the Global TechnoPolitics Forum -- geopolitics and technology. On its face, the war looks like something out of World War II, tanks and artillery pieces facing off across battlelines, something we thought we'd never again see in Europe. Yet, as this insightful paper by Dr. Pari Esfandiari makes clear, technology has changed this war. The cyber dimension was there from the beginning. In that sense, the war is indeed "cyber world war I." One intriguing puzzle is why Russia has been almost as inept in the cyber realm as on the battlefield.

At least part of the answer is that if technology has shaped the war, the war has also shaped both technology and geopolitics. Confronting Russia's aggression is not just the Ukrainian people and their armed forces, but a so-far surprisingly robust coalition of democracies, led by the United States. Their actions mean that Russia's opponents include not just soldiers but also "legions of financiers, bankers, business executives, hackers, influencers, and spin doctors."

In the longer run, as Dr. Esfandiari notes, the internet and its governance has been dragged into the Cold War 2.0. So far it has resisted choosing sides. But the intrusion of geopolitics has graphically increased the ideological pressures for splintering the net. How far and how long those pressures can be resisted is not just a core question for the Forum but for all those who value not just open commerce but open interchanges across people and nations. We hope Dr. Esfandiari's paper will advance that debate, and, as always, we welcome reactions from readers.

Gregory F. Treverton
Chairman

INTRODUCTION

Russia's invasion of Ukraine, for the most part, seems an old-fashioned war of invasion and terror that demands boots on the ground. In reality, it has blended traditional and innovative elements, and while the cyber dimension has been less visible, it has been fully-fledged from the very start. A study by Microsoft[1] indicates that, as a prelude to the war, on Feb 23, 2022, one day before the official invasion, Russia launched a cyberweapon called 'Foxblade' "against computers in Ukraine. Reflecting the technology of our time, those among the first to observe the attack were half a world away, working in the United States in Redmond, Washington." As for the Ukrainian defense, it has been quick "to disburse its digital infrastructure into the public cloud, where it has been hosted in data centers across Europe."

What we are witnessing, in the words of Ukraine Vice Prime Minister and Minister of Digital Transformation, Mykhailo Fedorov, is a twenty-first century's Cyber World War One (CWWI).[2] In the borderless cyber world, codes have become weapons that move at the speed of light, and war narrative is crowdsourced to be constructed and documented. This war's soldiers are not just "regular Russian and Ukrainian servicemen or even irregular warriors. It also involves legions of financiers, bankers, business executives, hackers, influencers, and spin doctors."[3] As for the ensuing cold war 2.0, it involves an alliance of countries, but also a coalition of the private sector, civil society, and government. The evolving concept and conduct of war pose serious questions about the nature of war, the meaning of soldier, the practice of propaganda, and the role of government.

If technology is changing the meaning of war, the war is also changing the technology by

[1] Microsoft, Defending Ukraine: Early Lessons from the Cyber War-Jun, 2022 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

[2] Bartosz Sieniawski - The first large-scale "digital" conflict, June 2022, https://www.euractiv.pl/section/bezpieczenstwo-i-obrona/news/first-cyber-world-war-ensuring-security-in-times-of-digital-warfare/

[3] Jose Miguel Alonso-Trabanco, SITUATION REPORTS**, A World Remade? Lessons from the Ukraine War** - June, 2022 https://www.geopoliticalmonitor.com/a-world-remade-lessons-from-the-ukraine-war/

expediting innovation and leading its direction through hefty funds offered by governments. When science and technology go to war, what to make of their role in our society, economy, and politics? Because of the nature of cyber technology, the war has gone far beyond the Russia-Ukraine dispute and borders and is now an ideological war involving global powers. As a result, the Internet has been dragged into geopolitics and forced to choose a side. So far, it has shown remarkable resilience, but how long and how far can it endure the ideological pressures? This paper is an attempt to answer some of these questions by stepping back and reflecting on the war so far before looking forward. The outcomes of the war are far from clear, but we can learn about the developing trends and attempt to envision the future to prepare accordingly. The study unfolds in two parts; part one is a brief discussion of the key actions taken by Ukraine and Russia and some of their allies within the realm of cyber technologies, it then proceeds to the analysis of the potential impact of this war on the technology itself. Part two focuses on solutions, it begins with a discussion of the concept of internet governance and its core principles. It then presents the various actors involved, tools employed, strategies adopted, and geopolitical alliances made in the technology space. This is followed by a discussion of potential conditions for collaboration in setting the rules and safeguarding an open universal and accessible internet.

UKRAINE

When the invasion took place on Feb 24th, Ukraine's Internet technology (IT) industry was already highly developed; with over 250,000 engineers, it accounted for over 10% of all Ukrainian exports in 2021. Since Russia's aggression, the industry has shifted to wartime mode with a mandate "to repelling Russian aggression, protecting civilians, evacuating and helping refugees, and keeping the Ukrainian economy alive".[4] Ukraine also launched one of the most successful public relations campaigns ever, by taking command of the war's narrative, at least in the Western block. This section offers a summary of actions taken by Ukraine and its allies in the digital realm so far.

[4] Strategist East - Ukrainian Digital Resistance to Russian Aggression, 2022, https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf

Government Initiated Actions

Recruiting - The key player in this scene is the country's 31 year old Fedorov. "He successfully crowdsourced operations in Russia. His recruitment campaign began on Feb. 24th when his request for volunteers appeared on various hacker forums, stating: "Ukrainian cybercommunity! It's time to get involved in the cyber defense of our country" asking hackers and cybersecurity experts to submit an application via Google docs, listing their specialties and professional references." By Feb 26th, he publicly appealed to the global hacktivists to take down Russia's key websites.[5]

It did not take long for him to amass an international IT and information army of 500,000 hacktivists.[6] They have successfully defended the Internet, energy, and financial systems despite the aggressive attempts by Russia to knock them offline. At the same time, hacktivists targeted Russia's information system, for example, on the symbolic Victory Day, some Russian satellite television menus were hacked to display "You have the blood of thousands of Ukrainians and hundreds of dead children on your hands."[7] Meanwhile, Anonymous _the decentralized international hacktivist collective_ declared a "cyberwar" on Russia shortly after the invasion. They have claimed responsibility for disabling prominent Russian government, news, and corporate websites; and leaking data from entities such as Roskomnadzor _ the federal agency responsible for censoring Russian media. [8]

Changing Law - Under Fedorov's leadership, the country's laws and legislation were rapidly amended to allow for IT activities. This included allowing foreigners to access state data by

[5] Joel Schectman and Thomson Reuters
Joel Schectman and Christopher Bing, Ukraine calls on hacker underground to defend against Russia, Feb. 2022
https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/

[6] Strategist East - Ukrainian Digital Resistance to Russian Aggression, 2022,
https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf

[7] SOPHIE MELLOR, You have blood on your hands – May 2022
https://fortune.com/2022/05/10/russia-smart-tvs-online-platforms-hacked-anti-war-messages-victory-day/

[8] Monica Buchanan Pitrelli, Anonymous declared a 'cyber war' against Russia. Here are the results – March 2022
https://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html

passing the “Criminal Code”, allowing the use of cloud services in government agencies, and allowing foreign and Ukrainian crypto exchanges to work legally by passing the “Virtual Assets” code. At the same time, the Ministry of Transformation launched hundreds of applications, websites, platforms, and channels; the “eVorog” chatbot crowdsources intelligence by enabling Ukrainians to report on the movements and deployment of enemy troops; the Telegram bot offers up-to-date information about mobilization, the search for ammunition, evacuation, humanitarian aid, and much more; the Dokaz portal collects evidence of war crimes committed by Russian military forces; the Moya Viyna Platform allows Ukrainians to describe their personal experiences during the war; the Metahistory NFT Museum provides for the chronology of events during the Russian military invasion of Ukraine; Aid for Ukraine enables people around the world to donate via 16 different cryptocurrencies (it has already raised $60 million); Diia application enables fund transfer to the “Return Alive” foundation (it has raised over $200 million by April 5th 2022); finally, AI and facial recognition technologies are used to inform the relatives of deceased Russian soldiers in the war in Ukraine.[9]

[9] Strategist East - Ukrainian Digital Resistance to Russian Aggression, 2022, https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf

Sanctions

At the same time President Volodymyr Zelenskyy successfully lobbied for tough sanctions on Russia and was rewarded with the most severe sanctions ever levied on a major economy, aimed at the economic, financial, and technological isolation of Russia. Two stop Russia's propaganda —RT and Sputnik— were silenced, banned, blocked, and removed from search engines and social networks altogether.[10] The most devastating sanctions were on Russia's financial system, especially barring it from the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system "which connects more than 11,000 financial institutions in more than 200 countries and facilitates the majority of global money transfers".[11]

Fundamental technologies that power the Internet were also subject to sanctions. The EU has limited Russian access to IP technology and software in foundational technologies like semiconductors.[12] The United States has employed the Foreign Direct Product Rule (FDPR) and imposed new license requirements and licensing policies regarding exports to Russia and certain regions of Ukraine (Feb 2022) and subjected Belarus to the same sanctions (March 2022).[13] These measures are similar to those used against companies like Huawei but have never before been used against an entire country.[14] It is interesting to note that in response to concerns expressed by Internet institutions and activists, the U.S. issued a new General License to exempt from sanctions some communications services, software, hardware, and other

[10] The Economist - Russia looks to Chinese financial plumbing to keep money flowing – March 2022 https://www.economist.com/finance-and-economics/russia-looks-to-chinese-financial-plumbing-to-keep-money-flowing/21808071

[11] AMY GUNIA - Sanctions on Russia Could Drive Moscow Closer to Beijing and Change the Global Financial System https://time.com/6154189/russia-swift-china-usd-rmb-finance-trade/

[12] European Council EU sanctions against Russia explained - 2022 https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/

[13] David Mortlock, Britt Mosman, Peter Bogard, Nikki M. Cronin, Ahmad El-Gamal, Sweeping Export Controls on Russia and Belarus Reach New Heights – March 2022. https://www.willkie.com/-/media/files/publications/2022/sweepingexportcontrolsonrussiaandbelarusreachnewhe.pdf?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration

[14] Annie Froehlich, Foreign Direct Product Rule: Is Russia the next Huawei? – Feb 2022 https://www.atlanticcouncil.org/blogs/econographics/foreign-direct-product-rule-is-russia-the-next-huawei/

connectivity-related technologies such as “instant messaging, videoconferencing, chat and email, social networking, sharing of photos, movies, and documents, web browsing, blogging, web hosting, and domain name registration services”.[15]

[15] OFFICE OF FOREIGN ASSETS CONTROL – 31 CFR part 587 GENERAL LICENSE NO. 25 – April 2022 https://home.treasury.gov/system/files/126/russia_gl25.pdf

Private Sector

The Ukraine government's defense strategy included partnerships with innovative companies such as Microsoft to safeguard its data. At the same time, Mykhailo Fedorov lobbied the international community and orchestrated a digital embargo. He singled out and pressurized the Silicon Valley's tech giants, tweeting "They kill our children, now kill their access!", he tagged Apple's, Tim Cook. Apple paused all product sales in Russia. Fedorov then tagged Elon Musk, tweeting "while you try to colonize Mars — Russia try to occupy Ukraine!", asking for Starlink satellite Internet systems to keep Ukraine's critical infrastructure online. Musk replied that satellites were on their way. He activated Starlink in Ukraine and sent the necessary terminals to connect. On March 2nd Fedorov acknowledged that the systems had arrived.[16]

He "appealed to more than 500 technology companies" to withdraw from Russia and/or expand to Ukraine. His message to global development agencies and international financial institutions was "to support the Ukrainian government's IT-related initiatives".[17] While Fedorov openly pressurized companies for aid, behind the scenes a network of Ukrainian ex-pats and regulators from other countries echoed his voice. The private sector, obliged by sanctions, and/or pressured by Fedorov and his allies, and/or motivated by ethical concerns reacted rapidly; "Facebook and YouTube cracked down on Russian state media, Google disabled some features on Google Maps to protect the safety of Ukrainian citizens,"[18] and many voluntarily withdrew from the Russian market, including Microsoft, Intel, TikTok, Sony, Netflix, Google, Apple, IBM, Oracle, and a host of others.[19] Financial services such as Coinbase blocked 25,000 wallet

[16] Cat Zakrzewski & Gerrit De Vynck, The Ukrainian leader who is pushing Silicon Valley to stand up to Russia – March 2022
https://www.washingtonpost.com/technology/2022/03/02/mykhailo-fedorov-ukraine-tech/
[17] Strategist East - Ukrainian Digital Resistance to Russian Aggression, 2022,
https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf
[18] Cat Zakrzewski & Gerrit De Vynck, The Ukrainian leader who is pushing Silicon Valley to stand up to Russia - March 2022
https://www.washingtonpost.com/technology/2022/03/02/mykhailo-fedorov-ukraine-tech/
[19] Global TechnoPolitics Forum, May 2022
https://technopolitics.org/wp-content/uploads/2022/05/DigitalCohesion.pdf

addresses in Russia, while Visa, Mastercard, American Express, Google Pay, Apple Pay, and PayPal pulled out, impacting e-commerce.[20] In addition, digital certificates that browsers require to ensure safe and encrypted traffic, are not being renewed in Russia. The Russian government is working to replace these with their own Russian-issued certificates, but Google, Microsoft, and Firefox have not accepted these new Russian certificates.[21]

Some businesses have chosen to show solidarity with Ukraine by providing direct support. "Together, major tech companies have committed over $130 million in humanitarian aid to Ukraine and refugees in Poland, with millions more in in-kind donations, matching employee giving, and platform-based fundraising."[22] Others helped with in-kind donations and/or waiving fees to services, or providing hardware/software and other requirements. For example, as early as March 3rd, 2022, several members of the European Telecommunications Network Operators' Association took actions to support people in Ukraine; these included: free international calls to Ukraine, waiving roaming charges, distribution of SIM cards to Ukrainian refugees in neighboring countries, free WiFi in refugee camps, activation of the "SMS donation" function for organizations supporting refugees, including Ukrainian channels in IPTV packages for a fee.[23] Another good example is Starlink. There is also increasing discussion on offering free online services to hacktivists in Russia.

Even the Russian Internet's quasi/infrastructure was not immune. For example, Cogent, one of the largest providers of Internet backbone services in Russia has cut service to customers there; and Lumen, another major Internet carrier pulled out of Russia.[24] Other companies, like domain

[20] BBC – March 2022
https://www.bbc.co.uk/news/technology-60661763
[21] Jim Love - March 2022
https://www.itworldcanada.com/article/splinternet-will-russia-pull-itself-off-the-internet/475791
[22] Diya Li, On the Digital Front Lines: How Tech Companies are Supporting Ukraine – March 2022
https://americaninnovators.com/news/on-the-digital-front-lines-how-tech-companies-are-supporting-ukraine/
[23] Access Now - Digital rights in the Russia-Ukraine conflict - 2022
https://www.accessnow.org/digital-rights-ukraine-russia-conflict/
[24] Karl Bode, U.S. Eases Off Telecom Sanctions That Could Encourage A Russian Splinternet - April 2022

registrar Namecheap, have stopped services for Russian residents.[25] In addition, due to the current digital embargo, a shortage of cloud storage in Russia is predicted.

https://www.techdirt.com/2022/04/12/u-s-eases-off-telecom-sanctions-that-could-encourage-a-russian-splinternet/

[25] Namecheap-March 2022
https://www.namecheap.com/support/knowledgebase/article.aspx/10519/5/faq-transfer-of-russian-customers-services-from-namecheap/

Internet Governance Institutions

In another move, President Volodymyr Zelenskyy called for Russia's right to vote in the UN Security Council to be discounted [26]and there are calls for similar action in other international institutions. While Fedorov sent a request to various Internet governance institutions including ICANN[27] and RIPE NCC[28] to cut Russia off from the Internet (February 28th). Fedorov's appeal received a collective but sympathetic "no." ICANN was asked to revoke Russia's top-level domains (TLD) including .ru and .su along with their Secure Socket Layer (SSL) certificates, in response ICANN president and CEO Goran Marby referred to legal authority and mission, stating; "we take actions to ensure that the workings of the Internet are not politicized, and we have no sanction-levying authority. ICANN has been built to ensure that the Internet works, not for its coordination role to be used to stop it from working."[29] While Hans Petter Holen, managing Director of RIPE NCC pointed to the multi-stakeholder model of decision making, lack of legal authority, and the principles of the open Internet. RIPE argued that the "means to communicate should not be affected by domestic political disputes, international conflicts, or war.". It explained that the organization doesn't have a mandate to take such actions, is governed by community-developed policy and Dutch law, and cannot take such action unilaterally. He then stated that RIPE NCC believes that the Internet number resource registrations should remain apolitical, to avoid serious implications for the global Internet.[30] While Andrew Sullivan, president of the Internet Society said the request misses '"something

[26] Zelenskyy – Feb 2022
https://twitter.com/ZelenskyyUa/status/1497633468586541057?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1497633468586541057%7Ctwgr%5E%7Ctwcon%5Es1_c10&ref_url=https%3A%2F%2Fwww.foxnews.com%2Fpolitics%2Frussias-role-un-under-scrutiny-as-ukraine-calls-security-council-status-removed

[27] Request letter to ICANN – Feb 2022
https://www.icann.org/en/system/files/correspondence/fedorov-to-marby-28feb22-en.pdf

[28] Request letter to RIPE NCC – Feb 22
https://www.ripe.net/publications/news/announcements/request-from-ukrainian-government.pdf

[29] ICANN – March 2022
https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

[30] RIPE NCC – March 2022
https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

fundamental about the Internet: it was never designed to respect country borders. The idea of unplugging a country is as wrong when people want to do it to *another* country as it is when governments want to do it to their own."[31]

As listed above, it seems that Ukraine has rapidly launched a truly impressive operation, but this operation has been evolving since 2014 and Ukraine's cyber forces have been building connective tissues with Western governments and their allies as well as with tech giants in Silicon Valley. Today, Ukraine receives robust intelligence cooperation from the US,[32] while the European Union offers cyber capacity-building support through Permanent Structured Cooperation (Pesco).[33] Meanwhile, an agreement has been signed between the State Archival Service of Ukraine and the National Archives of the United Kingdom on the temporary transfer of cloud data storage and backup copies of digital materials of Ukrainian state archival institutions in case of their potential loss.[34]

[31] ISOC – March 2022
https://www.internetsociety.org/blog/2022/03/why-the-world-must-resist-calls-to-undermine-the-internet/

[32] CATO institute – March 2022
https://theintercept.com/2022/03/17/us-intelligence-ukraine-russia/

[33] European Defense Agency – Feb 2022
https://eda.europa.eu/news-and-events/news/2022/02/24/-of-first-capability-developed-under-pesco-points-to-strength-of-cooperation-in-cyber-defence

[34] Ukraine War 24 – March 2022
https://ukrainewar24.com/kmu-the-first-agreement-on-backup-storage-of-digital-copies-of-naf-documents-of-ukraine-in-cloud-storage-of-foreign-partners/

RUSSIA

In contrast, Russia finds itself facing a strong, antagonistic global coalition since the invasion of Ukraine, with global activists joining the scene in the digital realm. On March 29th, Russia issued a public statement warning the "anonymous hackers and provocateurs" supported by the U.S. and Western allies" of "grave consequences".[35]

Historically, Russia has been a spoiler in the cyber world, mainly engaged in disseminating mis/dis information and hacking but always making sure that its mischief is within the "gray zone," often referred to as Article 4.7 —short of NATO's Article 4 or Article 5— to ensure that the Western response won't be armed conflict. In this recent conflict, it has employed "a cyber strategy that includes at least three distinct and sometimes coordinated efforts – destructive cyberattacks within Ukraine, network penetration and espionage outside Ukraine, and cyber influence operations targeting people around the world."[36] It is interesting to note that the cyber-attacks began on Feb 23rd, one day before the official invasion. As a prelude to the war a cyber weapon called 'Foxblade' "was launched against computers in Ukraine."[37] Attacks on data centers and internet infrastructures remain an ongoing practice.

However, the invasion lacks a visibly major cyber offense element. This may be deliberate and strategic since Russia's objective is physical invasion and that translates to boots on the ground. Revealing digital capability could be viewed as unnecessary or even disadvantageous.[38] Today, Russia's digital posture for the most part is defensive, its information technology (IT) infrastructure is degrading due to sanctions and voluntary withdrawal of private companies,

[35] Jennifer Shore, Don't Underestimate Ukraine's Volunteer Hackers – April 2022 https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/.
[36] Microsoft, Defending Ukraine: Early Lessons from the Cyber War-Jun, 2022 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK
[37] Microsoft, Defending Ukraine: Early Lessons from the Cyber War-Jun, 2022 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK
[38] Heli Tiirmaa-Klaar**,** American Council on Germany (Webinar) – May 2022 https://www.youtube.com/watch?v=ORZPniwJFk8&ab_channel=AmericanCouncilonGermany

while its sophisticated IT workforce is shrinking because a large number of experts are leaving the country.[39]

At the same time, Russia has tightened its control over local media and has passed legislation to criminalize the distribution of unfavorable content.[40] It has charged tech giant Meta (Facebook, Instagram, and What's App) with being an "extremist organization"[41], and blocked its operations, also banned Google News for being the source of "fake news." [42] At the same time Russia has launched Russian state-owned social media as an alternative to Western social media —Rutube (YouTube) owned by Gazprom, Fiesta, and Rossgram (Instagram),[43] and Yappy (TikTok). [44]

However, Russia's voluntary cyber isolation has been in the making since long before the Ukraine invasion. In the aftermath of the Cold War, a weakened Russia has advocated upholding the preeminence of state sovereignty as a foundational principle of international order. In the 2000s, Moscow joined forces with Beijing to spearhead the global movement for Internet sovereignty. Facing an unprecedented anti-government uprising from late 2011 to mid-2012, and realizing the Internet's instrumental role in organizing it, the Kremlin turned its attention to Russian cyberspace; mainly controlling content and regulating infrastructure. "The so-called

[39] Anthony Faiola, Mass flight of tech workers turns Russian IT into another casualty of war- May 2022 https://www.washingtonpost.com/world/2022/05/01/russia-tech-exodus-ukraine-war/

[40] Russia expands laws criminalizing 'fake news' – March 2022 https://www.politico.eu/article/russia-expand-laws-criminalize-fake-news/

[41] EuroNews, Russia bans Instagram and Facebook as court declares Meta an 'extremist organization. https://www.euronews.com/next/2022/03/21/ukraine-war-facebook-temporarily-allows-posts-calling-for-violence-against-russians-or-put

[42] Ukraine war: Russia bans Google News for 'spreading disinformation' weeks after Google blocks Russian media portals - March 2022 https://www.opindia.com/2022/03/russia-bans-google-news-over-disinformation-about-ukraine-war/

[43] Russians flock to domestic social media as Western sites barred – April2022 https://www.dailysabah.com/business/tech/russians-flock-to-domestic-social-media-as-western-sites-barred

[44] Russia Launches Homemade TikTok Alternative – nov 2021 https://www.themoscowtimes.com/2021/11/30/russia-launches-homemade-tiktok-alternative-a75701

Blacklist Law established a framework for blocking websites". [45] In the aftermath of the annexation of Crimea, the Russian government took the concept of digital sovereignty to a new level. "The data localization law, for example, required foreign technology companies to keep Russian citizens' data on servers located within the country", under "the pretext of fighting terrorism, another law required telecom and Internet companies to retain users' communications for six months and their metadata for three years and hand them over to authorities upon request without a court order."[46]

In April 2019, the Sovereign Internet Law was passed, which required all Internet service providers to install state-mandated devices "for counteracting threats to stability, security, and the functional integrity of the Internet"[47] within Russian borders. The Russian government has "interpreted threats broadly, including social media content". In addition, "the law establishes protocols for rerouting all Internet traffic through Russian territory and for a single command center to manage that traffic".[48] That center is called Roskomnadzor, the Russian telecom regulator. Russia claims that RuNet has been tested and works [49] and it has been encouraging official and public sites to use .ru domains and localize their data, and minimize the use of overseas service providers.[50] Lastly, the law "promises "to establish a Russian national Domain Name System (DNS)".[51] So far, it has created a database of its community suppliers and an Area Title System detailing all nationwide IP addresses which could produce personal IPs completely

[45] Stanislav Budnitsky, Kremlin tightens control over Russians' online lives – threatening domestic freedoms and the global Internet – June 2022
https://www.myjournalcourier.com/news/article/Kremlin-tightens-control-over-Russians-online-17276291.php
[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Krutika Patil, Russia–Ukraine Conflict and Geopolitics of Data Routing – April 2022
https://idsa.in/issuebrief/russia-ukraine-conflict-and-geopolitics-of-data-routing-kpatil-290422
[50] Steven Vaughan-Nichols, Russia may be cutting itself off from the Internet - March 2022
https://www.zdnet.com/article/how-to-jump-to-microsoft-edge-from-internet-explorer/
[51] Stanislav Budnitsky, Kremlin tightens control over Russians' online lives – threatening domestic freedoms and the global Internet – June 2022
https://www.myjournalcourier.com/news/article/Kremlin-tightens-control-over-Russians-online-17276291.php

divorced from the World Wide Web.[52]

The sovereign Internet law is a powerful tool of control, it may be true that “The law’s idea is not to isolate the country completely, but to have a tool to isolate regions if they face a crisis.”[53] On full display is also the geopolitics of data routing. In 2014, Russia gained control over the Internet networks of the annexed Crimea and Donbas regions. Gradually, by creating the Sovereign Internet/RuNet, Russia gained complete control of all Internet Transit Points there. As a result, “even before Russian troops set foot in Donbas in the current conflict, Russia had complete control over the region’s Internet network”.[54] Russia claims that this law is a backup in the event of a crisis, mainly for a scenario where the West decides to cut Russia off from the global Internet.[55] But as became clear during the Ukraine invasion, the request to cut off Russia from the Internet was rejected wholeheartedly by the Internet community, who voted for the integrity of the Internet over geopolitics and chose an apolitical stand.

[52] Webringnet - Kremlin Tightens Control Over Russians’ Online Lives – June 2022 https://webringnet.com/kremlin-tightens-control-over-russians-online-lives/2/

[53] Russia: Growing Internet Isolation, Control, Censorship – June 2022 https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship#:~:text=Russian%20internet%20users.-,The%20Sovereign%20internet%20Law,state's%20control%20over%20internet%20infrastructure.

[54] Krutika Patil, Russia–Ukraine Conflict and Geopolitics of Data Routing – April 2022 https://idsa.in/issuebrief/russia-ukraine-conflict-and-geopolitics-of-data-routing-kpatil-290422

[55] For a comprehensive discussion see: Kieren McCarthy, Russia threatens to set up its 'own Internet' with China, India and pals – let's take a closer look – Dec 2017 https://www.theregister.com/2017/12/01/russia_own_internet/?page=1

SPLINTERNET

There have been concerns that the severe reactions to Russia's invasion of Ukraine within the digital realm may have adverse consequences. The withdrawal of major U.S. tech and credit card companies hand in hand with the potential unavailability of cloud storage, could cause the ordinary Russian population hardship and exclude them from access to the essential software and even private network Apps which are deemed essential for activists inside Russia to fight propaganda and to organize protests. This argument is supported by the massive spike in the download of virtual private networks (VPNs), where the daily download has jumped from around 15,000 in mid-February to 475,000 in March.[56]

Sanctions on financial systems could cause unintended consequences encouraging "certain countries to bypass and even challenge both the status of the US dollar as the hegemonic reserve currency and the transnational financial arteries organically linked to its circuits through vehicles such as gold and other hard assets with intrinsic value, FinTech innovations, multilateral deals, and digital currencies."[57] Similarly, some services such as Amazon Web Services or Github Repositories, impact the back end of the Internet, and banning them from a particular territory would paralyze many other services, perhaps creating major problems globally, at least temporarily.[58]

Most important is the Internet community's warning that the combination of forced-upon and self-imposed measures in light of ideological and geopolitical interests, may encourage Russia to activate its capabilities and decouple from the World Wide Web. Such a move would fragment

[56] Sead Fadilpašić, VPN downloads in Russia have skyrocketed - May, 2022 https://www.techradar.com/uk/news/vpn-downloads-in-russia-have-skyrocketed
[57] Jose Miguel Alonso-Trabanco, SITUATION REPORTS, A World Remade? Lessons from the Ukraine War - June, 2022 https://www.geopoliticalmonitor.com/a-world-remade-lessons-from-the-ukraine-war/
[58] James Ball, Russia is risking the creation of a "splinternet"—and it could be irreversible – April 2022 https://www.technologyreview.com/2022/03/17/1047352/russia-splinternet-risk/

the Internet with ‘seismic’ consequences and may even lead to a long-lasting splinternet —a complete breakdown of the Internet into separate and independent networks.[59]

Tendencies towards fragmentation are hardly a new phenomenon, over the last two decades almost all countries have taken steps in that direction. Overall, the free flow of data and information, to various degrees, is seen by sovereign nations as posing a direct challenge to their political systems and hence they aim to control it. As a result, the “ideology undergirding the internet has been changing for some time in the direction of greater sovereign control of networks and network activities. According to Drake, W. Cerf, V., & Kleinwächter, W. Internet fragmentation could happen at three levels: government, technical, and commercial.[60]

- Fragmentation at the government level is usually directed at content and application layers. The real risk from expanding sovereignty is “fragmentation of governance, where the underlying protocols would still support global connectivity, but connectivity overlaid with many uncoordinated and often dissonant rules for data, privacy, and security.”[61] This mainly occurs in the form of the regulation of content, erosion of access to information, censorship, and blocking of specific web services, either temporarily during social unrest, or on a more permanent basis.[62]

- Technical fragmentation refers to fragmentation at the basic infrastructure and logistic layers of the Internet – the physical/link layer, the network/IP layer, and the transport layer.[63]

[59] CAITRÍONA HEINL, Debating the Tech Sanctions on Russia: Is ‘Splinternet’ Upon Us? – April 2022 https://www.orfonline.org/expert-speak/debating-the-tech-sanctions-on-russia/

[60] William J. Drake Vinton G. Cerf Wolfgang Kleinwächter, Internet Fragmentation: An Overview, Future of the Internet Initiative White Paper, World Economic Forum, January 2016. https://www3.weforum.org/docs/WEF_FII_internet_Fragmentation_An_Overview_2016.pdf

[61] James Andrew Lewis, CSIS, Sovereignty and the Evolution of Internet Ideology - October, 2020 https://www.csis.org/analysis/sovereignty-and-evolution-internet-ideology

[62] William J. Drake Vinton G. Cerf Wolfgang Kleinwächter, Internet Fragmentation: An Overview, Future of the Internet Initiative White Paper, World Economic Forum, January 2016. https://www3.weforum.org/docs/WEF_FII_internet_Fragmentation_An_Overview_2016.pdf

[63] ibid.

Widespread technical fragmentation would eliminate the global "network of networks" and replace it with a kind of multiverse of local, national, or regional networks with no information flows between them.[64] This is most popular among authoritarian countries; for example, China's Great Firewall (GFW), Iran's halal net, North Korea's Kwangmyong, Cuba's RedCuba, and of course Russian sovereign Internet, also known as Runet. Beyond national borders, some countries are grouped to create telecommunication networks that are independent from the Internet. For example, BRICS Cable is a 34,000-kilometre-long underwater fiber optic cable that aims to connect Brazil, India, South Africa, Russia, and China.[65] China and Chile are connecting through the construction of an underwater fiber optic cable as a first of its kind between Asia and Latin America.[66] Measures taken by some of the non-authoritarian countries are also concerning, for example, Europe's intention to create a European DNS resolver "DNS4EU") is an example. "The Internet's name system is an important topic of conversation in today's Internet. It appears that the DNS is the only remaining part left of the "glue" that holds the Internet together and is now the defining medium of what is "the Internet."[67]

- Fragmentation at the commercial level refers to business "practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources. These generally are targeted at the content and transactions layer in our model, but they may involve actions taken at the lower technical layers as well".[68]

Despite current trends towards fragmentation, an entire split from the global Internet is unlikely because nation states' political and economic strategic self-interests encourage remaining

[64] Wade Hoxtell and David Nonhof, Internet Governance, GPPI- 2019
https://www.gppi.net/media/internet-Governance-Past-Present-and-Future.pdf
[65] Kévin Limonier, Russia in Cyberspace: Issues and Representations - 2014
https://www.cairn-int.info/article-E_HER_152_0140--russia-in-cyberspace-issues.htm
[66] Han Jie, China, Chile mulling first undersea fiber optic cable linking Asia, Latin America – June 2017
https://news.cgtn.com/news/3d41444f7749444e/share_p.html
[67] Geoff Huston, Some Thoughts on DNS4EU – the European Commission's Intention to Support the Development of a New European DNS Resolver – Feb 2022
https://circleid.com/posts/20220213-some-thoughts-on-dns4eu-new-european-dns-resolver/
[68] William J. Drake Vinton G. Cerf Wolfgang Kleinwächter, Internet Fragmentation: An Overview, Future of the Internet Initiative White Paper, World Economic Forum, January 2016.
https://www3.weforum.org/docs/WEF_FII_internet_Fragmentation_An_Overview_2016.pdf

within the system. However, current political tensions could "exacerbate global trends towards technological decoupling, techno-nationalism, and turn investment into domestic substitutes which were already apparent before the Ukraine invasion"[69] to an essential digital strategy. "Sanctions and other decisions that are not well-targeted will undermine the Internet's connectivity and its apolitical nature, splitting it along geopolitical lines and opening the door for further restrictions across the globe".[70] The invasion of Ukraine has brought to sharp attention a major gap in Internet governance and posed new challenges, with open questions surrounding appropriate sanctions and their consequences, as well as an associated governance mechanism and tools.

[69] CAITRÍONA HEINL, Debating the Tech Sanctions on Russia: Is 'SplInternet' Upon Us? – April 2022 https://www.orfonline.org/expert-speak/debating-the-tech-sanctions-on-russia/

[70] Constance Bommelaer & David Frautschy, We sanction the Internet at our peril: Cutting off Russia will damage the global Internet-April 2022 https://www.euractiv.com/section/all/opinion/we-sanction-the-internet-at-our-peril-cutting-off-russia-will-damage-the-global-internet/

INTERNET GOVERNANCE

The UN WGIG (Working Group on Internet Governance)[71] defines Internet governance as "the application by governments, the private sector and civil society of principles, norms, rules, procedures, and programs that shape the evolution and use of the Internet".[72] In a given area of international relations, regimes form a framework to facilitate cooperation and reach treaties and agreements.[73] Joseph S. Nye, Jr points out that Internet governance is composed of three broad areas: tools (laws, policies, technical standards or codes of conduct), layers (infrastructure, logic, applications, and content), and actors.[74]

Tools - "Much of the governance efforts occur within national legal frameworks, although the technological volatility of the cyber domain means that laws and regulations are always chasing a moving target."[75] Meanwhile, international treaties and agreements are beginning to appear on the scene, while standards have played a critical role right from the start.

Actors - In its early days, ideological libertarians proclaimed that "information wants to be free," portraying the Internet as the end of governments' control. "In practice, however, governments and geographical jurisdictions have been playing a major role in cyber governance right from the start (see Goldsmith and Wu 2006)."[76] Yet, the majority of the Internet technology is

[71] The Working Group on Internet Governance (WGIG) was a United Nations multistakeholder Working group initiated after the 2003 World Summit on the Information Society (WSIS) first phase Summit in Geneva failed to agree on the future of Internet governance. Also see https://www.apc.org/sites/default/files/IG_10_Final_0.pdf
[72] Joseph S. Nye, Jr, The Regime Complex for Managing Global Cyber Activities – May 2014 https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf
[73] Tayyar Arı, Uludag University, THEORIES OF INTERNATIONAL RELATIONS-II – April 2019 https://www.researchgate.net/profile/Tayyar-Ari/publication/332130685_THEORIES_OF_INTERNATIONAL_RELATIONS-II/links/5cfd7db5299bf13a384a46fa/THEORIES-OF-INTERNATIONAL-RELATIONS-II.pdf
[74] Wade Hoxtell and David Nonhof, Internet Governance, GPPI- 2019 https://www.gppi.net/media/internet-Governance-Past-Present-and-Future.pdf
[75] Joseph S. Nye, Jr, The Regime Complex for Managing Global Cyber Activities – May 2014 https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf
[76] Ibid

produced by the private sector and the majority of infrastructure is owned by the private sector. Equally important is the role of the technical community in envisioning and coding the evolution of technology. These factors combined with the perception of the Internet as a public good have led to the multistakeholder model where no single stakeholder has a leading role in governing the Internet and decisions are made in discussion with multiple actors.

Figure 1: Internet Layers

5	Physical/Link Layer
4	Network/IP Layer
3	Transport Layer
2	Application Layer
1	Content and Transactions Layer

Source: Internet Fragmentation [77]

Layers - Discussing Internet governance, Drake, W. Cerf, V., & Kleinwächter, W. point out to five layers as shown in Figure 1. [78]

"In its early stages, the Internet was predominantly viewed as a purely technical infrastructure and, as such, Internet governance primarily took place along the infrastructure and logical layers". [79] Commercial use and increased users posed new challenges and concerns shifted to the application and content layer. Today, Internet governance happens at the global, regional, national, and local levels. As a basic rule, the physical, infrastructure, and technical layers, have a global approach. "Protocols, cables, and routers are maintained collaboratively by the

[77] Ibid

[78] William J. Drake Vinton G. Cerf Wolfgang Kleinwächter, Internet Fragmentation: An Overview, Future of the Internet Initiative White Paper, World Economic Forum, January 2016. https://www3.weforum.org/docs/WEF_FII_internet_Fragmentation_An_Overview_2016.pdf

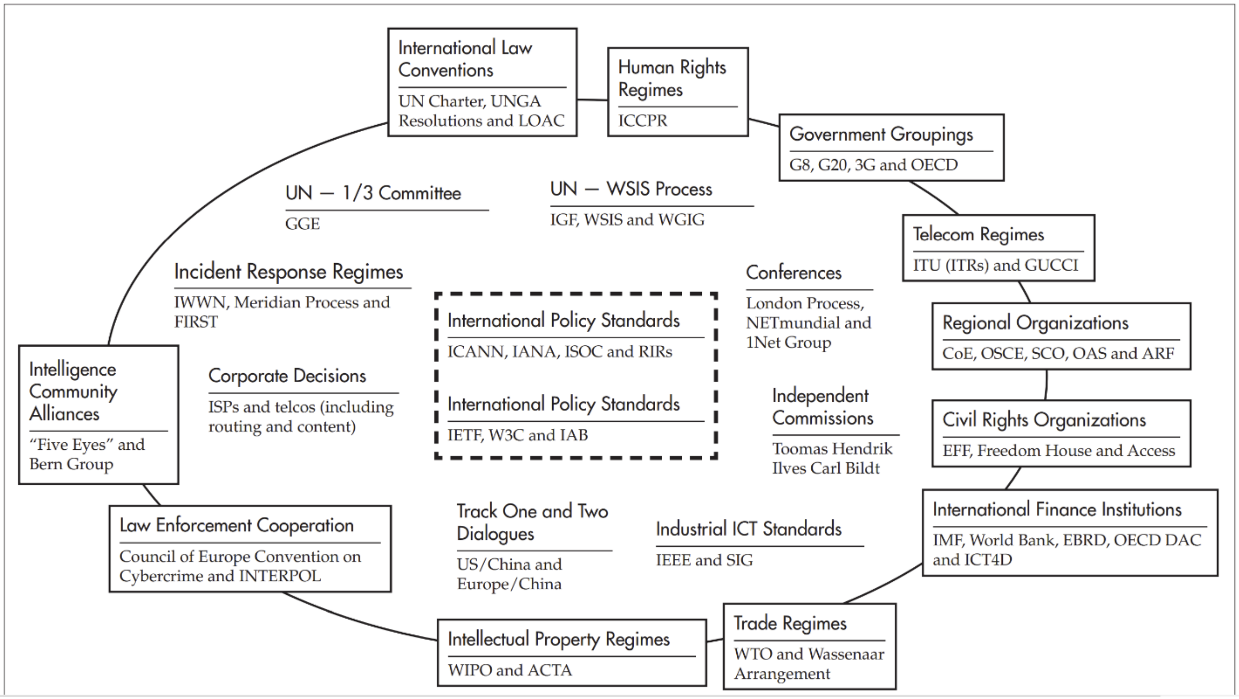
[79] Wade Hoxtell and David Nonhof, Internet Governance, GPPI- 2019 https://www.gppi.net/media/internet-Governance-Past-Present-and-Future.pdf

countries involved due to the value and need to keep the Internet functions as a cross-border and global technical structure.” [80] However, when it comes to regulating the application and content layers, national and local governance mechanisms seems more relevant.

Nye’s Regime Complex for Mapping Global Cyber Activities shown in Figure 2. is particularly useful in locating Internet governance within the larger context.
“First, it demonstrates the extent and wide range of actors and activities related to governance that exist in the space. Second, it separates issues related to the technical function of connectivity, such as the domain name system (DNS) and technical standards where a relatively coherent and hierarchical regime exists, from the much broader range of issues that constitute the larger regime complex. Third, it encourages us to think of layers and domains of cyber governance that are much broader than just the issues of DNS and ICANN, which have limited functions and little to do directly with larger issues such as security, human rights, or development.”[81]

[80] Ibid
[81] Ibid

Figure 2 – THE Regime Complex for Mapping Global Cyber Activities


International Law Conventions
UN Charter, UNGA Resolutions and LOAC
Human Rights Regimes
ICCPR
Government Groupings
G8, G20, 3G and OECD
UN — 1/3 Committee
GGE
UN — WSIS Process
IGF, WSIS and WGIG
Telecom Regimes
ITU (ITRs) and GUCCI
Incident Response Regimes
IWWN, Meridian Process and FIRST
International Policy Standards
ICANN, IANA, ISOC and RIRs
International Policy Standards
IETF, W3C and IAB
Conferences
London Process, NETmundial and 1Net Group
Regional Organizations
CoE, OSCE, SCO, OAS and ARF
Intelligence Community Alliances
"Five Eyes" and Bern Group
Corporate Decisions
ISPs and telcos (including routing and content)
Independent Commissions
Toomas Hendrik Ilves Carl Bildt
Civil Rights Organizations
EFF, Freedom House and Access
International Finance Institutions
IMF, World Bank, EBRD, OECD DAC and ICT4D
Law Enforcement Cooperation
Council of Europe Convention on Cybercrime and INTERPOL
Track One and Two Dialogues
US/China and Europe/China
Industrial ICT Standards
IEEE and SIG
Trade Regimes
WTO and Wassenaar Arrangement
Intellectual Property Regimes
WIPO and ACTA

Source: The Regime Complex for Managing Global Cyber Activities [82]

The unique combination of physical and virtual properties of cyberspace poses complex governance challenges. "The physical infrastructure layer largely follows the economic laws of rival resources and increasing marginal costs". Most importantly, it easily lends itself to the political laws of sovereign governmental jurisdiction and control. The virtual or informational layers on the other hand "have economic network characteristics of increasing returns to scale" and do not fit well within government jurisdictional control. "Attacks from the informational realm, where costs are low, can be launched against the physical domain, where resources are scarce and expensive." In contrast, control of the physical layer can have both territorial and extraterritorial implications for the informational layers. Within the complex Internet ecosystem, all actors cooperate and compete for power. "Cyber power can be defined

[82] Joseph S. Nye, Jr, The Regime Complex for Managing Global Cyber Activities – May 2014
https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

in terms of a set of resources that relate to the creation, control, and communication of electronic and computer-based information — infrastructure, networks, software, and human skills. This includes the Internet of networked computers, but also intranets, mesh nets, cellular technologies, cables, and space-based communications."[83]

As we can see from this brief discussion, the Internet governance ecosystem is very complex and does not lend itself to one simple solution that fits it all. Rather it demands flexibility to select the most impactful form of governance in each new situation. As such, agreement on principles becomes an essential starting point and establishing a regime is essential.

[83] Ibid

CORE PRINCIPLES

D**ecentralized** – the Internet was born in the United States as a project of the Advanced Research Projects Agency (ARPA) under the US Department of Defense. The concept was developed in the 1950s and 1960s, at the height of the Cold War, and out of fear of a potential nuclear attack on the country's centralized communication systems by the Soviet Union. "The idea was to build a decentralized system of communication that would utilize a "web" rather than a central hub. In such a system, messages could be sent through a large network of carrier lines without having to pass through a central and easily destroyable hub, allowing for different pathways to the destination. … The first such decentralized system was the Arpanet".[84]

Libertarian - Born out of libertarian ideals of the Internet's founding fathers in the United States, it was intended to expand individual freedoms worldwide, strengthen democracy, and create prosperity through innovation and economic progress. John Perry Barlow's *"Davos Declaration on Cyber-Independence*," in 1996 painted a "promised land" of Liberty, Equality, and Fraternity. Decisions made in those early days laid the foundation for a free and open Internet as well as a multistakeholder model. These traits have long been embedded into the DNA of the Internet. [85]

Free, Open, and Universal – This was the credo of the Internet founding fathers who believed that information should flow freely across all networks. That everyone should have equal access to use the Internet as they wish with limited interference from governments. "From a technical standpoint, it meant that different networks with different transmission technologies could connect into one large global network" using a common protocol – the Transmission

[84] Wade Hoxtell and David Nonhof, Internet Governance, GPPI- 2019 https://www.gppi.net/media/internet-Governance-Past-Present-and-Future.pdf
[85] Ibid

Control Protocol/Internet Protocol (TCP/IP). “From an economic, social, and political standpoint, this enabled anyone with a computer and an Internet connection to play a role in building the identity of the Internet which served as the key driver of the Internet’s astonishing growth and social/political position in our societies.”[86]

Multi-Stakeholder Governance Model – This is best described as “a transparent, open, and bottom-up consensus-building process.” Currently, the discussion about the multistakeholder model is centered around the **International Telecommunication Union** (**ITU**) model versus the ICANN model, with authoritarian countries and even some developing countries favoring ITU because they believe it is a better match to their internal security and politics. Moreover, they dislike the ICANN because it is an American corporation accountable to the U.S. government. In contrast, Western governments “fear that the cumbersome features of the ITU would undercut the flexibility of the “multi-stakeholder” process that stresses the role of the private and non-profit sectors as well as governments.”[87]

Public Good – The cyberspace domain is often referred to as a public good or global commons —the earth's unowned **supranational natural resource**. Nye argues that these terms are an imperfect fit, explaining that “A public good is one from which all can benefit, and none should be excluded”. Mapping it to the Internet, it describes some of the information protocols of the Internet, but not the “physical infrastructure, which is a scarce proprietary resource located within the boundaries of sovereign states” and available to some but not to all. Alternative terms are used such as “club good” (Raymond 2013), “imperfect commons (pers. comm. & James A. Lewis; CSIS 2008), and “common-pool resource” (Elinor Ostrom).[88]

It is argued that the public good nature of the Internet, even if it is imperfect, in hand with

[86] Wade Hoxtell and David Nonhof, Internet Governance, GPPI- 2019
https://www.gppi.net/media/internet-Governance-Past-Present-and-Future.pdf
[87] Joseph S. Nye, Jr, The Regime Complex for Managing Global Cyber Activities – May 2014
https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf
[88] Ibid

private sector ownership rights offer governments only a partial governing authority. Today, “there is no single regime for the governance of cyberspace”, but, as shown in Figure 2. “there is a set of loosely coupled norms and institutions that rank somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages.”[89]

Human Rights - Article 19 of the Universal Declaration of Human Rights states: "Everyone has the right to freedom of opinion and expression: this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers".[90] If access to information is a fundamental human right, then it must be a pillar of policy-making, especially in conflict zones. The right of access to information is a specific manifestation of freedom of expression. In the current information wars both on the national and international levels, enabling access to information, especially in conflict zones and authoritarian spaces is critical. As a result subsidizing VPNs has gained attention as did shortwave radio promotion during the cold war with RFTL. However, even though **“**The expression 'the right to know' is now well-entrenched in legal literature, much work still lies ahead in working out its status in international law and in domestic legal systems. What are its legal foundations, its constitutional and other limitations, and its conflicts with the public interest? What areas or knowledge are covered?”[91]

Apolitical - One, universal, open, and accessible Internet is the greatest human achievement in the 21st century which benefits all nations regardless of their political inclinations. To keep the Internet intact, it must remain apolitical. The internet pioneer, Paul Baran’s design for

[89] Joseph S. Nye, Jr, The Regime Complex for Managing Global Cyber Activities – May 2014
https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf
[90] United Nations, Universal Declaration of Human Rights
https://www.un.org/en/about-us/universal-declaration-of-human-rights
[91] CG Weeramantry· 1994
https://brill.com/downloadpdf/book/edcoll/9789004400634/B9789004400634_s008.xml

"ARPANET was a network of equals, of peers. No single machine had authority over the others." Similarly, Technology writer, Steven Johnson envisions the future as a “Networking that decentralizes intellectual power even as it boosts it”, he calls it "peer progressivism".[92]

The opponents of this position argue that the Internet is, and always has been, a very political tool. It is a crucial technology that is embedded in every aspect of our life and choosing an apolitical position is itself an intensely political act that follows the libertarian vision of the Internet founding fathers. This group is further divided between those who believe the Internet should be employed as an effective tool within current geopolitics and others who see the Internet’s role as a disruptive force shifting politics from tensions between nations to global citizens’ struggle against governments. They argue that the libertarian political activist, John Perry Barlow’s statement clarifies the Internet founding fathers' position for a world free of all governments and that the current arguments around the Internet’s role —as apolitical or political— are different strategies for the same end.

[92] Bernard Vaughan – Oct 2012
https://www.nbcnews.com/tech/tech-news/author-sees-blueprints-social-change-internet-design-flna1c6322018

CURRENT STATES OF AFFAIRS

As yet, there are no clear guidelines for Internet governance and while some international law may be applicable, the ambiguities leave individuals, organizations, and even governments vulnerable. There have been many attempts to establish global principles for Internet governance. Over the years, a cooperation framework on cyber stability has been established between the United States and most of the technologically advanced European countries, as well as Japan and Australia. In addition, there have been joint statements in the United Nations to set up a cyber stability regime and information sharing. Joint deterrence acts and statements, including the statements on attributing the different cyber-attacks on Russia and China, have been issued since 2018. Even though they may not be as effective as desired, they had some impact.[93]

When it comes to Internet governance, again, many attempts have been made. These include the UN Secretary-General's publication of a "Roadmap on Digital Cooperation (2021); the UN-hosted Internet Governance Forum (IGF) which is now under reform towards an IGF+; the UN "Global Digital Compact" which will be adopted at the "UN World Summit on the Future"; and the review conference of the outcomes of the UN World Summit on the Information Society (WSIS+20) (2025).[94] The US-EU Trade and Technology Council (TTC) was established in 2022 to navigate European and American understandings of "digital sovereignty" and the resulting market regulations.

Finally, the latest attempt is an initiative of the U.S. government; the "*Declaration on the Future of the Internet". It was announced on* April 28, 2022, and is signed by 60 out of 193 UN

[93] Heli Tiimaa-llaar, America Council on Germany, Panel discussion: Cyber and Tech Dimension of Russian War on Ukraine - May 6 2022
https://www.youtube.com/watch?v=ORZPniwJFk8&ab_channel=AmericanCouncilonGermany
[94] Wolfgang Kleinwächter, How to Save the "Past" in the "Future of the Internet" – April 2022
https://circleid.com/posts/20220507-how-to-save-the-past-in-the-future-of-the-internet-principles-the-washington-declaration

governments. It creates transatlantic harmony around democratic principles and "is intended to serve as a reference document for future international negotiations on Internet-related issues"[95] in the same way that the universal charter on human rights has served. As for its vision of the Internet, it is really old wine in a new bottle, recalling the Internet founding fathers' vision for "an open, free, global, interoperable" Internet but adding a new orientation. It is based on five principles*;* Protection of Human Rights and Fundamental Freedoms, A Global Internet, Inclusive and Affordable Access to the Internet, Trust in the Digital Ecosystem, and Multistakeholder Internet Governance.[96] This Declaration is an offshoot of the Biden Administration's Summit for Democracy (S4D) and supports "the preservation of the universality of the Domain Name System (DNS), globally applicable Internet standards, and network neutrality. Its message is clear: regardless of all political disputes, the "technical core of the Internet" should not be attacked."[97] This is in line with recent statements made by ICANN, RIPE NCC, and ISOC" that we discussed earlier in this paper. However, the Declaration is criticized for being a top-down initiative, only involving governments and as yet, no procedure has been published on how to join the declaration, this applies above all to the inclusion of non-governmental stakeholders.[98]

[95] ibid

[96] White House, A Declaration for the Future of the Internet – April 2022 https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-internet_Launch-Event-Signing-Version_FINAL.pdf

[97] Wolfgang Kleinwächter, How to Save the "Past" in the "Future of the Internet" – April 2022 https://circleid.com/posts/20220507-how-to-save-the-past-in-the-future-of-the-internet-principles-the-washington-declaration

[98] Ibid

GEOPOLITICS OF INTERNET GOVERNANCE

The positions that are taken toward the Declaration and Internet governance are a reflection of broader geopolitics and trends that are currently at full play in the Ukraine invasion. Russia is engaged in a dangerous gamble to rewrite the architecture of European security, the West and its allies have joined forces and are testing Russia's resilience, but even the cohesiveness of the Western block should not be taken for granted. Meanwhile, China is caught in a complicated position and its choice is hard to predict. Meanwhile, most "countries from the Middle East, the Asian subcontinent, Southeast Asia, Latin America, and Africa" are acting cautiously and avoiding choosing a side. This will change once there is a clear winner or loser."[99] A decisive Russian triumph could give birth to a more multipolar world. Russia's collapse could lead to turmoil, civil war, or balkanization. Both scenarios entail a high degree of unpredictability.[100]

Adding to the complexity are changing attitudes and current trends. The Ukraine war demonstrated the strength of nationalism: "The invasion turned Ukraine into a cohesive nation despite previous differences in our society," Oksana Prykhodko, a Ukrainian journalist and the former member of the European Regional At-Large Organization (EURALO) at ICANN, said in an interview with the author in June 2022 during ICANN74. [101] While the increasing ostracism of Russia has encouraged widespread popular resentment towards the West among Russians.[102] At the same time, the increasing ostracism of Russia has encouraged widespread popular

[99] Jose Miguel Alonso-Trabanco, SITUATION REPORTS, A World Remade? Lessons from the Ukraine War - June, 2022 https://www.geopoliticalmonitor.com/a-world-remade-lessons-from-the-ukraine-war/
[100] Ibid
[101] My interview with Oksana Prykhodko, Ukrainian journalist and the former Secretariat of EURALO at ICANN, ICANN74, June 2022
[102] Jose Miguel Alonso-Trabanco, SITUATION REPORTS, A World Remade? Lessons from the Ukraine War - June, 2022
https://www.geopoliticalmonitor.com/a-world-remade-lessons-from-the-ukraine-war/

resentment toward the West among Russians. Meanwhile, the pandemic has sharpened the tension between globalization and sovereignty, climate change has become visible, and the need for global action is more real than ever. Finally, the war in Ukraine has further exposed the polarized global order and its inability to apply its long-standing tools of international law. Add to this complex mix the U.S. versus China battle over hardware and technology. Consequently, the internet governance ecosystem that has been formed on the basis of a globalized world is suffering. This unfortunate situation is manifested in the posturing of nation-states toward the declaration.

The signatories to the Declaration are the US, all EU countries, Canada, Japan, New Zealand, and Australia, and also some post-colonial or developing countries concerned about issues of sovereignty such as Argentina, Uruguay, and Senegal. While the geopolitical divide is very visible and runs across democratic lines, it is an oversimplification to treat this as a bipolar dispute over liberal versus authoritarian approaches. As mentioned, the United States and Europe alliances should not be taken for granted considering the important differences that exist within the liberal democratic bloc. We also see some of the G77 nations that used to be non-aligned, now feel the moral obligation to choose sides, especially in issues related to technology. Naturally, these nation-states are acting in their perceived national interest, but to what extent their perceptions will prove accurate considering that the technology is new, and these states are still struggling to understand and define their interests.[103]

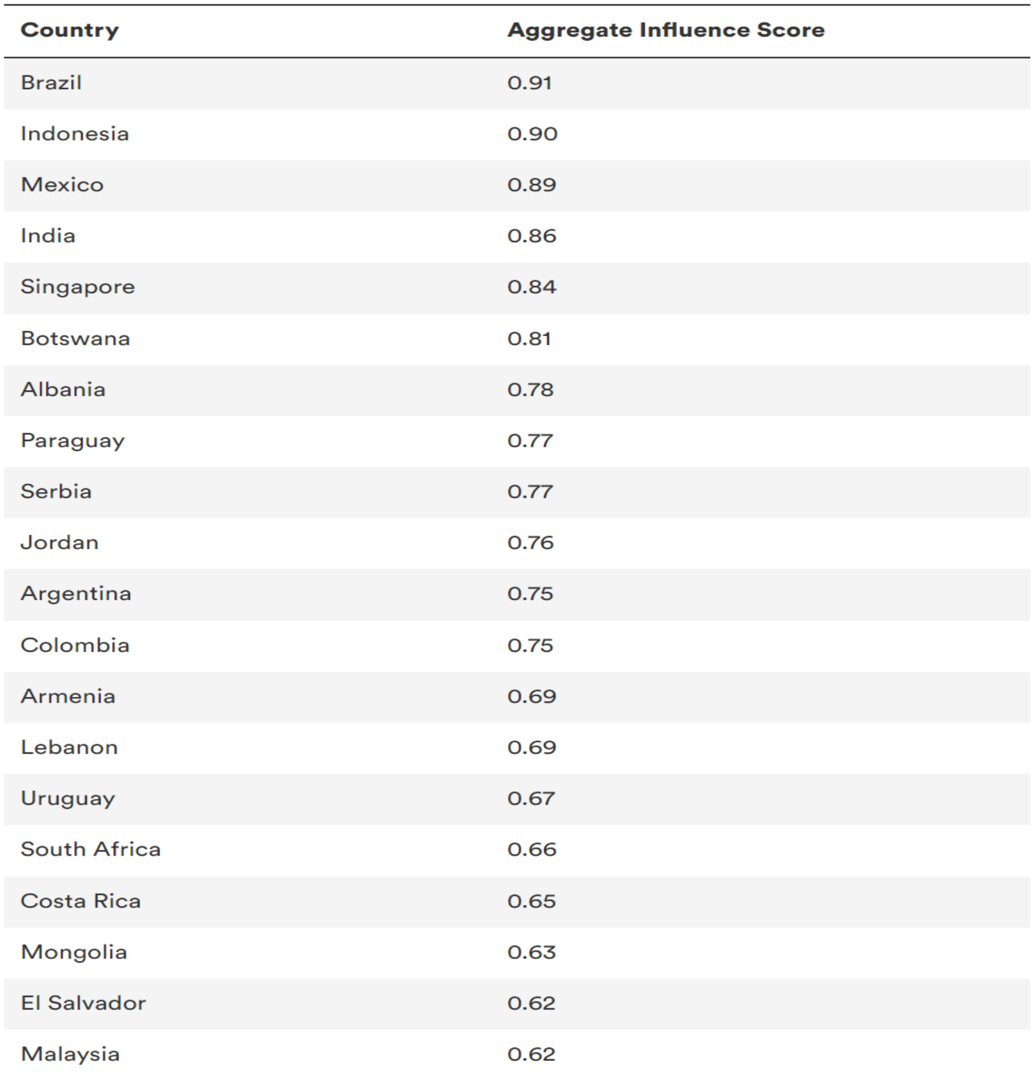
But what will make the critical difference are the “digital deciders” or “swing states” —countries that until now have not assumed a solid position about the future of the Internet.[104] Figure 3. shows the top twenty digital decider nation-states with the degree of their influence.

[103] Heli Tiimaa-llaar, America Council on Germany, Panel discussion: Cyber and Tech Dimension of Russian War on Ukraine - May 6 2022
https://www.youtube.com/watch?v=ORZPniwJFk8&ab_channel=AmericanCouncilonGermany

[104] Robert Morgus, Jocelyn Woolbright, Justin Sherman; The Digital Deciders – Oct 2018
https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/analyzing-the-clusters

"The Influence Score combines the international internet policy participation score and the international political influence score and is meant to provide insight into which countries may have an outsized impact or influence over international internet policy."

Figure 3: Top Twenty Digital Deciders Nations



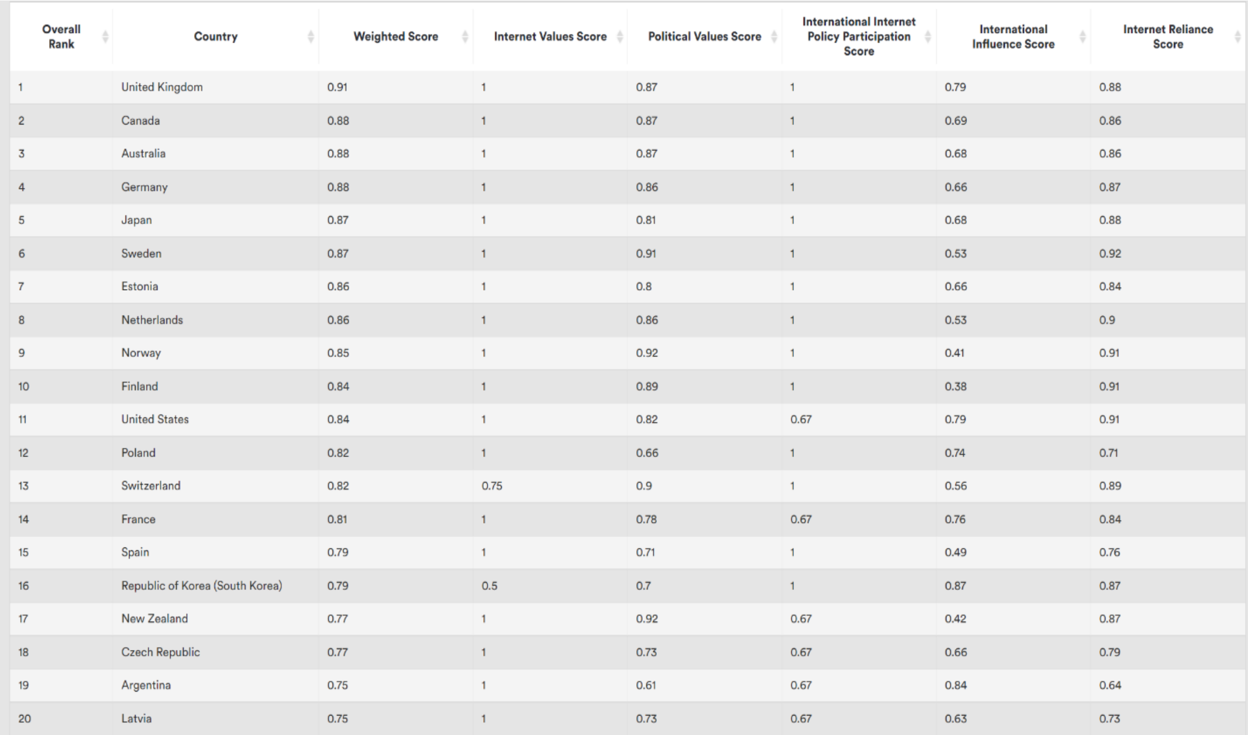
Country	Aggregate Influence Score
Brazil	0.91
Indonesia	0.90
Mexico	0.89
India	0.86
Singapore	0.84
Botswana	0.81
Albania	0.78
Paraguay	0.77
Serbia	0.77
Jordan	0.76
Argentina	0.75
Colombia	0.75
Armenia	0.69
Lebanon	0.69
Uruguay	0.67
South Africa	0.66
Costa Rica	0.65
Mongolia	0.63
El Salvador	0.62
Malaysia	0.62

Source: The Digital Deciders [105]

[105] Robert Morgus, Jocelyn Woolbright, Justin Sherman; The Digital Deciders – Oct 2018
https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/analyzing-the-clusters

Figure 4 – Top Twenty Influential Nation States

Values: Libertarian (1) -> Authoritarian(0)



Overall Rank	Country	Weighted Score	Internet Values Score	Political Values Score	International Internet Policy Participation Score	International Influence Score	Internet Reliance Score
1	United Kingdom	0.91	1	0.87	1	0.79	0.88
2	Canada	0.88	1	0.87	1	0.69	0.86
3	Australia	0.88	1	0.87	1	0.68	0.86
4	Germany	0.88	1	0.86	1	0.66	0.87
5	Japan	0.87	1	0.81	1	0.68	0.88
6	Sweden	0.87	1	0.91	1	0.53	0.92
7	Estonia	0.86	1	0.8	1	0.66	0.84
8	Netherlands	0.86	1	0.86	1	0.53	0.9
9	Norway	0.85	1	0.92	1	0.41	0.91
10	Finland	0.84	1	0.89	1	0.38	0.91
11	United States	0.84	1	0.82	0.67	0.79	0.91
12	Poland	0.82	1	0.66	1	0.74	0.71
13	Switzerland	0.82	0.75	0.9	1	0.56	0.89
14	France	0.81	1	0.78	0.67	0.76	0.84
15	Spain	0.79	1	0.71	1	0.49	0.76
16	Republic of Korea (South Korea)	0.79	0.5	0.7	1	0.87	0.87
17	New Zealand	0.77	1	0.92	0.67	0.42	0.87
18	Czech Republic	0.77	1	0.73	0.67	0.66	0.79
19	Argentina	0.75	1	0.61	0.67	0.84	0.64
20	Latvia	0.75	1	0.73	0.67	0.63	0.73

Source: The Digital Deciders [106]

Figure 4, shows details of top digital infuncers' scoring system. The overall scoring system in this figure is based on five factors:

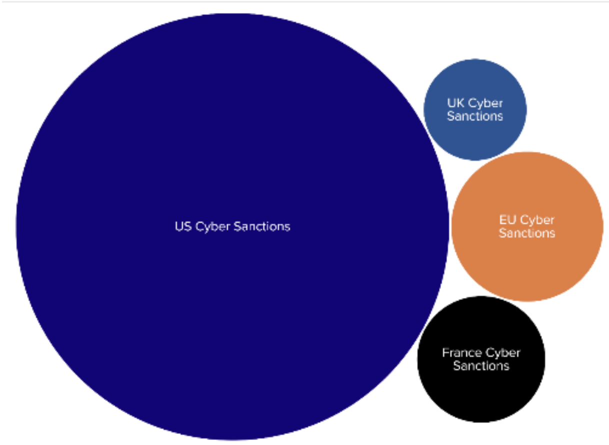
- Values that govern their Internet, from liberal and democratic to authoritarian tendencies.
- Overarching political values, from liberal and democratic to authoritarian tendencies.
- International/regional participation/involvement in Internet policy processes and debates.
- International/regional influence on all political and policy issues.
- Internet reliance on commerce, governance, and broader societal interaction.

[106] Robert Morgus, Jocelyn Woolbright, Justin Sherman, The Digital Deciders – Oct 2018 https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/

MOVING FORWARD

As presented in this brief discussion, a single overarching governance regime for cyberspace seems unlikely any time soon. “A good deal of fragmentation exists now and is likely to persist”.[107] Yet, it is crucial to set cyber rules, and considering the escalating geopolitical tensions and ensuing confusion over the Ukrainian government’s request, rules for digital sanctions seem to be a timely point to start. As Figure 5 shows, despite the fact that cyber sanctions are a new domain, they have become very popular with governments around the world.

Figure 5: Governments Sanctions



Source: Castellum.AI • Data reflect cyber sanctions on April, 2022.[108]

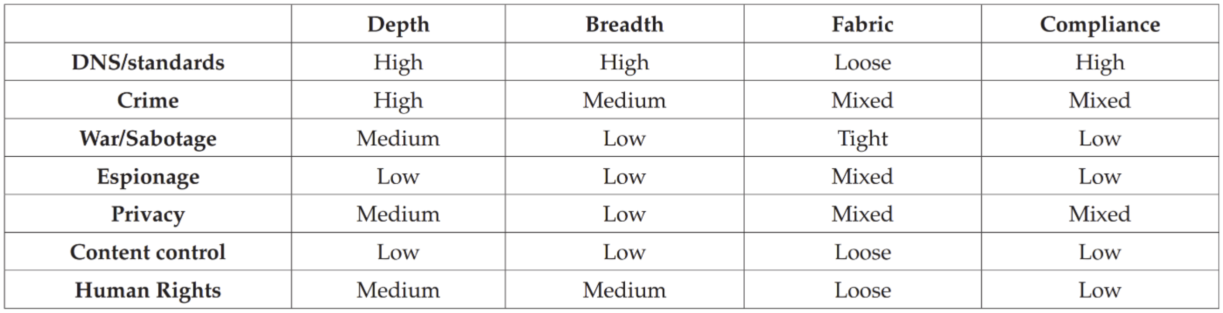
As discussed under the splinternet section of this paper, cyber sanctions that are not well thought out could have unintended consequences with a seismic impact. In producing a roadmap, it is critical to set up a process dedicated to establishing a comprehensive strategy.

[107] Joseph S. Nye, Jr, The Regime Complex for Managing Global Cyber Activities – May 2014 https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf
[108] Charles Lichfield, Maia Nikoladze, Sophia Busch and Castellum.AI - Atlantic Council – 2022 https://www.atlanticcouncil.org/blogs/econographics/global-sanctions-dashboard-russia-and-beyond/

Equally important are core principles and standards, and the US Declaration document, discussed earlier has listed five core principles that have been embedded in the DNS of the Internet from its early days. That said, the Internet is a relatively new and complex technology, and its frontiers are imagined and owned by the private sector. Its infrastructure doesn't lend itself easily to national borders. To avoid unintended consequences, the already well-established multistakeholder model of Internet governance must be the guideline.

Next is the difficult task of selecting cyber sanction measures and mechanisms. Sanctions have been levied by governments throughout history, and that long history provides lessons. . For example, appropriate scope, feasibility, effectiveness, targetability, and collective sense of responsibility are required in order to minimize detrimental consequences. In making a roadmap for sanctions, it is "useful to look at cyber issues in terms of four dimensions: depth (the hierarchical coherence of a set of rules or norms), breadth (the scope of the numbers of state and non-state actors that have accepted a set of norms), fabric (the mix of state and non-state actors in an issue area), and compliance.[109]

Figure 6 Issues in Cyber Regime Complex



	Depth	Breadth	Fabric	Compliance
DNS/standards	High	High	Loose	High
Crime	High	Medium	Mixed	Mixed
War/Sabotage	Medium	Low	Tight	Low
Espionage	Low	Low	Mixed	Low
Privacy	Medium	Low	Mixed	Mixed
Content control	Low	Low	Loose	Low
Human Rights	Medium	Medium	Loose	Low

Source: *The Regime Complex for Managing Global Cyber* Activities [110]

[109] Joseph S. Nye, Jr, The Regime Complex for Managing Global Cyber Activities – May 2014 https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf
[110] Ibid

The Internet ecosystem is extremely volatile, given rapid technological change, lacks coherence, and has loose coupling among issues. However, those same characteristics offer flexibility and adaptability, which are critical in this complex context where many actors with different interests interact. It permits actors to cooperate in some areas despite disagreements in others, and enables them to adjust to uncertainty. When it comes to international commitments, the implementation is often interdependent [not sure what "interdependent" means here], yet governments vary widely in their interest and ability to implement them. Here again, adaptability and flexibility make it possible.[111]

In conclusion, it is important to note that the current crisis in Internet governance is manifested in the post-pandemic environment that has expedited the transformation to the digital age. It also unfolds at a time of escalating geopolitical tensions the outcome of which is unclear, as is the geopolitical configuration that will eventually arise from it. Would it favor the Western bloc – undergirded by American leadership – or the Eurasian axis of continental powers? In any event, it is worth remembering that "the balance of power – a geopolitical concept based on a Newtonian understanding of physics – is never static."[112]

It is within this chaotic geopolitical context that Internet governance has to define itself. This is a significant moment, as decisions about the Internet's role in geopolitics and in our society are all coming under renewed scrutiny, and the outcome could be determinant not just for the technology but also for our democratic values and lifestyles. Never before has safeguarding the Internet's apolitical position and its principles of "one, open, universal, and accessible Internet" been more crucial. The Internet is an extraordinary human achievement and the defining technology of our time, which must be safeguarded before it is too late.

[111] Ibid
[112] Ibid

APPENDIX

RESPONSE TO RUSSIA'S AGGRESSION AGAINST UKRAINE

May 2022

ACTIONS BY TECH GIANTS

(listed in alphabetical order)

Adobe

General response: halt all new sales of Adobe products and services.
Update: Adobe has not put forth any additional sanctions. Its sales are still halted.

Mendelovich, Yossy. “Adobe and Avid Ban Russia: Stop All Sales and Support.” *Y.M.Cinema Magazine*.
March 6, 2022.
https://ymcinema.com/2022/03/06/adobe-and-avid-ban-russia-stop-all-sales-and-support/

- Adobe halted all new sales of its products and services and terminated previous access to Adobe Creative Cloud to Russian government-controlled media outlets.
- Donated $1 million in direct aid and military assistance.

Alphabet (Google and Youtube)

General response:

- Block Russian state media channels.
- Prohibit Russian state media from running ads and monetizing content on Youtube.
- Disable location tracking information to protect the community.
- Protect account security to combat malicious hacking activities.
- Provide protection against DDoS (Distributed Denial of Service attacks) for more than 100 Ukrainian news sites, including local news services.

Update: Alphabet has also not imposed new sanctions, but Russia has fined Google News for alleged “fake news.”

“Russia fines Google over Ukraine 'fakes', far-right content - TASS.” *Reuters*. April 21, 2022.
https://www.reuters.com/business/media-telecom/russia-fines-google-over-youtube-fakes-tass-2022-04-21/

- Russia accused and fined Google 11 million roubles ($137,763) for news content and YouTube videos sponsored or posted by “far-right groups.”
- There has been no response from Google.

Vincent, James. “YouTube Blocks Russian News Channels RT and Sputnik in Europe.” *The Verge*. March 1, 2022.
https://www.theverge.com/2022/3/1/22956114/youtube-blocks-russian-media-rt-russia-today-sputnik-europe

- YouTube blocked Russian news channels RT and Sputnik across Europe.
- This move can prevent revenue generation via advertising and restricts access to these channels in general.

Fung, Brian. “Google Follows YouTube in Cutting Off Ad Revenue to Russian State Media.” *CNN Business*.
February 28, 2022.
https://www.cnn.com/2022/02/28/tech/google-russia-media-cut-off-ad-revenue-intl-hnk/index.html

- Google doesn’t allow Russian state media outlets to run ads on its platform.
- This announcement came only a day after YouTube’s decision.

Amazon

General response:

- Discontinue shipments, or halt sales and other revenue streams starting March 8.
- Provide cybersecurity and logistics support for Ukraine.

Update: Amazon has not put forth any new sanctions. It continues to halt all sales and shipments, but there are no logistics made available on the cybersecurity support that it has provided.

Spangler, Todd. "Amazon Shuts Off Prime Video in Russia, Halts Product Shipments to Country Amid
Ukraine War." *Variety*. March 9, 2022.
https://variety.com/2022/digital/news/amazon-suspends-prime-video-russia-shipments-1235199942/

- After being criticized for providing logistical support and not giving up profits, Amazon halted product shipments and shut down Prime video access on March 8.
- Amazon will also cease shipment of retail products and its video game, "New World," to customers in Russia and Belarus.
- Merchants will no longer be accepted as Amazon third-party sellers.
- Amazon no longer accepts new Russia or Belarus-based customers for cloud computing services.

Weise, Karen. "Amazon Web Services Blocks New Sign-Ups from Russia and Belarus." *The New York*
Times. March 8, 2022.
https://www.nytimes.com/2022/03/08/technology/amazon-web-services-russia.html
Amazon has stopped letting customers in Russia and Belarus open new cloud computing accounts prior to its official announcement on March 8, 2022.

Reuters. "Amazon CEO Pledges Logistics, Cybersecurity Support for Ukraine." *Reuters*. March 2, 2022.
https://www.reuters.com/technology/amazon-ceo-pledges-logistics-cybersecurity-support-ukraine-2022-03-03/

Amazon is using its logistics capability to get supplies to those in need, and cybersecurity expertise to help governments and companies as part of its support for Ukraine.

Apple

General response:

- Pause all product sales.
- Services:
  - Apple Pay has been limited.
  - Disabled traffic, live incidents, as well as location tracking, in fear of attacks on population-dense areas.
- Removed applications of Russian state-controlled media, Russian Times (RT), and Sputnik.

Update: Apple's original sanctions were quite extensive. It has put forth no new sanctions.

Goode, Lauren. "Apple Stops Sales in Russia — and Takes a Rare Stand." *Wired*. March 1, 2022. https://www.wired.com/story/apple-russia-iphone-ukraine-traffic-maps-rt-sputnik-app-store/

- Apple paused all product sales through Apple stores in Russia.
- On the software front, Apple limited certain services, including Apple Pay and location tracking in its Maps app, and removed Russian news apps from its App Stores in countries outside of Russia.
- Apple is the last tech company to take a stand.

Chinese Brands (Huawei, Xiaomi, Alibaba, Tiktok, etc.)

General response: no response. However, China-based TikTok has suspended live streaming and blocked all new uploads from Russia. It has also conducted a review process for videos that went against its content guidelines.

Soon, Weilun. "How China's tech giants, from TikTok to Tencent, are reacting to Russia's invasion of
Ukraine." *Insider*. April 13, 2022. https://www.businessinsider.com/how-chinas-tech-giants-reacting-to-ukraine-crisis-tiktok-tencent-2022-3

- March 6: users residing in Russia are unable to live stream or upload new content to the global platform. They are also only allowed to watch videos uploaded to the Russian platform.
- Removed 41,191 videos from February 24 to March 31.
- Blocked Russian Times in the EU.

Horwitz, Josh, and Brenda Goh. "Analysis: Chinese Brands Stay Put in Russia for Now Despite Western
Exodus." *Reuters*. March 6, 2022. https://www.reuters.com/business/chinese-brands-stay-put-russia-now-despite-western-exodus-2022-03-04/

- Brands involved include Huawei, Xiaomi, Alibaba, Didi Chuxing (a ride-sharing app similar to Uber, which announced that it would pull out of Russia but later revoked its decision without explanations), Lenovo, Honor, and others. As of the publication of this article, none of the companies has pulled out of the Russian market; neither did they publicly announce any decisions or responses to the situation.
- Echoes Beijing's stance, refraining from explicitly criticizing Moscow's actions and blaming NATO expansion for the crisis, urging diplomatic talks to resolve the situation.

Cisco

General response: stop all business operations (sales and services) in Russia and Belarus, and offer cyber support.
Update: Cisco has not put forth additional sanctions.

Narcisi, Gina. “Cisco Stops Business In Russia, Ups Security Efforts In Ukraine.” *CRN*. March 8, 2022.
www.crn.com/news/networking/cisco-stops-business-in-russia-ups-security-efforts-in-ukraine

- Cisco has stopped all business operations, including sales and services, in Russia and Belarus for the foreseeable future.
- It is also offering auto-renewals and Webex meetings free of charge for Ukrainian customers.
- Cisco enabled security layers to protect Ukrainian organizations and infrastructure from Russian cyberattacks, monitoring critical organizations 24/7 through Cisco Talos.
- Established a Ukraine Humanitarian Assistance Fund.

Mukherjee, Spuantha, and Paul Sandle. “Cisco CEO Says Quarter of Staff in Ukraine Have Left.” *Reuters*. March 1, 2022.
https://www.reuters.com/business/cisco-ceo-says-quarter-staff-ukraine-have-left-2022-03-01/

- Cisco helped a quarter of its employees in Ukraine to evacuate the conflict zone.
- Those who decided to remain have been offered support.

Coinbase

General response: will only freeze Russian crypto if legally bound.
Update: Coinbase froze accounts and complied with EU sanctions.

Sundararajan, Sujha. "Russian crypto users face another blow from Coinbase." *Yahoo! Finance*. May 9,
2022.
https://finance.yahoo.com/news/russian-crypto-users-face-another-095306339.html#:~:text=Coinbase%20to%20block%20Russian%20user%20accounts%20under%20EU%27s%20sanctions&text=Per%20the%20local%20business%20news,future%20will%20also%20be%20blocked

- 25k accounts under concerns that cryptocurrency would be used to evade sanctions.
- Compliance with EU's sanctions: Warned certain Russian accounts that "Until May 31, 2022, you must withdraw all funds from your account or provide us with special documents that confirm that you do not fall under these sanctions. Failing to do so, your crypto assets may be frozen."

Brooks, Khristopher J. "Cryptocurrency Companies Resist Pressure to Close Russian Accounts." *CBS News*. Last updated March 7, 2022.
https://www.cbsnews.com/news/coinbase-binance-freeze-accounts-russia-ukraine/.

- Coinbase has been hesitant to pull out of the Russian market as "ordinary Russians are using crypto as a lifeline."
- It stated that "if the US government decides to impose a ban, we will, of course, follow those laws" in the CEO's tweets.

Barrabi, Thomas. "Coinbase Blocks 25k Russia-Linked Crypto Addresses Over 'Illicit Activity.'" *The New*
York Post. March 7, 2022.
https://nypost.com/2022/03/07/coinbase-blocks-25k-russia-linked-crypto-addresses/

- These blocks are not a direct response to the Ukrainian crisis but due to reports of illicit activities, tackling concerns that cryptocurrencies can be used to evade sanctions.
- The blocks were shared with the government to "further support sanctions enforcement."

Intel

General response:

- Condemned Russia's actions and suspended all shipments.
- Ceases supply of semiconductor (microchip) devices to cut off military and non-military usage.

Update: Intel has suspended all business in Russia and essentially exited the Russian market.

Lee, Timothy B. "Intel suspends all operations in Russia 'effective immediately." *ArsTechnica*. April 6.
2022.
https://arstechnica.com/tech-policy/2022/04/intel-suspends-business-operations-in-russia-over-ukraine-war/

- Suspends all business operations "effective immediately" on April 5.
- Such a decision is mainly due to sweeping "Western sanctions that have made it difficult for global companies to operate in Russia."

White, Monica J. "Intel Joins List of Companies to Halt Shipping to Russia." *Digital Trends*. March 4, 2022.
https://www.digitaltrends.com/computing/intel-stops-shipping-to-russia-and-belarus/

- Suspends all shipments to customers in Russia and Belarus.
- Raised funds for relief efforts ($1.2 million on March 3).

Meta (Facebook, WhatsApp, Instagram)

General response:

- Block RT and Sputnik access to Facebook and Instagram, and any access to these two channels across the EU.
- Removed the option to monetize content on their platform.
- Blocked Russian state media from running ads, demoting their content, and fact-checking posts on the conflict. Meta has already been facing restrictions in Russia due to non-alignment with official Russian rhetoric on the conflict.
- Locked down accounts of state-sponsored trolls and disabled information warfare networks.
- Imposed additional account privacy and security protections to prevent targeting social media accounts of civil society and the protesters.

Update: Meta's original sanctions were quite extensive. It has put forth no new sanctions.

"Meta's Ongoing Efforts Regarding Russia's Invasion of Ukraine." *Meta*. February 26, 2022. https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/

- Established additional account privacy and security protections.
- Established monitoring operations to combat ongoing disinformation campaigns.

Frater, Patrick. "Meta Restricts Russian State Media on Facebook, WhatsApp, and Instagram Following Invasion of Ukraine." *Variety*. March 1, 2022. https://variety.com/2022/digital/global/meta-restricts-russian-state-media-1235192727/

- Meta restricts access to Russian state media within the European Union across all its subsidiary social media platforms.
- Meta has been contacted by the EU and Ukrainian government on limiting potential Russian disinformation regarding the conflict.

Microsoft

General response:

- Removed Russian state-owned media outlet, RT's mobile apps from the Windows store and de-ranked RT and Sputnik on Bing, its web browser.
- Banned advertisements from Russian state-sponsored media.
- Has been and will be monitoring digital space, and advising the Ukrainian government on attacks targeting its digital infrastructure.
- Halted new sales since March 5.

Update: Microsoft has put forth no new sanctions.

Smith, Brad. "Digital Technology and the War in Ukraine." *Microsoft*. February 28, 2022. https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/

- Microsoft's original statement did not mention sales and shipments.
- *Protecting Ukraine from cyberattacks*: monitor cyberspace, alert the government and provide defensive advice regarding attacks targeting Ukrainian critical infrastructure, then share intelligence with NATO officials and the American government.
- *Protection from state-sponsored disinformation campaigns*: Reduce the exposure of Russian state propaganda by not displaying RT and Sputnik content, removing corresponding apps, and de-ranking the content on Bing.
- *Support for humanitarian assistance*: provide support for humanitarian organizations and activate the Microsoft Disaster Response Team.

Bishop, Todd, and Taylor Soper. "Microsoft Suspends Sales of Products and Services in Russia, Condemns
'Unlawful' Invasion of Ukraine." *GeekWire*. March 4, 2022. https://www.geekwire.com/2022/microsoft-suspends-sales-of-all-products-and-services-in-russia-condemns-unlawful-invasion-of-ukraine/

- This came a few days after its initial response that failed to mention its operations in Russia.
- Microsoft will suspend all new sales of its products and services and stop "many aspects" of its business in Russia in line with government sanctions.

Samsung

General response:

- Suspend shipments of both tech devices and microchips into Russia, but will continue to operate its factories.
- Donate $6 million to Ukraine Red Cross

Update: Samsung has not imposed new sanctions and has remained cautious to be as clear-cut as its Western counterparts.

Byung-Wook, Kim. "Samsung joins Russia sanctions, donates $6m to Ukraine." *The Korea Herald*. March 6, 2022. http://www.koreaherald.com/view.php?ud=20220306000101

- Samsung donated $6 million to the Ukraine Red Cross, including $1 million in consumer electronics.
- Samsung factories located in Russia continue to be in operation.

Kim, Sohee. "Samsung Suspends Shipments of Phones, Chips to Russia." *Bloomberg*. March 4, 2022.

https://www.bloomberg.com/news/articles/2022-03-04/samsung-suspends-shipments-of-phones-chips-to-russia

- Samsung suspended product shipments to Russia, ranging from chips to smartphones and other consumer electronics.
- This statement was emailed to Bloomberg and not publicly announced.

Sony (Playstation)

General response:

- To pause all theatrical releases and suspend all operations of PlayStation stores in Russia.
- To suspend all software and hardware shipments.
- Unclear whether all operations have been suspended.

Update: Sony has not imposed new sanctions.

Loh, Matthew. "Disney, Warner Bros, and Sony are Pausing Theatrical Releases in Russia in Response to the Invasion of Ukraine." *Business Insider Africa*. March 1, 2022. https://africa.businessinsider.com/entertainment/disney-warner-bros-and-sony-are-pausing-theatrical-releases-in-russia-in-response-to/ydhm9w0

- Sony paused theatrical releases in Russia.
- The statement immediately followed Disney and Warner Media announcements.

Franklin, Jonathan. "Sony Halts PlayStation Sales in Russia Due to Ukraine Invasion." *NPR*. March 9, 2022.

https://www.npr.org/2022/03/09/1085611369/sony-playstation-russia

- Sony stopped all sales of its PlayStation consoles and software in Russia.
- The company suspended all shipments to Russia and closed its PlayStation Stores.

Tesla

General response: sales are to continue as Russia is a large consumer of Tesla vehicles.
Update: no new sanctions were imposed, and Tesla was revealed to continue aluminum imports from a Russian company.

Kolodny, Lora. “Tesla has bought aluminum from Russian company Rusal since 2020, showing how war
complicates supply chain.” *CNBC*. March 14, 2022.
https://www.cnbc.com/2022/03/14/tesla-has-bought-aluminum-from-russian-supplier-rusal-since-2020.html

- Tesla continues to import aluminum from a Russian company.
- Rusal, the company in question, was previously subject to U.S. sanctions but those were lifted by Trump’s administration.

Morrison, Sara. “Does Ukraine Really Need Elon Musk’s help?” *Vox*. March 4, 2022.
https://www.vox.com/recode/22958373/ukraine-russia-starlink-spacex-elon-musk

- Elon Musk personally sent Starlink satellite dishes to ensure internet connectivity in Ukraine.
- There are potential pitfalls as Russians would be able to triangulate the signal and attack Ukrainians using these services on the ground.

Falcon, Russell, and Nextar Media Wire. “Tesla Paying Ukrainian Employees Who are Called Back to Fight Russia: Report.” *Wavy*. March 10, 2022.
https://www.wavy.com/news/national/tesla-paying-ukrainian-employees-who-are-called-back-to-fight-russia-report/#:~:text=While%20Tesla%20doesn't%20have,to%20respond%20to%20the%20requests

- Tesla employees will retain employment and be paid up to 3 months in compensation if they are conscripted to fight in Ukraine.
- Ukrainian Tesla drivers have free access to Tesla Superchargers in Poland, Slovakia, and Hungary to aid their evacuation.
- Tesla has not responded to whether it will suspend sales (it currently remains unaffected), and Musk has disabled its PR department to avoid journalists’ inquiries.

General Sources

"The Ukraine Corporate Index Tracks Companies' Response to Russia's Invasion." *The Good Lobby*. Last

updated March 9, 2022.
https://www.thegoodlobby.eu/2022/03/04/ukraine-corporate-index/

- A corporate index tracker that synthesizes information from news sources and presents a list, (updated when there's new information available), to provide a relatively comprehensive overview of the response from major corporations to the Conflict.
- Used this source as a jumping board to identify the corporations.

"How Are the Big Tech Companies Responding to the Invasion of Ukraine?" *Sky News*. March 7, 2022.

https://news.sky.com/story/how-are-the-big-tech-companies-responding-to-the-invasion-of-ukraine-12555497

- Additional information on several corporations that Ukraine's prime minister, Mykhailo Federov, directly appealed to for aid.
- Identified how critical technology companies are in times of conflict, both as a means to disseminate information to a large audience, as well as a potential channel for corruption, propaganda, and manipulation.
- Used for Apple, Google (Alphabet), Meta, and Microsoft.

Nicholls. Rob. "The Power of Tech Giants: How They are Sanctioning Russia Over Ukraine War." *Business Standard.* Last updated March 7, 2022.
https://www.business-standard.com/article/international/the-power-of-tech-giants-how-they-are-sanctioning-russia-over-ukraine-war-122030700258_1.html

- Focuses on responses from the Big Five tech companies.
- Used for Google (Alphabet), Apple, Meta, Amazon, and Microsoft.

Gain, Vish. "How the Tech Sector is Responding to Russia's Invasion of Ukraine." The *Silicon Republic*.

February 28, 2022.
https://www.siliconrepublic.com/business/tech-response-ukraine-social-media-apps-infosec-crypto

- Provides more information and analysis behind these self-imposed, voluntary tech sanctions.
- Used for Google (Alphabet), Apple, Meta, and other social media platforms.

ACTIONS BY KEY INTERNET INSTITUTIONS

On February 28th, Ukraine's Vice Prime Minister, Mykhailo Fedorov, sent a request to various internet governance institutions including, ICANN and RIPE NCC to cut off Russia from the Internet. His appeal received a collective sympathetic no. These organizations pointed out that they do not have power by law, rather they are independent international bodies that work by agreement, not by force, and that their function is to ensure the functionality of the internet.

Internet Corporation for Assigned Names and Numbers (ICANN)

- **Fedorov's letter to ICANN:** https://technopolitics.org/wp-content/uploads/2022/05/Ukraine-ICANN.pdf
- **ICANN's response:** https://technopolitics.org/wp-content/uploads/2022/05/ICANN-Response.pdf

Réseaux IP Européens Network Coordination Centre (RIPE NCC)

General response: echoed ICANN's statement, a sympathetic "no."

- **Fedora's letter to RIPE NCC:** https://technopolitics.org/wp-content/uploads/2022/05/Ukrainian-RIPE-NCC.pdf
- **RIPE NCC Response:**
    - https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government
    - https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government#:~:text=Dear%20Vice%20Prime%20Minister%2C,the%20heart%20of%20the%20Internet
    - https://www.ripe.net/participate/member-support/the-ripe-ncc-and-ukraine-russia
    - "RIPE NCC Executive Board Resolution on Provision of Critical Services." *RIPE NCC*. March 1, 2022. https://www.ripe.net/publications/news/announcements/ripe-ncc-executive-board-resolution-on-provision-of-critical-services
        - RIPE NCC is a regional internet registry for Europe, the Middle East, and parts of Central Asia.
        - "The means to communicate should not be affected by domestic disputes, international conflicts or war."
        - RIPE NCC must remain neutral to guarantee equal treatment and provide authoritative, free-from-bias information.

Internet Society

Andrew Sullivan, president of the Internet Society called the request the “antithesis of how the internet was designed and meant to function.”

Electronic Frontier Foundation (EFF)

General response: echoed ICANN’s statement, and supports the decision of upholding the global internet.

McSherry, Corynne, and Konstantinos Komaitis. “Wartime Is a Bad Time To Mess With the Internet.”

Electronic Frontier Foundation. March 3, 2022. https://www.eff.org/deeplinks/2022/03/wartime-bad-time-mess-internet

- Remaking fundamental internet infrastructure protocols can lead to dangerous and long-lasting consequences.
- Deprives people of a powerful tool (or a fundamental human right) to share information.
- Sets a dangerous precedent for independent, autonomous organizations to interfere with politics.
- Compromises security and privacy for everyone.
- Undermines trust in the network and policies upon which it is built.

General Sources

Moss, Sebastian. “Ukraine Invasion Brings Internet Governance Neutrality Question into Focus.” *Data*

Center Dynamics. March 3, 2022. https://www.datacenterdynamics.com/en/analysis/ukraine-invasion-brings-internet-governance-neutrality-question-into-focus/

- This article provides an evaluation of internet governance neutrality, primarily in response to RIPE NCC’s response to the Ukrainian plea to cut off access to all Russian domains.
- It mentioned ICANN and RIPE NCC, but wasn’t able to identify other internet governance organizations that provided input, suggesting no additional organizations responded.

Wakefield, Jane. “Russia-Ukraine: Is Internet On Verge of Break-Up?” *BBC*. March 8, 2022. https://www.bbc.com/news/technology-60661987

- Provided an analysis of the implications of potentially cutting off internet access from Russia.
- Identified several institutions, including ICANN and EFF.

GOVERNMENTAL SANCTIONS

United States

General response:

- Oil refining sector: ban exports of refining technologies, making it more difficult for Russia to modernize its oil refineries.
- Banks: bar certain Russian banks from the SWIFT international payments system.
- Technology sector: wide restrictions on semiconductors, telecommunication, encryption security, lasers, sensors, navigation, avionics, and maritime technologies.

Update: the U.S. increased the scope of its sanctions to fully ban several Russian banks and Putin’s family and close colleagues. It has also exempted the internet communication providers from U.S. sanctions against Russia.

- Barred Russia from making debt payments with the $600 million in U.S. banks.
- Banned Russian oil and energy.

Moss, Sebastian. “US Treasury exempts Internet communication providers from Russia sanctions.” *Data Center Dynamics*. April 11, 2022. https://www.datacenterdynamics.com/en/news/us-treasury-exempts-internet-communication-providers-from-russia-sanctions/

- The US Treasury has exempted the provision of Internet communication services from US sanctions against Russia, an exemption welcomed by human rights and open access groups.
- Content delivery networks and web infrastructure companies have long opposed the restriction of the rights of Russian citizens to access the internet.
- Individuals: sanctions on Russian oligarchs and lawmakers

“U.S. Treasury escalates sanctions on Russia for its atrocities in Ukraine.” *U.S. Department of the*

Treasury. April 6, 2022. https://home.treasury.gov/news/press-releases/jy0705

- Full-blocking sanctions on Sberbank and Alfa-Bank, the largest government, and private-owned banks, respectively, and their subsidiaries.
- Individually targeted sanctions on Putin, Putin’s family (two adult daughters), Foreign Minister Lavrov and family (wife and daughter), and other Russian Security Council Members.

“War in Ukraine: West hits Russia with oil bans and gas curbs.” *BBC News*. March 9, 2022. https://www.bbc.com/news/world-us-canada-60666251

- The U.S. is completely banning all imports of Russian oil, gas, and energy.
- 8% of U.S. oil comes from Russia.

"What is SWIFT and Why Were Some Russian Banks Excluded From It?" *Al Jazeera*. February 27, 2022.
https://www.aljazeera.com/news/2022/2/25/what-is-swift-could-be-used-punish-putin

- Russia has the second-largest number of users in the Russian National SWIFT Association. There are 300 financial institutions in the system, which is more than half of Russia's financial institutions.
- Blocking Russia out of SWIFT can cripple its ability to trade with the rest of the world.
- The ban will slow down trade and make transactions costlier.

"FACT SHEET: United States, European Union, and G7 to Announce Further Economic Costs on Russia."
The White House. March 11, 2022.
https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/11/fact-sheet-united-states-european-union-and-g7-to-announce-further-economic-costs-on-russia/

- Revoking Russia's most-favored-nation status that comes along with its WTO membership.
- Denying borrowing privileges for Russia from the Bretton Woods institutions.
- Full-blocking sanctions on Russian elites and family members.
- Banning exports of luxury goods to Russia.
- Banning U.S. import of goods from signature sectors of Russia's economy, including seafood, vodka, and non-industrial diamonds.

Macias, Amanda, and Thomas Franck. "Biden Administration Expands Sanctions Against Russia, Cutting Off U.S. Transactions with Central Bank." *CNBC*. Updated March 1, 2022.
https://www.cnbc.com/2022/02/28/biden-administration-expands-russia-sanctions-cuts-off-us-transactions-with-central-bank.html

- Prohibits Americans from doing business with Russia's central bank and freezes the bank's assets in the U.S.
- These measures also target the National Wealth Fund of the Russian Federation and the Ministry of Finance of the Russian Federation.

European Union

General response:

- Oil refining sector: ban exports of specific refining technologies.
- Transportation: close airspace to Russian aircraft, including private jets of Russian oligarchs.
- Block Russian state-owned RT and Sputnik.
- Belarus: ban imports from mineral fuels to tobacco, wood and timber, cement, iron, and steel.
- Freeze European assets of Putin and foreign minister Sergey Lavrov.

Update:

- Energy sanctions: comprehensive phase-out by the end of 2022.
- Individual sanctions on military officers suspected of war crimes.
- Broad bans of Russian state-run broadcasters.

Kirby, Paul. "Ukraine war: EU plans Russian oil ban and war crimes sanctions." *BBC News*. May 4, 2022.
https://www.bbc.com/news/world-europe-61318689

- Energy sanctions:
  - Halt Russian coal imports by August 2022.
  - Russian crude oil to be phased out in six months.
  - Refined oil products are to be phased out by the end of 2022.
  - Gas imports to be reduced by two-thirds by the end of 2022.
- Individual bans have been targeting suspected war criminals.

"EU restrictive measures against Russia over Ukraine (since 2014)." *European Council*. n.d.
https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/

The EU has adopted five packages of sanctions since the conflict began.

Monard, Eva, Renato Antonini, Guy Soussan, David O'Sullivan, Stefan Tsakanakis, Byron Maniatis, Elli
Zachari, and Charlotte Brett. "Update: EU Adopts Far-Reaching Sanctions following Russian Invasion of Ukraine." *Steptoe International Compliance Blog.* February 27, 2022.
https://www.steptoeinternationalcomplianceblog.com/2022/02/update-eu-adopts-far-reaching-sanctions-following-russian-invasion-of-ukraine/

- Targeted restrictions against specified individuals.
- Expanded financial measures aiming at cutting Russia's access to the EU capital markets.
- Trade restrictions target the energy and aviation sectors. Bans on most exports of dual-use items, as well as certain semiconductors and cutting-edge technologies from the EU to Russia.

"Ukraine: EU Agrees to Extend the Scope of Sanctions on Russia and Belarus." *European Commission*.
March 9, 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1649

- Limits Belarus' participation in the SWIFT system, similar to those of Russia.
- New restrictions on the export of maritime navigation and radio communication.
- Places limits on the movement and assets of oligarchs and politicians.

United Kingdom

General response:

- Impose sanctions on Russian banks, locking out Russia's Sberbank altogether.
- Freeze assets on all Russian lenders.
- Ban Russia's flagship airline Aeroflot from landing in the UK.
- Suspend dual export licenses.
- Ban exports of high-tech exports and selected parts of the extractive industry.

Update:

- Trade tariffs on platinum and palladium.
- Sanctions on individual Russian military generals for alleged war crimes.

M, Muvija. "UK sanctions Russian generals it says have 'blood on their hands'." *Reuters*. April 21, 2022.
https://www.reuters.com/world/uk/uk-sets-out-26-new-sanctions-against-russia-2022-04-21/
Asset freeze and travel bans on individual Russian military generals for alleged war crimes.

"New UK sanctions for Russia and Belarus." *BBC News*. March 9, 2022.
https://www.bbc.com/news/uk-61372302

- Import tariffs on £1.4bn of platinum and palladium, which are metals used for mobile phones and computers.
- Planned export bans on products worth more than £250m in sectors of the Russian economy that are most dependent on UK goods.

"War in Ukraine: West hits Russia with oil bans and gas curbs." *BBC News*. March 9, 2022.
https://www.bbc.com/news/world-us-canada-60666251

- In-line with the U.S. ban, the UK plans to phase out Russian oil imports by Dec. 2022.
- 6% of UK oil is imported from Russia.

Ruck, Michael E., and Rosie Naylor. "UK Imposes Further Sanctions in Response to Russia's Invasion of Ukraine." *K&L Gates*. February 25, 2022.
https://www.klgates.com/UK-Imposes-Further-Sanctions-in-Response-to-Russias-invasion-of-Ukraine-2-25-2022

- UK individuals and entities are now prohibited from any dealings with, or providing any funds to or for the benefit of, directly or indirectly, any of the Russian banks or individuals.
- Freezes assets of all major Russian banks, and excludes them from the UK financial system.

Foreign, Commonwealth & Development Office. "UK Sanctions Relating to Russia." *UK Government*.
Updated March 8, 2022. https://www.gov.uk/government/collections/uk-sanctions-on-russia.
Offers a comprehensive list of all UK-imposed sanctions on Russia.

Switzerland

General response:

- Adopt all EU sanctions, and freeze the assets of Russian individuals and assets.
- Sharp deviation from its traditional neutrality.

Update: Switzerland has continued to adopt all EU sanctions against Russia and Belarus.

"Swiss have frozen $8 billion in assets under Russia sanctions." *Reuters*. April 7, 2022. https://www.reuters.com/world/europe/swiss-have-frozen-8-billion-assets-under-russia-sanctions-2022-04-07/

- Switzerland has traditionally been a popular destination for Moscow's elite and a holding place for Russian wealth.
- It has frozen $8.03 billion in Russian funds and assets.

Reich, Philippe M., and Rolaz, Meera. "Situation in Ukraine: Switzerland tightens sanctions against
Belarus and Russia." *Sanctions News: A Blog by Baker McKenzie*. March 18, 2022. https://sanctionsnews.bakermckenzie.com/situation-in-ukraine-switzerland-tightens-sanctions-against-belarus-and-russia/

- Expansion of the Designated Parties List (resulting in asset freezes and travel restrictions).
- Further restrictions on dual-use and high-tech goods exports to Belarus.
- Prohibitions on the supply of various types of machinery to Belarus.
- Enhancement of the existing tobacco sector restrictions.
- Procurement restrictions on wood, cement, iron and steel, and rubber originating from Belarus.
- Introduction of numerous financial sanctions in line with those imposed against Russia.

Global Sanctions Team. "Switzerland Reinforces Its Sanctions Against Russia." *White & Case*. March 7, 2022.
www.whitecase.com/publications/alert/switzerland-reinforces-its-sanctions-against-russia

- Modeled after EU sanctions.
- Freeze assets in line with the EU.
- Ban listed individuals from entering Switzerland.
- Restricted exports of dual-use, high-tech, and aircraft-related goods as well as oil/gas equipment to Russia and Ukraine, and tightened various monetary and financial sanctions.

Japan

General response:

- Financial institutions and military equipment: sanction exports.
- Target individuals and financial institutions, freezing their assets.

Update:

- Targeted sanctions on individuals and related companies, including the prohibition of crypto transactions.
- Expelled eight Russian diplomats.
- Banned or restricted imports.

Kim, Victoria. "Japan dials up measures against Russia, aligning itself with the U.S. and Europe." *The New York Times*. April 9, 2022.
https://www.nytimes.com/2022/04/09/world/asia/japan-russia-ukraine.html

- Expelled eight Russian diplomats.
- Imposed a ban on Russian coal, and restrictions on imports including timber, vodka and machinery.

Ohashi, Koichiro. "Japanese financial sanctions on Russia over invasion into Ukraine." *The National Law*
Review. April 8, 2022.
https://www.natlawreview.com/article/japanese-financial-sanctions-russia-over-invasion-ukraine/

- Japan is in line with the international community with regard to imposing sanctions and asset freezes.
- Measures include prohibitions on payments via crypto assets.

Rich, Motoko, and Makiko Inoue. "Japan, Hesitant to Impose Sanctions on Russia in 2014, Embraces Them Now. One Reason: China." *The New York Times*. February 24, 2022.
https://www.nytimes.com/2022/02/24/world/europe/japan-russia-sanctions.html

- Prohibits Russia from issuing new sovereign bonds in Japanese markets.
- Bans trade with the breakaway republics in eastern Ukraine.
- Freezes the assets of representatives of those republics and bars them from receiving visas.

"Japan Freezes Assets of More Russian Officials, Oligarchs." *Al Jazeera*. March 8, 2022.
https://www.
aljazeera.com/economy/2022/3/8/japan-freezes-assets-of-dozens-of-russian-officials-oligarchs.

- Additional freezing of the assets of dozens more Russian and Belarusian officials and oligarchs.
- Bans exports of Russia-bound oil refinery equipment and Belarus-bound general-purpose items that could be used by its military.

South Korea

General response:

- Block Russian banks from the SWIFT international payments system.
- Tighten export controls against Russia by banning exports of strategic items (semiconductors).
- Release oil reserves to stabilize the international energy market and insulate prices against bans of exports of Russian oil.

Update: South Korea has continued to adopt U.S. and EU sanctions. However, it is notable to mention that South Korea has been criticized for being too mild on its approach to Russia.

Jun, Kwanwoo. “South Korea Bans Transactions With Russia’s Central Bank.” *The Wall Street Journal*.

March 7, 2022.
https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-07/card/south-korea-bans-transactions-with-russia-s-central-bank-96B5xib2OW41u03krYrp

- Banned transactions with Russia's central bank and sovereign wealth funds.
- Restricted exports of strategic and nonstrategic items to Russia.

Canada

General response:

- Cancel all export permits.
- Sanctions against 62 individuals and entities, including elites and major banks.
- Prioritize immigration applications for Ukrainians.

Update: Canada imposes sanctions on 203 additional individuals and their relationship to the annexation of the Donbas region.

"Canada imposes sanctions on 203 individuals complicit in attempted annexation of certain areas of
Donbas, Ukraine." *Government of Canada*. April 27, 2022. https://www.canada.ca/en/global-affairs/news/2022/04/canada-imposes-sanctions-on-203-individuals-complicit-in-attempted-annexation-of-certain-areas-of-donbass-ukraine.html

Imposed restrictions on 11 senior officials and 192 other members of the People's Councils of the so-called Luhansk and Donetsk People's Republics and froze their assets.

"Canadian Sanctions Related to Russia." *Government of Canada*. Updated March 10, 2022. https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/russia-russie.aspx?lang=eng

- Complete asset freeze against a comprehensive list of Russian elites.
- Prohibits any person in Canada and any Canadian outside Canada from importing specific petroleum products.

Czech Republic

General response:

- Ban Russian airlines from landing (its strategic central European location is leverage).
- Exit two international banks set up in the Soviet era.

Update: the Czech Republic adopts all EU, U.S., and NATO sanctions against Russia.

Saidel, Peter. “Czech Republic takes further steps to support Ukraine.” *The Wall Street Journal*. May 11,
2022. https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-05-11/card/czech-republic-takes-further-steps-to-support-ukraine-YU9NwDZ1L1hQRtKge360-YU9NwDZ1L1hQRtKge360

- The Czech Republic adopted a resolution in support of NATO and EU sanctions.
- It will accelerate its supply of weapons to the Ukrainian army and send troops to join NATO.

“Czech Government Announces A Series of Unilateral Sanctions Against Russia.” *Radio Prague International*. February 25, 2022. https://english.radio.cz/czech-government-announces-a-series-unilateral-sanctions-against-russia-8743153.

- Stopped issuing visas to Russian citizens and currently reviewing already issued residence visas for Russians living in the Czech Republic.
- Inspects Russian companies or companies with Russian owners in relation to the drawing of public funds in the Czech Republic.
- Speeds up the process of withdrawing from two post-Soviet banks - the International Bank for Economic Cooperation and the International Investment Bank - and will call on other EU members to do the same.

Australia

General response: target elite citizens and lawmakers and freeze assets.
Update: Australia has continued to add to its list of individuals and has also expanded sanctions to include state-owned corporations.

Jose, Renju. "Australia imposes more sanctions on Russian state-owned enterprises." *Reuters*. April 13,
2022. https://www.reuters.com/world/asia-pacific/australia-imposes-more-sanctions-russian-state-owned-enterprises-2022-04-14/

- Australia imposed targeted financial sanctions on 14 Russian state-owned enterprises.
- Companies involved include defense-related entities, shipping companies, Russian Railways, and electronic manufacturers.

Petterd, Anne. "Australia Announces Plans to Impose New Sanctions Upon Russia." *Global Compliance*
News. March 6, 2022. https://www.globalcompliancenews.com/2022/03/06/australia-announces-plans-to-impose-new-sanctions-upon-russia-23022022/

- Travel bans placed on individuals and government-related entities.
- Economic sanctions are imposed on Russian banks.
- Economic sanctions are imposed on the two independent Ukrainian regions, especially transport, energy, telecommunications, oil, gas, and mineral reserves sectors.

"Russia Sanctions Regime." *Australian Government Department of Foreign Affairs and Trade*. Accessed
on March 11, 2022. https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/russia-sanctions-regime#:~:text=Why%20are%20sanctions%20imposed%3F,extended%20in%202015%20and%202022
Prohibits the import of oil, refined petroleum products, natural gas, coal, and other energy products from Russia.

New Zealand

General response:

- Travel bans on Russia.
- Prohibit trade with Russian military and security forces.

Update:

- Increase tariffs for all imports from Russia and extend existing export prohibitions.
- Impose asset freezes on banks and financial institutions.

Mahuta, Hon Nanaia, and O'Connor, Hon Damien. "New Zealand to apply trade sanctions in response to
Russian atrocities." *New Zealand Government*. April 6, 2022. https://www.beehive.govt.nz/release/new-zealand-apply-trade-sanctions-response-russian-atrocities

- Apply 35% tariffs to all imports from Russia.
- Extend the existing export prohibitions to industrial products closely connected to strategic Russian industries.

"New Zealand imposes new sanctions on Russian banks." *Reuters*. April 18, 2022. https://www.reuters.com/world/asia-pacific/new-zealand-imposes-new-sanctions-russian-banks-2022-04-19/.

- Freeze assets of the central bank and the sovereign wealth fund.
- The asset freeze also applies to eight of Russia's largest banks and seven others with ties to oligarchs.

"New Zealand, South Korea Announce New Sanctions on Russia." *Al Jazeera*. March 7, 2022. https://www.aljazeera.com/economy/2022/3/7/new-zealand-south-korea-announce-new-sanctions-on-russia

- Freeze Russian assets in New Zealand.
- Prevent Russians and Russian companies from moving their money and assets to New Zealand to escape sanctions imposed by other countries.
- Stop superyachts, ships, and aircrafts from entering New Zealand waters or airspace.

General Sources

"What sanctions are being imposed on Russia over the Ukraine invasion?" *BBC News*. May 4, 2022. https://www.bbc.com/news/world-europe-60125659

- Includes all new updates, including prospective sanctions, by multiple states.
- Used as a jumping board for additional research.

Al Jazeera Staff. "List of Sanctions against Russia after it Invaded Ukraine." *Al Jazeera*. Updated March 3,
2022.
https://www.aljazeera.com/news/2022/2/25/list-of-sanctions-on-russia-after-invasion.

- Provides a comprehensive list of all sanctions imposed on Russia since the Ukrainian Crisis.
- Used as a jumping board for more in-depth research.

Moss, Sebastian. "U.S., Japan, Taiwan Impose Sanctions, Restrict Sales of Semiconductors and Telco
Equipment to Russia." *Data Center Dynamics*. February 25, 2022. https://www.datacenterdynamics.com/en/news/us-japan-taiwan-impose-sanctions-restrict-sales-of-semiconductors-and-telco-equipment-to-russia/.

- Moves to cut off Russia's access to technology, especially semiconductors used in software, and military and non-military technology.
- Used for the U.S. and Japan.

Rubio-Licht, Nat, Alex Eichenstein, Sarah Roach, and Veronica Irwin. "The War in Ukraine is Putting Tech — from Companies to Governments — to the Test." *Protocol.* March 1, 2022. https://www.protocol.com/policy/russia-ukraine-war-tech?rebelltitem=1#rebelltitem1

- Provides a comprehensive analysis of the tech sanctions imposed by both companies and governments.
- Encompasses chips (semiconductors), cargo shipments, and space co-operations.
- Used for the U.S., South Korea, Japan, and the EU.

CYBER ATTACKS

Milmo, Dan. “Anonymous: The hacker collective that has declared cyberwar on Russia.” *The Guardian*.

February 17, 2022. https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

- Anonymous has claimed credit for:
    - DDoS attacks against Russia Today (propaganda site) and other government websites.
    - The Ministry of Defense database hack.
    - Russian state TV hack that broadcasts patriotic pro-Ukraine content.
- Difficult to deter as it is a loosely organized individual group.

ABOUT THE AUTHOR

Pari Esfandiari

Pari Esfandiari is the co-founder and president at the Global TechnoPolitics Frum. She is a member of the At-Large Advisory Committee (ALAC) – Euralo at the Internet Corporation for Assigned Names and Numbers (ICANN). She servers at the APCO Worldwide's International Advisory Council and is a member of the Action Council at the Atlantic Council's GeoTech Center. She is also the founder and CEO at the Pario Consultants, an international technology investment and incubating company. Previously, she was a Nonresident Senior Fellow at the Atlantic Council.

Esfandiari is a serial entrepreneur, internet pioneer, and sustainable development executive. Her extensive international background includes leadership, advisory, and investment positions with organizations and corporations in China, Europe, the Middle East, and the United States. She has worked across diverse industries ranging from FinTech, gaming, communications, and e-commerce to sustainability and smart cities. Her social enterprise offers cross-border/discipline collaborative tools to champion women's role in sustainable development. It was showcased by UNESCO and supported by the Google Foundation. She has a doctorate from Oxford Brookes University in the sustainability business and is an avid environmentalist.

GLOBAL TECHNOPOLITICS FORUM LEADERSHIP

Chairman

Gregory F. Treverton

President

Pari Esfandiari

Board of Advisors

Philip Chase Bobbitt

David Bray

Thomas A. Campbell

Shelby Coffey

Shanta Devarajan

C. Bryan Gabbard

Nancy K. Hayden

Jim Herriot

Molly Jahn

Spencer Kim

Robert Klitgaard

Ronald Marks

Kevin M O'Connell

Barry A. Sanders

Rod Schoonover

Davide Strusani

Peter Vale

John Walcott

James F. Warren

David K. You

The Global TechnoPolitics Forum is a 501(C)(3) nonprofit educational organization with a mission to shape the public debate and facilitate global coordination at the intersection of technology and geopolitics. It achieves this mission through: convenings, research, and community building.

www.TechnoPolitics.org
ISBN: 978-1-7362034-1-5
info@technopolitics.org
Tel: +1.202.735.1415