GLOBAL PARTNERS DIGITAL

NOVEMBER 2013

DECIPHERING RUSSIA
Russia's Perspectives on Internet Policy and Governance

EDITED BY **GLOBAL PARTNERS** DIGITAL

GLOBAL PARTNERS DIGITAL

NOVEMBER 2013

DECIPHERING RUSSIA
Russia's Perspectives on Internet Policy and Governance

BY DANIEL KENNEDY

gp-digital.org

Global Partners Digital
Development House
56–64 Leonard Street
London
EC2A 4LT
+44 (0)207549 0337
info@gp-digital.org
gp-digital.org

Global Partners & Associates Ltd
Registered in England and Wales

Company Nº 520 1603
VAT Nº 840 1912 54

Designed by Soapbox, www.soapbox.co.uk

CONTENTS

Executive Summary 06

Background 07

Issues 08
- Domestic internet regulation in Russia 08
  - Russia's internet blacklist 08
  - Child protection initiatives 08
  - Combatting piracy 09
  - Combatting online fraud and cybercrime 09
- International internet governance 09
  - Main Russian initiatives on the international stage 09
  - The normative framework of Russian views 10
  - Ensuring state sovereignty and state control 10
  - Combatting cybercrime 11
  - Convention on International Information security 11
- Russian and international governance bodies 12
  - ICANN 12
  - The GAC 12
  - The IGF 13
  - The ITU-led bodies 13

Actors 14
- Government ministries 14
- The coordinating for top level domains 14
- Industry Groups 14
- Civil Society Organisations 15

Russia at the WCIT 16

The Way Forward 17
- Upcoming Russian initiatives on internet governance 17
- How to engage Russia 17
  - Engaging industry groups 17
  - Engaging CCTLD 18
  - Engaging the Russian Government 18

EXECUTIVE SUMMARY

In the last few years, Russia has become an important player in the international internet governance debate, pushing for a governance model that is state-centric, hierarchical and based on the inviolability of state sovereignty. Russia has not only articulated an alternative model at forums like the World Conference on International Telecommunications (WCIT), it has formed alliances with states such as China and Saudi Arabia, who share its vision. Russia's views on internet governance stem from security concerns about the potential of independent information sources to harm its state and society, as well as from a normative aversion to what it views as US domination of internet governance through the Internet Corporation for Assigned Names and Numbers (ICANN). Russia has favoured the UN and particularly the International Telecommunications Union (ITU) as the organisation best suited for ultimately settling questions of governance – a view government representatives have articulated consistently at ITU meetings and summits, and in domestic media.

Russian policy on international internet governance is set by the Ministry of Communications and Mass Media and the Ministry of Foreign Affairs. Technical issues are the remit of the Russian Coordination Centre for Top Level Domains (CCTLD). Civil Society pressure and lobbying from internet industry groups such as the Russian Association for Electronic Communications (RAEC) have had little effect on policy at the domestic or international level although there is some evidence that for industry groups this situation has very recently been changing. Russia is unlikely to change its policy in the coming years but through the targeting of key non-government actors such as the CCTLD and RAEC it may be possible to convince policy makers in Russia to pursue a more moderate or inclusive model of internet governance. It should also be noted that Russia has considerable experience in the diplomatic field and, in the person of Sergey Lavrov, Foreign Minister since 2004, a formidable and experienced negotiator who has the full backing of the Russian leadership.

It is possible that the Russian government could be engaged to work more closely with governments on issues where Russian and Western views and interests more closely align such as child protection and combatting cybercrime. However, any such engagement would need to be approached with extreme caution given that initiatives in these areas can easily by misused to restrict speech unnecessarily or violate citizen privacy.

Internet usage and the internet industry in Russia have grown dramatically in the last ten years, and the Russian government is proud that it boasts "the largest internet industry in Europe." [1] The increasing penetration of Information and Communication and Technologies (ICTs) in Russian life has greatly increased the importance of internet regulation on the domestic policy agenda of the Russian government. The Russian Duma has passed tough new legislation against online piracy and created an "internet blacklist" designed to prevent access to harmful and illegal content, especially by minors. Cybercrime and fraud has also become a greater source of concern for Russia's government and Ministry of Internal Affairs in recent years. These initiatives have attracted criticism from civil society organisations, who worry they infringe upon free expression and privacy, and from industry groups who worry over-regulation will hurt their business.

NOTES

[1] http://tasstelecom.ru/news/one/10097#ixzz2ehWSvcao

BACKGROUND

Since the beginning of the current century, internet use in Russia has increased exponentially by virtually every metric imaginable. While as recently as 2003, 81 per cent of Russians claimed to never use the internet, by 2013, this figure had fallen to 38, with over half of Russians stating they used the internet at least once a week. Over the same period, the number of domain names using the main Russian top level domain ".ru" rose from slightly over 200,000 to just under 4.5 million, a growth of over 2,100 per cent.

The Russian-language internet (popularly known as the "RuNet") has not only exploded in terms of usage, it has developed a unique landscape, with popular services like search engines, social network sites, blogging platforms and email being provided primarily by indigenous companies rather than Western multinationals. Russia is one of the few countries where neither Google nor Facebook are market leaders in their fields. Instead, Russia's most popular search engine is Yandex, whose algorithms were designed to deal with the complexities of the Russian language. Russia's most popular social network, VKontakte, has been derided as a "Facebook clone" but has distinguished itself in allowing peer to peer sharing and a lax attitude towards enforcing intellectual copyright. And while LiveJournal's popularity as a blogging platform fell dramatically in the West, its continued popularity with Russian users, who refer to it by its Russian initials "ZheZhe", eventually led to its being sold to a Russian consortium in December 2007. These peculiarities have occasionally led some to falsely view the RuNet as distinct and isolated from the rest of the internet. This can be seen in conceptions of the RuNet as Russia's "national internet segment." In reality, much of the internet infrastructure Russians use is located beyond the country's physical borders and Russian internet users are engaged not only with major Russian speaking communities in Ukraine, central Asia, Israel, and America, but with users from all over the world.

DOMESTIC INTERNET REGULATION IN RUSSIA

Although the RuNet developed a reputation as a space for largely unfettered free expression and light regulation during the first decade of the 21st century, its rapidly growing popularity has not gone unnoticed by the Russian government. If the Russian government's attitude towards the internet had previously been one primarily of benign neglect, in the last two years it has proposed and introduced a plethora of new laws aimed at preventing online piracy, and combatting child pornography, political extremism, and the propagandisaton of suicide and drug use. These efforts have led to the creation of an online "blacklist" of prohibited sites, to which ISPs are required to cut off all access, and to a strict anti-piracy law, which has been referred to by the Russian and Western press as "the Russian SOPA." These initiatives have created a nascent industry and civil society backlash among those who worry that increased government control over the internet will diminish its capacity to provide for free expression and/or its economic benefits.

The last two years have seen a tremendous number of new legal initiatives on the national level. Industry and civil society groups have opposed many of these initiatives. The Russian Association of Electronic Communications (RAEC), an industry umbrella group created to represent Russian and Western internet companies operating in Russia, has been monitoring these legal initiatives since the beginning of 2012. Out of 47 new bills proposed in the Duma between January 2012 and March 2013, RAEC found 23 to have the potential to negatively affect the internet industry and three likely to have an extremely negatively effect.[2]

Russia's internet blacklist

One of the most prominent and controversial new laws in Russia was the creation of the so-called internet blacklist, which sets up a unified register of banned IPs, internet addresses and domain names, under the control of ROSKOMNADZOR, the internet monitoring division of the Russian Ministry of Communications and Mass Media. ROSKOMNADZOR monitors websites for illegal content through reports from individual internet users and the use of deep packet inspection technology. While an official website has been set up where users can query whether a given site has been blocked, the complete registry is not available to the public. The Russian black list has been primarily justified as a means of protecting children from inappropriate or illegal content, such as child pornography, information on how to obtain or prepare illegal drugs, or that promotes suicide. Sites that violate Russia's intellectual copyright laws also end up on the blacklist. Despite considerable criticism (including a number of prominent Russian websites "going black" for a day in protest) the blacklist has remained a fixture of Russian domestic internet governance since coming online in November 2012. Critics argue ROSKOMNADZOR's system is non-transparent, lacks proper oversight and is open to abuse by authorities.

Child protection initiatives

The blacklist initiative is largely in keeping with an increased interest in both child protection and public morality that has marked Putin's third term as president. Similar initiatives have included a law mandating an age-based rating system for print and screen media and a law limiting the usage of profanity in media. Many of the concerns behind these new laws are similar to those of the West: fighting child pornography and limiting children's access to age inappropriate content. The Russian government's particular focus on combatting sites that promote suicide is a reflection of Russia's unfortunate status as the country with the highest underage suicide rate in Europe.

Much of this legislation appears to be a reaction to what is seen as the excessive sexualisation or moral nihilism in society that followed the break-up of the Soviet Union. Some legislative initiatives however have taken forms antithetical to Western liberal ideas. Russia's much criticised "gay propaganda" law, which mandates fines for the distribution of "propaganda about non-traditional sexual relations among minors" is overwhelmingly seen in Russia as an uncontroversial child protection law, rather than a gay rights issue.

Combatting piracy

Another prominent law, which RAEC has strongly criticised, is the Russian anti-piracy law, which came into effect in July 2013. Some dubbed this law "the Russian SOPA" for what was seen as its draconian ability to shut down entire IP-addresses with no judicial oversight. The law was originally drafted and passed without any concerns or proposals from civil society groups or the internet industry being taken into consideration. The law attracted strong condemnation in Russia. Over 100,000 online signatures on Russian Popular Initiatives, an e-governance site, called for its repeal, which legally required the issue to be raised in the Duma.

The backlash seems to have forced the Russian government to reconsider its position. The Duma's Committee on Information Policy and Information Technology and Communications held a new session with industry representatives to discuss improvements to Russia's intellectual property laws. In September 2013, President Putin himself expressed the opinion that "intellectual property rights must be ensured, but we also can't overdo it and kill the internet." [3]

Combatting online fraud and cybercrime

Russia has long had an abnormally high level of sophisticated online fraud and cybercrime. Mark Galeotti, an expert on Russian security services, has attributed this phenomenon to the fact that the country produces a high number of well-educated programmers and IT specialists but does not have an IT-sector capable of producing enough jobs for all of them. Many of these programmers have joined organised gangs of criminals and use their skills to create and sell malware, steal personal data and commit sophisticated acts of online fraud and theft.[4] In 2012, Russian cybercrime was worth an estimated 1.936 billion US Dollars, a slight fall from 2011 when it was worth an estimated 2.055 billion.[5] Russia's domestic market makes up a small fraction of this amount at an estimated 260 million, though this represents a growth on 230 million for 2011.

Russia's reputation as a significant source of cybercrime and fraud has frustrated industry representatives for years. RAEC sees it as damaging to legitimate Russian business and has lobbied the Russian government to combat cybercrime more proactively. Combatting cybercrime is primarily the remit of the Ministry of Internal Affairs, whose "Directorate K" is charged with investigating online crimes including fraud. In recent years the government has promised to work more closely with the private sector and ordinary citizens to combat cybercrime. The head of Directorate K, Aleksey Moshkov has called for greater integration of different law enforcement branches and industry to combat crime, claiming that currently many criminals go free due to a lack of coordination.

INTERNATIONAL INTERNET GOVERNANCE

Main Russian initiatives on the international stage

The Russian government has not confined its newfound interest in internet regulation to the domestic sphere. In the last two years, Russia has made three major proposals aimed at creating new international standards on internet governance. The first was a proposal at the ITU 2010 plenipotentiary meeting in Guadalajara to replace the Governmental Advisory Committee (GAC) with an ITU-led body that would hold the power to veto ICANN. The second was a proposed "Convention on International Information Security", which was presented to the United Nations Assembly in December 2011. The third and most recent was the Russian proposal for the updated International Telecommunication Regulations (ITRs) at the WCIT in Dubai in December 2012.

The normative framework of Russian views

These initiatives showed that Russian ideas of internet governance differ substantially from Western ones. The Russian conception of internet governance is highly state-centred and based on normative ideas of the inviolability of state sovereignty. These ideas do not mesh easily with the diffused, multi-national and non-hierarchical nature of the internet, or with the model of multistakeholderism that has arisen in the global technical community since the creation of the internet. In addition, Russia's foreign policy is predicated on the idea that the world has shifted from a state of US unipolarity to a more multipolar world, in which Russia is once again a key player. The privileged position of ICANN (which is seen by many in Russia as simply a department of the US government, notwithstanding attempts to internationalise its governance) in a number of key aspects of internet governance thus runs contrary to Russia's view of how international governance should work.

Since Russian views on internet governance are usually motivated by security concerns, Russia differs from the West in its desire to securitise access to online content. While Western policymakers often express concern about online political extremism, they do not tend to view seditious information coming from other states as a serious threat to national security. Rather Western states security concerns primarily relate to curtailing illegal online activity or protecting the information infrastructure. The differing paradigm can be observed in the tendency of Western and Russian discourses to refer to "cyber security" and "information security" respectively.

While Russian initiatives on internet governance have met with resistance from the US and Europe, Russia has been cultivating an array of allies on the international stage who share its vision of internet governance. Many of these states, such as Tajikistan and Uzbekistan, both of whom signed the 2011 Proposed Convention, are not normally considered to be proactive on internet governance issues. While some of these countries, such as Tajikistan, are traditionally close allies of Russia on most issues, others like Nicaragua and Saudi Arabia, are new allies who have made common cause on several internet issues. These overtures and new alliances make Russia an important actor on the international stage.

Ensuring state sovereignty and state control

Russian policy on international internet governance is, as mentioned above, primarily based on Westphalian notions of sovereignty. Elements of the Russian security services have long regarded with suspicion the capacity of the internet to allow outside (or merely non-state) actors to remove or decrease state control over the domestic "information space." This view can be seen most explicitly in the Ministry of Defence's 2000 white paper "Information Security Doctrine of the Russian Federation" which notes that

> Particular undertakings for ensuring the informational security of the Russian federation in the sphere of domestic policy are:
> The creation of systems, counteracting the monopolisation by domestic and foreign structures of the informational infrastructure, including the information services market and mass media.
> The activation of counter-propaganda actions, directed at preventing negative consequences of the distribution of disinformation about the internal politics of Russia.[6]

The Russian government traditionally paid little attention to online content during the first decade of the century, regarding the internet as primarily a niche market, and content to focus on its control of "the information space" to terrestrial television stations (the primary source of news for most Russians).

The growing popularity of the internet, and the post-election protests that emerged in the wake of the December 2011 Duma elections (which were organised to a large extent online) have arguably changed this view. There is evidence that President Putin took the protests of 2011 as a personal attempt to overthrow him and attributed the strength of the opposition as deriving from their use of the internet and connections with other countries, notably the US. While this would arguably be a domestic political concern, it also reinforces the traditional Russian concern to protect state sovereignty. As First Deputy Director of the Federal Security Service, Sergei Smirnov stated in March 2012,

> New technologies are used by Western secret services to create and maintain a level of continual tension in society with serious intentions extending even to regime change…. Our elections, especially the [2012] presidential election and the situation in the preceding period, revealed the potential of the blogosphere.[7]

Combatting cybercrime

Western governments and analysts have often expressed the opinion that Russia is either unable or unwilling to clamp down on online fraud and cybercrime originating within its borders, as most of the economic damage takes place outside Russia's borders. The growing problem of cybercrime targeting domestic interests may be prompting Russia to take this issue more seriously. Russia has consistently ruled out acceding to the Budapest Convention on Cybercrime. Article 32 of the Convention allows signatories (in certain limited circumstances) to access data on an information system in the territory of another party without that party's authorisation. Russia believes this provision to be an infringement on its sovereignty. Russia has instead put forward its own draft convention, the details of which are outlined in the next section.

Despite its scepticism towards the Budapest Convention, Russia has recognised the importance of working with other governments to combat transnational cybercrime. The deputy Minister of Internal Affairs, Igor Zubov, has called for "wider international cooperation in the fight against cybercrime." [8] Russia has discussed enhanced cooperation on this issue at a variety of bilateral and multilateral events, including the G8. At a bilateral meeting with the United States in May 2013, the Russian Minister of Internal Affairs, Vladimir Kolokoltsev announced that a "decision was taken to examine the possibility of setting up a working group on questions of the fight against cybercrime and the sexual exploitation of children, combatting contraband, human trafficking and also an information exchange, especially in the run-up to events like the Sochi Olympics."[9] While there are almost certainly legitimate – as defined by human rights standards - concerns that the Russian government is attempting to address, illegitimate concerns (such as a clampdown on activities by lesbian and gay groups) are also intimately tied up in these efforts.

Convention on International Information Security

Russia's securitised views on internet governance were made most explicit in a proposed "Convention on International Information Security" in September 2011. The convention was first unveiled at a high level meeting of international security experts in Yekaterinburg, Russia, and then presented to the United Nations. The Convention was signed by China, Uzbekistan and Tajikistan. The proposed convention stated among its main clauses that participatory states would "guarantee the free exchange of technology and information, while maintaining respect for the sovereignty of States and their existing political, historical, and cultural specificities." The convention further stated that some of the main threats to "international peace and security in the information space" were "actions in the information space aimed at undermining the political, economic, and social system of another government, and psychological campaigns carried out against the population of a State with the intent of destabilising society" and "the manipulation of the flow of information in the information space of other governments, disinformation or the concealment of information with the goal of adversely affecting the psychological or spiritual state of society, or eroding traditional cultural, moral, ethical, and aesthetic values." [10]

While Russia's proposed convention failed to gain traction in the international community, it clearly demonstrates elements of the Russian state consider the internet to be composed of "national segments" (a concept that would reappear at the WCIT), which are ultimately the sole preserve of the state to which they supposedly belong. Some analysts have dubbed this conception the "sovereign internet", playing off the Kremlin's infamous conception of "sovereign democracy", where democracy is allowed to exist but must be subservient to supremacy of the state and free from foreign interference.

RUSSIAN AND INTERNATIONAL GOVERNANCE BODIES

ICANN

Russia has taken issue with ICANN's dominance of international governance for years. Increased interest in securitising online content can be traced back to at least October 2010, when Igor Shchegolev, then Russian Minister for Communications, submitted a proposal to the quadrennial ITU plenipotentiary on behalf of the Regional Commonwealth for Communications, a telecom consortium formed of former Soviet Republics. The proposal suggested ICANN's GAC should be replaced by an ITU-run body, which would have a power of veto over ICANN's board of directors. In a statement to the ITU, Shchegolev said,

> The massive influence of the internet, the use of digital services and structures in the everyday life of wide sections of society forces us to consider the problems of security; first and foremost, that of informational security. The member states of the ITU recognise the wide range of problems in this sphere - from ethnical norms when using the World Wide Web to defence from cyber attacks. In our opinion, the provision of the rights of the subjects of informational cooperation, both national and cross-border, must be based on the resolution of legal, organisational and ICT-related questions with the consideration of the creation of a planed mechanism of defence.
>
> The work led by the ITU on the development of information and communication infrastructure, the provision of widespread access and on informational security is the primary activity defined at the WSIS. We consider the ITU to be capable of ensuring the fulfilment of the aims of global state politics, such as internet governance, internet development and finally the defence of the interests of the countries in ICANN. [11]

While Shchegelov's proposal did not lead to any concrete changes within the ITU itself, it set the tenor for Russian initiatives at the WCIT two years later, where Russia would advocate for a large number of technical issues to become the ultimate remit of the ITU.

The GAC

Despite its official misgivings about ICANN, Russia was quite active within it a few years ago, and as the country with the largest number of Cyrillic alphabet users, worked hand in glove with the GAC on developing the .рф domain as well as a host of other Cyrillic TLDs. On this issue, the Russian Coordinating Centre for Top Level Domains (CCTLD) has been highly successful and was granted exclusive monopolistic rights to issue many Cyrillic domains. Russian interest in the GAC as a forum for discussion has waned in recent years as the scope for cooperation on technical issues such as new TLDs has largely been exhausted.

The IGF

Russia has not been particularly active in the IGF. Though it has taken part in the annual conferences, it has made no major proposals to the consultative groups.

ITU-led bodies

Russia has consistently argued it believes the ITU is the most appropriate body for settling questions of international internet governance and fulfilling the Tunis Agenda. Consequently, it has favoured ITU-led platforms such as the WCIT and the World Telecommunication/ICT Policy Forum (WTPF) for announcing major proposals or debating internet governance models. Russia has offered to host the WSIS+10 summit in Sochi in Russia.

NOTES

[2] http://raec.ru/upload/files/2013_04_raec_monitoring_legislation_2012-2013.pdf

[3] http://izvestia.ru/news/556703

[4] http://themoscownews.com/siloviks_scoundrels/20111121/189221309.html

[5] http://report2013.group-ib.com/

[6] http://www.scrf.gov.ru/documents/6/5.html

[7] http://www.infosecisland.com/blogview/22638-Russia-deploys-a-massive-surveillance-network-system.html

[8] http://tasstelecom.ru/news/one/13576

[9] http://tasstelecom.ru/news/one/19902

[10] http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument

[11] http://www.itu.int/plenipotentiary/2010/statements/russian_federation/shchegolev-ru.html

ACTORS

GOVERNMENT MINISTRIES

Russian policy on international internet governance is the remit of the Russian Ministry of Communications and Mass Media, and the Russian Ministry of Foreign Affairs. The Russian security services have a strong interest in the issue as well, although the exact role they play is difficult to ascertain. The Ministry of Communications is headed by Nikolai Nikiforov, who was appointed to the position in May 2012. Aged 29 when appointed, he is Russia's youngest minister. The ministry represents Russia's interests at the ITU. In the Ministry of Foreign Affairs, policy on internet governance is largely shaped by Andrey Krutskikh, who holds the title of "Special Coordinator of the Ministry of Foreign Affairs for the Political Use of Information and Communication Technology." Krutskikih, previously represented Russia at the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. He enjoys the status of an "ambassador at large" and has worked in this capacity since March 2012.

The two ministries have largely acted in concert publically. The Ministry of Communications has tended to emphasise multistakeholderism to a greater extent in public statements[12] while the Ministry of Foreign Affairs has preferred to focus on security. But both have articulated the same view of internet governance at ITU events including the WCIT.

THE COORDINATING COUNCIL FOR TOP LEVEL DOMAINS

Russia's Top Level Domains (.ru and .рф) are administered by the Coordinating Centre for Top Level Domains of the Russian Federation (CCTLD). The CCTLD is an independent non-governmental organisation whose membership is drawn from Russian technical experts in the telecommunications field. The CCTLD is headed by an elected council drawn from academic and industry experts, whose membership includes at least one official from the ministry of communications. In July 2012, the CCTLD became a member of ISOC.

In addition to granting domain names, the CCTLD has also been active in organising the Russian Internet Governance Forum. Established in 2010, the Forum is an open conference for government, industry, academic, and civil society stakeholders from Russia and abroad to discuss questions of internet governance. The CCTLD's director, Andrei Kolesnikov, has spoken in favour of ITU taking on a more active role in internet governance, but has underlined that this can only be permitted in the context of a multistakeholder model. At the same time, he has also declared that "every state will always have the right to establish norms of internet governance in accordance with its national laws and to defend its interests." [13]

INDUSTRY GROUPS

Russia's internet industry is most visibly represented by the Russian Association of Electronic Communications (RAEC). RAEC was founded in 2006 and draws its membership from some of the biggest and most profitable internet companies in Russia. RAEC has been an active and vocal lobby group, publishing its findings and positions on every piece of legislation it feels has the potential to affect the internet industry. RAEC has consistently spoken out in favour of industry self-regulation and multistakeholderism.

While RAEC has been active in its lobbying attempts to both the Russian Duma and Ministry of Communications, its efforts have not been particularly successful. Despite several meetings with Duma Deputy Robert Shlegel, who sits on the Committee on Information Policy and Information Technology and Communications, RAEC's suggestions and concerns on pieces of key legislation such as Russia's new anti-piracy law and the new child protection laws were ultimately ignored or discounted. Analysts within RAEC believe that the anti-piracy law in particular passed due to the extensive lobbying of Russia's indigenous film industry, which already receives generous state subsidies, and the influence of trade agreements with the United States that required Russia to be seen as clamping down on intellectual property theft. RAEC's earlier lack of success as a lobbying force was a key factor in the decision of one of Russia's largest internet companies, VKontakte, to unilaterally announce its withdrawal from the organisation in January 2013. VKontakte executive Ilya Perekopsky explained, "2012 showed that RAEC has no purpose and no influence."[14]

The lack of industry input into Russia's internet governance policy could be seen at the WCIT, where not a single advisor from Russia's internet-industry was represented on the Russian delegation. Despite RAEC's poor track record, recent developments suggest that the Russian government may be more willing to engage with RAEC in future. In September 2013, the Duma chaired new sessions re-examining the anti-piracy law and several government figures, including President Vladimir Putin himself, spoke out in favour of industry self-regulation and the need for more consultations between government and industry when drafting laws.

CIVIL SOCIETY ORGANISATIONS

Civil society is relatively underdeveloped in Russia. Russia's civil society organisations, particularly those with a human rights focus, have only recently begun to take an interest in issues like internet governance and digital rights. Much of this recent reaction has arisen in response to recent Russian legal initiatives that are seen as impinging on online free expression or privacy. New civil society organisations, such as eLiberator, which provides legal and technical advice to internet users who believe their online rights are being violated, and the Association of Internet Users, which aims to bring together civil society, industry and ordinary internet users into a cohesive advocacy group, have arisen in 2013. Russia has also seen the emergence of its own Pirate Party and branch of ISOC within the last year. Encouragingly, civil society and industry show signs of beginning collaboration on digital rights, with the Association of Internet Users having founders from the Pirate Party of Russia, Russian-language Wikipedia, the Agora human rights group, and RAEC. RAEC chose to publish its analysis of the new anti-piracy law on the Association's website.

Despite this interest, civil society groups remain politically weak and lack input into government decisions on key questions like internet anonymity, piracy and the limits of free expression. Civil society actors have claimed that most Duma Deputies refuse even to meet with them for discussions. Given the domestic situation in Russia, questions such as international internet governance are primarily seen as academic by groups concerned with more pressing human rights concerns. Nevertheless, figures such as Damir Gainutdinov of eLiberator have written about the issues raised around the WCIT and their potential consequences for the rights of Russia's internet users.

NOTES

[12] See e.g. http://tasstelecom.ru/news/one/19487; http://tasstelecom.ru/news/one/19118; and http://tasstelecom.ru/news/one/10744

[13] http://www.tasstelecom.ru/articles/one/3743

[14] http://www.gazeta.ru/business/news/2013/01/28/n_2728085.shtml

RUSSIA AT THE WCIT

Russia's role in the WCIT in Dubai in December 2012 can perhaps be seen as the culmination of its attempts to reshape internet governance on the global level. Russia's representation both at the Council Working Group and the WCIT itself was composed entirely of Ministry of Communications and Ministry of Foreign Affairs figures, augmented by several representatives from Russia's large, semi-state telecommunications companies and research institutes. The delegation was headed by Nikiforov, with Krutskikh also serving as a delegate. There were no delegates or observers from Russian civil society or internet industry groups.

Russia's interest in using the WCIT to expand the role of the ITU in internet governance was apparent long before the conference in Dubai. As far back as March 2011 at the Council Working Group in Geneva, Russia was proposing making the ITU responsible for at least some aspects of the allocation of IPv6 addresses and for a definition of "online child protection." Reports that Russia (and other countries) were preparing proposals that would greatly expand the ITU's responsibilities in the field of internet governance led to a civil society and industry backlash in Europe and the United States, but were broadly ignored in Russian media in the run-up to the conference.

Russia's proposals at the plenary conference called for a definition not only of "internet", but of "national internet segment", which they proposed to mean "telecommunication networks or parts thereof which are located within the territory of the respective State and used to carry Internet traffic and/or provide Internet access." In addition, Russia proposed that the ITRs should include a clause that "Member States shall have the sovereign right to establish and implement public policy, including international policy, on matters of Internet governance, and to regulate the national Internet segment, as well as the activities within their territory of operating agencies providing Internet access or carrying Internet traffic." Aside from attempting to enshrine the primacy of state sovereignty in questions of internet regulation, the Russian proposal also pushed for many of the functions of ICANN to be taken over by the ITU.

Several days into the summit, Russia put forward a working proposal for new ITRs together with the United Arab Emirates, China, Saudi Arabia, Algeria, Sudan and Egypt. The proposal contained many ideas and definitions from Russia's original proposal to the plenary. The proposal was eventually withdrawn, following concerted opposition from the United States and others, when Egypt eventually revealed it did not in fact support it. Russia's delegation did try to revive the proposal several days later, but this was apparently an attempt to force a vote on the "compromise" proposal put forward by the WCIT chairman, Mohamed Al-Ghanim. Russia ultimately supported the compromise vote along with 86 other countries but was unable to get the United States or the vast majority of Europe to vote for it.

THE WAY FORWARD

UPCOMING RUSSIAN INITIATIVES ON INTERNATIONAL INTERNET GOVERNANCE

Although the new ITRs were ultimately not unanimously accepted by the countries at the WCIT, Russia is unlikely to view this as a defeat of the principles it put forward. Rather it is likely to view itself as having a mandate supported by a numerical majority of states including rising powers like China, Brazil and South Africa. Krutskikh stated back in April 2013 that Russia is willing to return to the issues raised at the WCIT at other international summits and does not consider the matter settled. Similarly, Russian views on internet governance continue to be coloured by distrust of ICANN which is seen as an American institution. As Shlegel stated immediately following the end of WCIT,

> One side cannot and must not have a monopoly in such an [important] area, whether it is ICANN or someone else. The world is not unipolar; the world is multipolar, in this sphere as well as in others. Despite the fact that the internet was created by the Americans in the recent past, like television and other inventions it belongs to the whole world and not to one country. [15]

Indeed, at the WTPF in Geneva in April 2013, the Russian delegation continued to push for a top down, state-centric governance model, indicating their position has not altered in any way since WCIT. At the same time, Russia's proposal to host the 2015 WSIS+10 conference in Sochi indicates that Russia is indeed redoubling its efforts on the international stage.

Russia's distrust of what it perceives as the American model of internet governance, and preference for state sovereignty as the foundation of any international governance model is also likely to only increase in the wake of former NSA contractor Edward Snowden's revelations about the extent of US monitoring of internet traffic and the collusion of American internet companies. Even before these revelations, Russian political figures had expressed concern about the growing popularity of "non-indigenous" internet services among Russian users. Sergei Zheleznyak, a prominent Duma Deputy and member of the Committee on Information Policy and Information Technology and Communications, has gone as far as proposing a law to force all companies holding the personal data of Russian citizens to store this data on servers located within Russian territory. While such a law is almost certainly unfeasible or unenforceable, it shows that Russian opinions on governance and "information security" are unlikely to soften under the present circumstances and are, in fact, likely to harden among certain policymakers in future.

There is very little indication that the make-up of Russian government will change radically in the next 3-5 years. The protest movement that emerged in the wake of the December 2011 Duma elections has largely faded away and any sign of political liberalisation in the period that followed has largely been cosmetic. Russian President Vladimir Putin's current term runs out in 2018, after which he is eligible to run for another.

HOW TO ENGAGE RUSSIA

Engaging industry groups

This does not mean that Russia cannot be engaged with governance issues in a constructive manner. The reaction of both the Russian Duma and President Putin to the public outcry over the anti-piracy laws shows that the government may be becoming more receptive to economic arguments in favour of lighter internet regulation and a more inclusive and consultative model of domestic internet governance. As Russia's internet industry continues to grow and its leadership seeks to diversify its economy, it is likely that consultation with organisation like RAEC will become more substantial when formulating domestic policy. For this reason, representatives of Russia's internet industry should be invited to events such as the Freedom Online Coalition in Estonia in 2014, in order to engage them in the global debate on digital rights and the broader debate on internet governance and establish a lasting dialogue.

Engaging the CCTLD

The Coordination Council on Top Level Domains in Russia has been very active in fostering the debate on online internet governance within Russia through the Russian Internet Governance Forum. Members of the CCTLD have also been active participants at summits and forums around the world. The CCTLD has been supportive of the multistakeholder model and their experience working within the GAC means they are likely to be more receptive to ideas of dialogue outside of ITU-based platforms. The Russian Internet Governance Forum, which is held annually, offers a unique opportunity to engage with representatives of the Russian Ministry of Communications, industry, academia and civil society. It also offers an excellent opportunity to engage the CCTLD itself in dialogue.

Engaging the Russian Government

While Russia appears likely to take a securitised approach to content and to advocate for a state-based governance model that does not easily mesh with current thinking about multi-stakeholder governance, there remain key areas on which the Russian government can be productively engaged.

Russia's increased interest in child protection and other forms of transnational cybercrime suggests there might be a higher possibility of engagement with the US and Europe on these issues than on others. Though child pornography is occasionally seen as a domestic problem in Russia, the transnational nature of the clandestine sharing of such materials means law enforcement agencies benefit immensely from the sharing of information. Though Russia opposes Article 32 of the Budapest convention, it has been open to dialogue and especially to bilateral agreements on cooperation and information sharing, with countries as diverse as Iran and the United States. However, any such engagement would need to be approached with extreme caution. If an approach enables constructive human rights-promoting engagement then that would be positive, but it could easily be used to legitimise restrictions upon speech. Similarly while Russia has been criticised in the past for not being cooperative in combatting cybercrime and fraud, its government is likely to see the benefits of enhanced cooperation on this issue. As the domestic internet industry becomes more important to the overall economy, and as Russia enjoys both greater prosperity and greater ICT penetration, domestic fraud is likely to become an even greater concern to its government.

Russia has already begun more proactively addressing these issues in the domestic sphere and has shown signs of increased interest in engaging the West on them. They represent the best chance for productive engagement with Russia on internet governance.

NOTES

[15] http://vz.ru/politics/2012/12/13/611692.html

GLOBAL PARTNERS DIGITAL

Human rights in a connected world

GLOBAL PARTNERS DIGITAL

Development House
56–64 Leonard Street
London EC2A 4LT

+44 (0)20 7549 0336

gp-digital.org