



UNITED NATIONS RESEARCH INSTITUTE FOR SOCIAL DEVELOPMENT

Mapping Russian Cyberspace: Perspectives on Democracy and the Net

Rafal Rohozinski

UNRISD Discussion Paper No. 115, October 1999

The **United Nations Research Institute for Social Development (UNRISD)** is an autonomous agency engaging in multidisciplinary research on the social dimensions of contemporary problems affecting development. Its work is guided by the conviction that, for effective development policies to be formulated, an understanding of the social and political context is crucial. The Institute attempts to provide governments, development agencies, grassroots organizations and scholars with a better understanding of how development policies and processes of economic, social and environmental change affect different social groups. Working through an extensive network of national research centres, UNRISD aims to promote original research and strengthen research capacity in developing countries.

A list of UNRISD's free and priced publications can be obtained by contacting the Reference Centre.

**United Nations Research Institute
for Social Development
Palais des Nations
1211 Geneva 10
Switzerland**

Fax: +41(0) 22 917 06 50

E-mail: info@unrisd.org

World Wide Web Site: www.unrisd.org

Reference Centre Telephone: +41 (0)22 917 30 20

ISSN 1012-6511

Copyright © United Nations Research Institute for Social Development (UNRISD). Short extracts from this publication may be reproduced unaltered without authorization on condition that the source is indicated. For rights of reproduction or translation, application should be made to UNRISD, Palais des Nations, 1211 Geneva 10, Switzerland. UNRISD welcomes such applications.

The designations employed in UNRISD publications, which are in conformity with United Nations practice, and the presentation of material therein do not imply the expression of any opinion whatsoever on the part of UNRISD concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The responsibility for opinions expressed in signed articles, studies and other contributions rests solely with their authors, and publication does not constitute an endorsement by UNRISD of the opinions expressed in them.

◆ Contents

◆ Summary/Résumé/Resumen	iv
◆ Abbreviations and Acronyms	x
<u>INTRODUCTION</u>	<u>1</u>
<u>OF MAPS AND METHODOLOGIES: THE “BARNEY SYNDROME”</u>	<u>4</u>
<u>THE BIG PICTURE</u>	<u>5</u>
<u>THE SOVIET TELECOMMUNICATIONS INHERITANCE</u>	<u>6</u>
<u>RUSSIA’S NETWORK SEGMENTS</u>	<u>8</u>
<u>DISTRIBUTION AND PENETRATION</u>	<u>12</u>
<u>NETWORKS AND THE DIALECTICS OF CONTROL</u>	<u>14</u>
<u>NETWORKS OF CONTROL: THE PUBLIC SPHERE</u>	<u>15</u>
<u>NETWORKS OF EVERYDAY LIFE: THE PRIVATE SPHERE</u>	<u>18</u>
<u>SUMMARY AND PERSPECTIVE: THE SOCIAL SIGNIFICANCE OF RUSSIAN CYBERSPACE</u>	<u>22</u>
<u>BIBLIOGRAPHY</u>	<u>25</u>

◆ Summary/Résumé/Resumen

Summary

In 1991, a group of senior Soviet officials attempted to oust President Gorbachev from power. They were unsuccessful in part because an unofficial computer network named Relcom/Demos helped maintain the flow of information required to mobilize against them. This experience, which exposed the latent power of a small but growing civil society, encouraged many analysts to speak confidently of the democratising potential of the Internet in Russia.

Rafal Rohozinski shares some of their optimism. But he suggests that in Russia, as in any other part of the world, it is necessary to adopt a socially and historically specific approach to cyberspace. The Net is not a single undifferentiated phenomenon whose properties can be taken for granted wherever it appears. It is a technological system that exists within widely varying economic contexts, structures of power and organizational settings. And the role it can play in the construction of democracy depends very much upon the way these factors shape the specific nature of cyberspace in each concrete case.

Rohozinski begins by explaining the technological characteristics of the Russian Net, which is the 23rd largest in the world and is currently growing more modestly than the global average. Its scope has been limited by an underdeveloped telecommunications sector, fragmented among a number of competing and, in some cases, mutually exclusive systems. This not only restricts ease of access to the Net but also affects the quality of on-line connections. Therefore, unlike their colleagues in the West, the majority of Russian users experience the Net only through off-line e-mail and Usenet groups.

These users may be involved in one or more of at least four different segments of the Russian Net, each with its own technology and organizational history. The first, Relcom/Demos, which appeared during the late 1980s, was based in the Kurchatov Institute of Atomic Energy of the Russian Academy of Sciences. Despite this official background, it was from the outset a commercial venture. Service providers within the Relcom/Demos system charge for every byte of data they send or receive, providing little incentive for on-line services such as the Web, for which per-byte accounting is practically impossible.

The second segment of the Russian Net consists of a variety of non-profit academic and research efforts, led by the Russian Academy of Sciences and a number of universities and research institutes. This initiative has been supported by foreign sponsors, including the Soros-funded International Science Foundation. FreeNet is the most successful of these ventures. The latter are nevertheless far more modest than those to be found in the third segment of the Russian Net, which is made up of Internet Service Providers (like Glasnet and Sovam) that are entirely on-line and similar in some respects to CompuServe or America Online. The clientele of this group is largely Moscow-based, including many foreigners and the new class of rich Russians.

The fourth and final segment of the Russian Net—Fidonet—rarely receives attention in the West, but its penetration of Russian society is considerable and growing. Unlike Relcom/Demos and the premium services offered by Glasnet and Sovam, Fidonet is cost-free to anyone with a computer, a modem and a desire to

communicate. It is connected with the global Internet and offers roughly the same level of service as commercial providers, particularly in the regions. Finally, Fidonet preserves an ethos of sharing and community which attracts a wide-spread and loyal following. But even Fidonet is overwhelmingly an urban phenomenon, concentrated disproportionately—like other systems—along the Moscow-St. Petersburg axis.

All of these networks emerged as “private” spheres of activity during a period when the Soviet state still enjoyed formidable control over communication and information, and was furthermore engaged in a concerted effort to build large-scale official computer networks. In the second part of the paper, Rohozinski asks how this apparently paradoxical development was possible; and he finds an answer in the deepening contradiction between centralised bureaucratic control and the requirements of everyday survival that characterised the late Soviet social order.

State-run attempts to establish computer-mediated networks withered, despite the high priority they were accorded, because they suffered from the same difficulties as the larger public sphere: competition among institutions and power groups, the resistance of line managers at all levels to increasing centralised control of valuable information, and the pervasiveness of bureaucratic regulations, which made it very difficult for anyone to gain authorized access to a computer network without enormous delay.

At the same time, private networks flourished—often with the tacit agreement of the same line managers and directors who resisted official networking efforts—because they were congruent with everyone’s needs for reliable information. The informal social networks, or *blat*, which pervaded Russian society and facilitated day-to-day decisions in an ossified system, formed the basis for constructing Russian cyberspace. They routed around the hierarchies and blockages of the existing institutional order, utilizing state-provided resources to construct private networks of communication.

In this sense, it is possible to say that the construction of a Russian Net has facilitated the growth of civil society. Nevertheless it should be noted that the Russian Net, like its global counterpart, remains a relatively elitist phenomenon, more the preserve of the privileged than of society writ large.

Rafal Rohozinski is a doctoral candidate in the Faculty of Social and Political Sciences, University of Cambridge (Trinity College).

Résumé

En 1991, un groupe de hautes personnalités soviétiques ont tenté d’évincer Mikhail Gorbatchev du pouvoir. Elles ont échoué en partie à cause d’un réseau informatique privé appelé Relcom/Demos, qui a favorisé le maintien de la circulation des informations contribuant à la mobilisation des esprits contre elles. Cette expérience, qui a révélé le pouvoir latent d’une société civile modeste mais en pleine expansion, a encouragé de nombreux analystes à parler avec assurance du potentiel de démocratisation que représentait l’Internet en Russie.

Si Rafal Rohozinski partage en partie leur optimisme, il estime qu’en Russie, comme partout ailleurs dans le monde, il est nécessaire d’aborder le cyberspace en ayant à l’esprit la société et l’histoire du pays. L’Internet n’est pas un phénomène unique et indifférencié ayant les mêmes propriétés partout où il opère.

C'est un système technologique qui existe dans des contextes économiques, des structures du pouvoir et des cadres organiques très divers. Le rôle qu'il peut jouer dans la construction de la démocratie dépend donc énormément de la manière dont ces facteurs influent sur la nature spécifique du cyberspace en chaque lieu.

Rafal Rohozinski commence par expliquer les caractéristiques technologiques du Net russe qui arrive en 23^{ème} position dans le monde et connaît actuellement une croissance inférieure à la moyenne mondiale. Un secteur des télécommunications sous-développé, morcelé entre un certain nombre de systèmes concurrents et, dans certains cas, incompatibles, en a restreint la portée, ce qui non seulement en limite l'accès mais affecte aussi la qualité des connexions en ligne. En conséquence, contrairement à leurs collègues occidentaux, la majorité des utilisateurs russes ne connaissent le Net que par le courrier électronique en mode local et les groupes du réseau Usenet.

Les usagers peuvent se raccorder à l'un ou à plusieurs des quatre différents segments du Net russe et qui ont chacun leur propre technologie et leur propre histoire. Le premier, Relcom/Demos, qui est apparu vers la fin des années 80, est né à l'Institut Kurchatov de l'énergie atomique de l'Académie russe des sciences. Malgré cette origine officielle, ce fut dès le début une entreprise commerciale. Dans le système Relcom/Demos, les fournisseurs de services, facturant chaque byte de données qu'ils envoient ou reçoivent, incitent peu leurs clients à utiliser des services en ligne tels que le Web pour lesquels une comptabilité par byte est pratiquement impossible.

Le deuxième segment du Net russe se compose de diverses initiatives sans but lucratif, émanant d'universitaires et de chercheurs et placées sous la direction de l'Académie russe des sciences et d'un certain nombre d'universités et d'instituts de recherche. Cette entreprise a bénéficié de l'appui de commanditaires étrangers, notamment de la Fondation internationale des sciences financée par Soros. FreeNet est la plus réussie de ces initiatives. Celles-ci sont néanmoins beaucoup plus modestes que celles du troisième segment du Net russe, qui regroupe des fournisseurs d'accès à l'Internet (comme Glasnet et Sovam) qui sont entièrement en ligne et présentent des similitudes avec CompuServe et America Online. La clientèle de ce groupe se recrute surtout parmi les moscovites, comprenant également de nombreux étrangers et la nouvelle classe des Russes riches.

Le quatrième et dernier segment du Net russe—Fidonet—retient rarement l'attention à l'Ouest mais il est très bien implanté dans la société russe et progresse toujours. Contrairement à Relcom/Demos et aux services de Glasnet et Sovam, facturés au prix fort, Fidonet est gratuit pour toute personne disposant d'un ordinateur, d'un modem et désireuse de communiquer avec le monde extérieur. Il est relié à l'Internet et offre en gros le même niveau de service que les fournisseurs d'accès commerciaux, en particulier dans les régions. Enfin, Fidonet garde un esprit communautaire et un sens du partage qui lui valent une large clientèle de fidèles. Cependant, même Fidonet est un phénomène presque exclusivement urbain, concentré de manière disproportionnée, comme d'autres systèmes, sur l'axe Moscou-Saint Petersburg.

Tous ces segments sont apparus alors que l'Etat soviétique avait encore un formidable pouvoir sur la communication et l'information et déployait en outre des efforts concertés pour constituer de vastes réseaux informatiques officiels. Dans la seconde partie de son étude, Rafal Rohozinski se demande comment cette évolution apparemment paradoxale a été possible. Il l'explique par le déclin de l'ordre social soviétique, où la contradiction entre le centralisme bureaucratique et les exigences de l'existence quotidienne était de plus en plus visible.

Les tentatives faites par l'Etat pour créer des réseaux informatiques ont fait long feu, malgré la priorité qui leur était accordée, parce qu'elles souffraient des mêmes carences que le secteur public en général: concurrence entre institutions et groupes de pouvoir, supérieurs hiérarchiques opposés à tous les niveaux à un contrôle centralisé plus grand des informations précieuses, règlements bureaucratiques envahissants retardant considérablement l'accès à un réseau informatique.

En même temps, les réseaux privés fleurissaient—souvent avec l'accord tacite des mêmes supérieurs hiérarchiques qui s'opposaient à la constitution d'un réseau officiel—parce qu'ils répondaient aux besoins de chacun en informations fiables. Les réseaux sociaux parallèles, ou *blat*, omniprésents dans la société russe, qui facilitaient les décisions de la vie quotidienne dans un système sclérosé, ont servi de support à la construction du cyberspace russe. Ils ont contourné les hiérarchies et les blocages des institutions en place et se sont servis de ressources fournies par l'Etat pour mettre en place des réseaux de communication privés.

On peut dire dans ce sens que la constitution d'un Net russe a favorisé l'expansion de la société civile. Il est à noter toutefois que le Net russe, comme son homologue mondial, reste un phénomène relativement élitiste, plus réservé aux privilégiés que caractéristique de l'ensemble de la société.

Rafal Rohozinski prépare un doctorat à la Faculté des sciences sociales et politiques de l'Université de Cambridge (Trinity College).

Resumen

En 1991, un grupo de altos funcionarios soviéticos trató de deponer al Presidente Gorbachov, pero fracasó en su intento, en parte porque una red informática extraoficial, Relcom/Demos, ayudó a mantener el flujo de información necesaria para luchar contra ellos. Esta experiencia, que reveló el poder latente de una sociedad civil pequeña pero creciente, alentó a muchos analistas a hablar con toda confianza del potencial democrático de Internet en Rusia.

Rafal Rohozinski comparte su optimismo, pero sugiere que en Rusia, como en cualquier otro lugar del mundo, es necesario adoptar un planteamiento social e histórico específico del ciberespacio. La Red no es un fenómeno único indiferenciado, cuyas propiedades puedan darse por sentadas donde quiera que surja. Se trata de un sistema tecnológico establecido en el contexto de una gran variedad de ámbitos económicos, estructuras de poder y marcos organizativos. Su función en la construcción de la democracia depende en gran parte del modo en que estos factores configuran la naturaleza específica del ciberespacio en cada caso concreto.

Rohozinski empieza explicando las características tecnológicas de la Red rusa, que se trata de la 23ª más extensa del mundo y que actualmente está experimentando un crecimiento más lento que el promedio mundial. Su alcance se ha visto limitado por un sector de telecomunicaciones subdesarrollado, dividido en una serie de sistemas competidores que pueden llegar a excluirse mutuamente, lo que no sólo limita el acceso a la Red, sino que afecta asimismo la calidad de las conexiones en línea. Por tanto, a diferencia de sus colegas de Occidente, la mayoría de los usuarios rusos conocen la red solamente por el correo electrónico fuera de línea y por grupos de Usenet.

Estos usuarios pueden participar en uno o más de al menos cuatro diferentes segmentos de la Red rusa, cada uno de los cuales cuenta con su propia tecnología e

historia organizativa. El primero, Relcom/Demos, que apareció a finales del decenio de 1980, se estableció en el Instituto Kurchatov de Energía Atómica de la Academia de Ciencias Rusa. A pesar de sus antecedentes oficiales, desde un principio se trató de una empresa comercial. Los proveedores del servicio del sistema Relcom/Demos cobran por cada byte de los datos enviados o recibidos, facilitando escasos incentivos para los servicios en línea como la Web, en los que la contabilidad por byte es prácticamente imposible.

El segundo segmento de la Red rusa consiste en una variedad de actividades académicas y de investigación sin afán lucrativo, dirigidas por la Academia Rusa de Ciencias y por una serie de universidades e institutos de investigación. Esta iniciativa ha recibido el apoyo de patrocinadores extranjeros, incluida la Fundación Internacional de Ciencias financiada por Soros. Freenet es la empresa de más éxito. No obstante, estas últimas empresas son mucho más modestas que las del tercer segmento de la Red rusa, compuesto por proveedores de servicios de Internet (como Glasnet y Sovam), permanentemente en línea y similares en algunos aspectos a CompuServe o America Online. Los clientes de este grupo se encuentran fundamentalmente en Moscú, entre los que se incluyen muchos extranjeros y la nueva clase de ricos rusos.

El cuarto y último segmento de la Red rusa—Fidonet—raramente se toma en consideración en Occidente, pero su penetración en la sociedad rusa es considerable y sigue aumentando. A diferencia de Relcom/Demos y de los servicios con recargo prestados por Glasnet y Sovam, Fidonet es gratuito para todo aquel que tenga un ordenador, un módem, y deseos de comunicarse. Está conectado a la Internet mundial y presta prácticamente los mismos servicios que los proveedores comerciales, particularmente en las regiones. Por último, Fidonet conserva una filosofía del compartir y de comunidad que atrae a muchos clientes fieles. Pero incluso Fidonet es fundamentalmente un fenómeno urbano, concentrado desproporcionadamente—al igual que otros sistemas—en el eje de Moscú-San Petesburgo.

Todas estas redes surgieron como sectores “privados” de actividad, en un periodo en que el Estado soviético aún ejercía un gran control en la comunicación y la información, y participaba asimismo en un esfuerzo concertado para construir redes informáticas oficiales a gran escala. En la segunda parte del documento, Rohozinski se pregunta cómo fue posible esta evolución, aparentemente paradójica, y halla la respuesta a su pregunta al profundizar en la contradicción entre control burocrático centralizado y las necesidades de la supervivencia diaria que caracterizaron el antiguo sistema social soviético.

Los intentos estatales de establecer redes informáticas perdieron fuerza, a pesar de la gran prioridad que se les concedió a las mismas, porque experimentaban las mismas dificultades que el sector público más amplio: la competencia entre las instituciones y los grupos de poder, la resistencia de los administradores de las líneas a todos los niveles para aumentar el control centralizado de la información valiosa, y la generalización de las reglamentaciones burocráticas, que dificultaron el acceso autorizado al público en general a una red informática, sin que hubiera grandes retrasos.

Al mismo tiempo, las redes privadas prosperaron—a menudo con el acuerdo tácito de los mismos administradores y directores de las líneas que se habían resistido a

las iniciativas oficiales de interconexión de redes—porque satisfacían las necesidades generales de obtener información fiable. Las redes sociales extraoficiales, o *blat*, que se extendieron en la sociedad rusa y facilitaron las decisiones diarias en un sistema estancado, constituyeron la base para la construcción del ciberespacio ruso. Se formaron en torno a las jerarquías y los bloqueos del sistema institucional establecido, utilizando los recursos que el Estado proporcionaba para la construcción de redes de comunicación privadas.

En este sentido puede decirse que la construcción de la Red rusa ha contribuido al crecimiento de la sociedad civil. No obstante, debería observarse que la Red rusa, al igual que su contraparte mundial, sigue siendo un fenómeno relativamente elitista, más bien al servicio de una sociedad privilegiada que de la sociedad en general.

Rafal Rohozinski es doctorando en la Facultad de Ciencias Sociales y Políticas de la Universidad de Cambridge (Trinity College).

◆ Abbreviations and Acronyms

APC	Association for Progressive Computing
CMEA	Council for Mutual Economic Assistance
CPSU	Communist Party of the Soviet Union
CIS	Commonwealth of Independent States
EARN	European Academic and Research Net
FAPSI	Federalnoye Agenstvo Pravitelsvey Sviazi I Informatiki
FTP	file transfer protocol
HQ	headquarters
IKI	Institute for Space Research
ISF	International Science Foundation
ISP	Internet service provider
ITs	information technologies
KGB	Committee for State Security
KIAE	Kurchatov Institute of Atomic Energy
MAN	Metropolitan Area Network
Minsviaz	Ministry of Communications
NASA	National Aeronautics and Space Administration
NGO	non-governmental organization
OECD	Organisation for Economic Co-operation and Development
PADS	Private Access Dial-up Service
Relcom	RELIable COMunications
SFMT	San Francisco Moscow Teleport
SPS	Sistema pravitelsvey svyazi
STR	scientific and technological revolution
US	United States
USSR	Union of Soviet Socialist Republics
UUCP	Unix-to-Unix Copy Protocol
VNIPAS	All-Union Institute for the Problems of Automated Systems
VNITI	All-Union Centre for Data
WAIS	Wide Area Information Service
WWW	World Wide Web

INTRODUCTION

On 19 August 1991, a group of senior Soviet officials attempted to oust President Gorbachev from power.¹ They formed a Committee for National Salvation, declared an Extraordinary State of Emergency and announced their intention to take over the state. To most Russians, that August morning was a throwback to a distant past: the radio played classical music—a sure sign of the gravity of the situation; Soviet television, the beacon of *perestroika* during the past five years, broadcast reruns of **Swan Lake**, interrupted only by the sombre news bulletins of anonymous announcers dressed in military uniform; and those newspapers that were published dutifully carried the full declaration of the Extraordinary State of Emergency.

Control over information was the coup Committee's greatest strength. Few people in Russia's regions knew what was really occurring in Moscow, while those Muscovites who opposed the coup could not judge whether regional authorities were complying with the Committee's directives. An informational vacuum once again threatened to descend upon the USSR. However, the coup plotters failed to completely shut down the telephone system.² Its continued functioning meant that Russia's fledgling computer network—a "private" Net that had been built largely outside of official Soviet state control—continued to operate without hindrance.

The programmers at one of Russia's private Net providers—Relcom/Demos—were among the first to see the coup in progress from their offices near the Kremlin.³ Within a few minutes of tanks appearing in Red Square, they began broadcasting information to network nodes across the USSR. Meanwhile, a group of programmers went to the Russian parliament (White House) in the hopes of making contact with Yeltsin's staff. Within hours, they had established a temporary network node at the White House and were e-mailing Yeltsin's defiant declaration, rejecting the legitimacy of the coup committee, to Russia's regions and abroad. Soon, local journalists joined in the effort and began to circulate news reports through the Net, many of which were reproduced in local press organs not under the direct control of the coup plotters.⁴ By evening, the Relcom network was acting as a major channel of information between Moscow and the regions, linking the multitude of major and minor actors opposed to the coup.⁵ As local and republican press organs increasingly drew upon Relcom for information about the

¹ The conspirators included the Vice-President, the chairman of the KGB, and the Ministers of Defence and Interior. The coup was timed to coincide with the August holidays when many key government officials, including Gorbachev, were absent from Moscow.

² Throughout the coup, most of Moscow's telephone exchanges, including the main international exchange and at least once intercity exchange, continued to operate.

³ The primary account of Relcom's role during the coup was gathered through interviews with the key actors. Secondary information was gleaned from a variety of published and unpublished accounts. See, for example, Belsie, 1991; Groves, 1991; Hogan, 1991; Press, 1991; Lawton, 1993; Klimov, 1995.

⁴ Demos staff also did the rounds of all major foreign press bureaux in Moscow, establishing networked connections to Demos headquarters.

⁵ As the outside world woke to the news, the volume of mail on Relcom's internal and external network doubled. At one stage, messages from abroad threatened to choke Relcom's mail server and its "thin" dial-up connection to Finland. Demos programmers had to plead with Westerners to stop sending messages to the network.

unfolding drama in Moscow, the information vacuum, a key factor in the coup plotters' game plan, was filled.⁶

After the coup attempt collapsed, the role played by Relcom/Demos did not go unnoticed. The very existence of this "unofficial" computer network in 1991 surprised many observers: How and when did this private network emerge, given that it was owned and operated outside of Soviet state control? Moreover, the network received considerable attention in the national and international press.⁷ Media accounts accentuated its role as a vital "back-channel" of communication and co-ordination among the opposition.⁸ Optimistic extrapolations about the future role of information technologies in the Soviet Union ensued, with many commentators espousing the "organic" connection between information technologies (IT), social change and democracy. As one study concluded:

. . . [these technologies] already have had social effects and more effects are to be expected. The coup case shows that networks were channels of information otherwise inaccessible, and generators of anti-coup action. In addition to supporting social democratization, networks can also facilitate emergence of invisible colleges, the development of telecommunications and computer industry, and dissolution of the information system that has been de-coupled from factual reality (Hogan, 1991).

The hype about the democratic potential and transformative power of Russian computer networks was hardly unique.⁹ It followed a long line of speculation, which has existed at least since the beginning of the modern industrial era, about the social impact of "advanced technology". The most recent wave of such thinking, ushered in with the "information revolution", is perhaps of a qualitatively different nature, given the sheer scale and speed with which information technologies have become a defining characteristic of modern societies. For the first time in history, technology appears to carry the very real potential to encompass all of humanity, everywhere, all the time. The comprehensive scope of ITs has led to utopian speculation regarding their potential for the empowerment of individuals, irrespective of race, language and social class. Thus, as analysts like Francis Cairncross (1997) have bravely predicted, "the death of distance

⁶ Demos staff also prepared an emergency contingency—a back-up node on a laptop computer hidden in the trunk of a staff member's car—consisting of an exact mirror of the Demos server, and a complete list of nodes, log-ins, passwords and telephone numbers, as well as details of unlisted "reserve" channels. The plan, had Demos been shut down by the authorities, was to have the back-up node move around and maintain contact with the regions and abroad for as long as possible.

⁷ As I detail below, Relcom/Demos was not the only unofficial network in 1991. Other parastatal networks had also formed and they, too, played a role in subverting the coup-makers' restriction of information. These other networks (such as Glasnet and Sovam, see below) acted mainly as a channel to the outside world, whereas Relcom/Demos acted as the main internal link, between Moscow and the regions.

⁸ Although the resistance of Yeltsin, the military, the Russian secret police and intelligence agency (KGB) and, ultimately, the mass media, was obviously key to the coup's demise, Relcom played a unique role in the sense that it facilitated widespread resistance along non-institutionalized lines.

⁹ Indeed, the rapid penetration of communist countries by information technologies, at a time of sweeping systemic change, reinforced the general idea that ITs were a harbinger of social change and, ultimately, of the democratic shift that followed the collapse of the Soviet bloc at the end of the 1980s.

[shifts] power downward, to the individual. It will both reinforce democracy and transform it". While pronouncements like this are intuitively appealing, they remain essentially rhetorical. From an analytical perspective, we need to consider how to frame an understanding of the relationship between the possibilities made available by technology and specific social consequences. Are computer-mediated networks really the midwives of democracy?

This paper takes a step back from this enormously complex question to argue that before we can even begin to understand the relationship between computer-mediated networks and social forms like "democracy", we need to have a much more grounded understanding of what, exactly, we are talking about when we speak of "the Net". Hence, this paper presents a contextualized portrait of the Russian Net—and more broadly, Russian cyberspace—by mapping out its present contours as well as its complex origins. It is only after we understand what the Net represents that we can begin to contemplate its ability to influence anything at all, including democracy.

I speak of mapping cyberspace, as well as the Net, to circumvent what I see as a tendency to reduce the social aspects of technology to a narrow technological or economic framework.¹⁰ My preference is to see the Net both as a technological artefact and as a virtual, computer-dependent social space—cyberspace—limited by its technical characteristics, subject to competing economic interests, and encompassing its own unique social forms.

This paper commences exploration of the Russian Net by mapping physical dimensions and technological characteristics: who the Net reaches and how. This exercise demonstrates the poverty of most contemporary studies that presume connectivity to be a generalizable indicator, the assumption being that if a country is connected, then the Net must be having an impact across the society as a whole.¹¹ This analytical tendency ignores the very real disparity in the Net's

¹⁰ To conceptualize the Net as a purely technological artefact tends to minimize the social characteristic—interactivity—which differentiates it from earlier communications systems. The Net collapses time as well as space. Thus while telephony allowed individuals to interact irrespective of distance, and television allows for an event to be experienced regardless of its fixture in time, the Net, with its inherent multimedia capacities, manages to accomplish both. In this sense, while the Net is undeniably a technical artefact, limiting the scope of analysis to its technological characteristics avoids the change it can affect in cognition. Similarly, seeing the Net as an economic object, an instrument or place to be fought over and claimed, tends to limit the level of analysis to a somewhat narrow political economy framework. While questions of ownership, control and regulation are undoubtedly important, concentrating solely on these questions may lead to a reductionist view of the Net, casting dynamic technological processes in static terms. The main problem, as I see it, is that the arguments which demonstrate how the Net is being "metered, packaged and sold back to us" have difficulty in accounting for its appearance and continued expansion, despite attempts to control or contain it.

¹¹ For example, a paper presented at the 1995 Internet Society conference sought to demonstrate, in empirical terms, a correlation between "democracy" and "interconnectedness." The study plotted an index of democracy (as developed by Freedom House) against an index of interconnectivity (based on the per capita distribution of network hosts in a country). The results demonstrated that "the correlation and coefficient for interconnectivity is not only large, it is substantially larger than that of any other traditional predictors of democracy". While the author stopped short of claiming a causal relationship, he nevertheless concluded: "... interconnectivity always proves to be a significant predictor

technical, social and demographic penetration, and hence leads to misleading extrapolations about its potential to influence society-wide forms like democracy.

The paper then goes on to examine Russian cyberspace in its social and historical context. The case of Russia is illuminating precisely because the Net emerged in the “private sphere” at a time when Soviet state control of communication and information was still quite formidable. Moreover, the Soviet state had invested considerable resources in building state-owned networks, but all of these had failed;¹² it was the privately run, “hidden” networks that flourished in Soviet cyberspace. How and why did these private networks and their private spaces emerge and flourish? Examination of this conundrum helps to shed some light on the Net’s past and present social functions.

OF MAPS AND METHODOLOGIES: THE “BARNEY SYNDROME”

In recent years the Internet Society has published maps showing the global spread of “Internet connectivity” by progressively colouring “connected” countries purple. The latest map, predictably, shows the world in monotone aubergine. I call this broadbrush proclivity “The Barney Syndrome”: like Barney, the purple dinosaur who embraces children in TV land with unconditional love, these maps unconditionally imply that even a single Internet connection will embrace the entire society, influencing its overall socioeconomic context. Thus, much like the “electricians” of the nineteenth century who attempted to measure the social impact of light bulbs by counting the number of light fixtures installed (Marvin, 1988), the “Barney maps” reify the social impact of the Net to a simple, misleading presence-or-absence, thereby obfuscating more than they enlighten.

Monitoring the spread of connectivity does warrant attention, as it allows us to come to terms with the evolving “tele-geography” of the information age (Graham and Marvin, 1996). However, to avoid the Barney Syndrome, our mapping should strive to be as specific and precise as possible. Our first prerequisite is to recognize that the Net does not reach everyone equally; within any given society, for example, economic disparities can play an important role in limiting *who* has the potential to be connected. Similarly, the Net is a complex technological system that requires a supporting infrastructure, including a functioning telecommunications system and threshold levels of education and computer penetration. The degree to which these supporting factors exist, as well as their characteristics, will shape the Net’s geographic reach and basic features. In this respect, the Net should not be seen as a technologically undifferentiated whole: different networks employ different technologies, which have a bearing on the cost of access, the services provided by Internet Service Providers (ISPs) and, by extension, the type of mediated experience they make possible for a user.

of democracy and economic development, but never was the reverse true. These analytical results overlay a background of mounting anecdotal evidence that the new information and communications technologies are facilitating democratic change world-wide” (Kedzie, 1995).

¹² See, for example, Campbell, 1995; United States Central Intelligence Agency, Directorate of Intelligence, 1987; Cave, 1980.

In the next section we will move beyond the “Barney” view of the Russian Net, by taking a close-up look at its variegated terrain, with special attention to its physical, technical and socioeconomic features.

THE BIG PICTURE

Mapping anything in Russia requires a leap in one’s conception of scale. The Russian Federation, the largest Soviet successor republic, occupies a sixth of the earth’s surface and encompasses more than 150 million people of some 200 different nationalities. Its population is spread among a bewildering array of administrative units ranging from Autonomous Republics and Oblasts through to Krai and Autonomous Okrugs, together totalling 97 regional units of various sizes (Goskomstat, 1997). For the most part Russia is counted among the developed nations of the world: its population is predominately literate, educated and urban, and, up until the early 1980s, the USSR was the second largest industrialized economy in the world. Despite these positive indicators, Russia’s telecommunications infrastructure is highly underdeveloped, a legacy of its Soviet past (OECD, 1992; Campbell, 1995). It is this infrastructural underdevelopment that has greatly circumscribed Russia’s stake in the global Internet.

In aggregate terms, the Russian Net constitutes a fraction of the global Net (see figure 1, below). 1998 figures indicate that Russia is the world’s twenty-third largest Internet power (as ranked by the number of hosts), although, given the dominance of the US segment, this amounts to only about 4 per cent of the world’s Internet domains¹³ (Network Wizards, 1998). Expressed as a ratio of its total population, this means that Russia has roughly one Internet-connected computer for every 2,189 people.¹⁴ In terms of end users, rough estimates suggest that there are between 600,000 and 2.6 million Russians with access to the Net,¹⁵ although

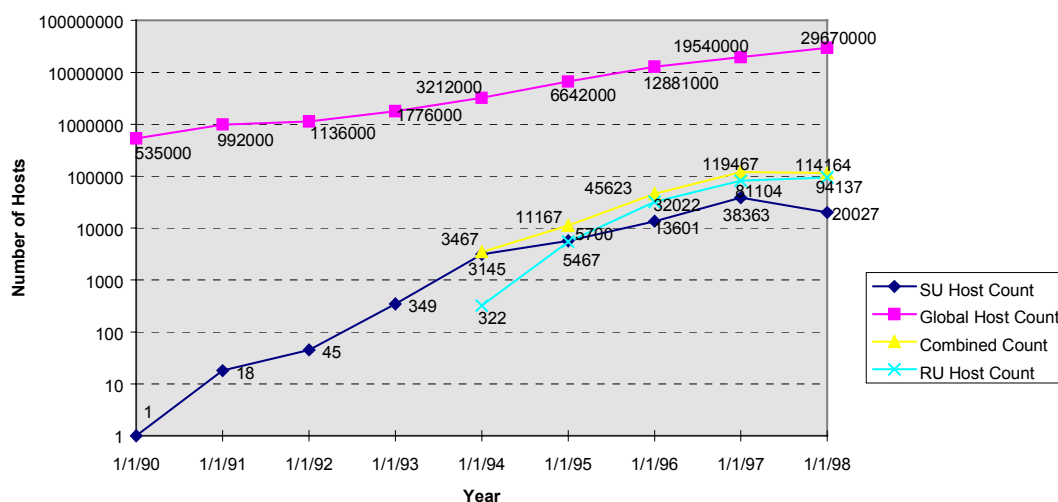
¹³ In real terms, Russia’s share may be marginally larger since the rate of “reserved” but unused domains is lower than in most Western countries (Tutubalin, 1998).

¹⁴ Author’s calculation.

¹⁵ The large discrepancy between high and low projections stems from the different methodologies used to arrive at a final figure. The low figure is the consequence of a straightforward domain count, using a fixed ratio between the number of users per host. The higher figure takes as its starting point the maximum number of hosts possible, ignoring duplicate and “unused domains” and applies a standard Western number of users per host to arrive at an estimate. For obvious reasons, this figure may overstate the number of users by a considerable amount. However, in the Russian context, domain and host counts do not adequately account for machines that do not use the Internet protocol to connect to the Net. For a variety of reasons, mostly dealing with the poor quality of Russian telephony and the generally low level of computerization outside Moscow and St. Petersburg, the bulk of Net users in Russia’s regions have access to e-mail alone. Their connection to the Net is “off-line” and uses the older but more robust Unix-to-Unix Copy Protocol (UUCP) to bundle mail between client machine and server. The UUCP addressing scheme means that only the domain of an ISP possessing a registered second-level domain actually appears in the Internet DNS. Consequently, third- and fourth-level UUCP sub-domains, which potentially represent the bulk of end-user domains, simply do not show up in aggregate DNS-based domain counts.

several leading *Setoviki* (Russian network luminaries) place the real figure at around 1.2 million users of network services of all kinds.¹⁶

Figure 1
Internet growth rates, global and Russian compared



The Russian Net has expanded exponentially over the past nine years (figure 1). However, in absolute terms, the Russian segment of the Internet is growing more slowly than the global average: while the global Internet is expected to continue expanding at a rate of between 51.8 and 63.2 per cent over the next year, the Russian segment is expected to grow at a more modest 16 per cent. Given this differential, Russia's real share of the global Internet is expected to decline over the next few years.

To some extent, this relative decline is a reflection of the both the continuing economic hardships of the ongoing process of reform, and the increasing pace of computerization in other parts of the world. However, the fecundity of the Russian Net has also been limited by the legacy of its inherited Soviet telecommunications environment.

THE SOVIET TELECOMMUNICATIONS INHERITANCE

In terms of its basic communications infrastructure, the Soviet Union shared similarities with the developing world. For its size, Soviet Russia's road network was among the least developed of any country, and basic penetration rates for telephony were at Third World levels.

Russia inherited the bulk of the USSR's surprisingly underdeveloped telecommunications system (OECD, 1992). The legacy of this inheritance is twofold. First, Russia suffers from a low penetration of basic telephony services, significantly behind the West (see table 1, below). Overall figures for 1996 show that only 48.7 per cent of urban families and 19.7 per cent of rural families have

¹⁶ Based on the author's interviews with the systems administrators and managers of four leading Internet providers (Relcom, Demos, Sovam and Glasnet) in November 1997.

access to a private telephone (Goskomstat, 1997). These figures are even lower in some of Russia's economic regions (see table 2, below).

Table 1
Comparison US-USSR: Telephone systems and usage (1991)

	No. of private phones	Main lines (trunks)	Volume of intercity calls	International calls	Residential phones (POTS) as % of total
USSR	31.1 m	24.5 m	1.7 b	1.8 m	55%
USA	180.0 m	122.2 m	37.0 b	410.0 m	84%

Source: Campbell, 1995.

Table 2
Penetration of private telephony in Russia, 1996

Region	Number of telephones per 100 families	
	Urban	Rural
Northern region	48.2	28.2
North-Western region	76.9	23.2
Central region	64.5	17.5
Volgo-Vyatka region	45.3	15.0
Central Black Earth region	47.6	19.5
Volga region	36.3	17.9
North Caucasus region	40.5	18.9
Ural region	40.7	19.4
West Siberian region	42.1	24.2
East Siberian region	32.2	17.1
Far East region	39.1	27.3

Source: Goskomstat, 1997.

Second, Russia's telephony and data networks are fragmented among a number of competing and, in some cases, mutually exclusive systems. Soviet telephony comprised a multiplicity of networks, each representing a different layer of bureaucracy. (Indeed, popular wisdom during the Soviet era held it was possible to ascertain the importance of an official by the number of telephones on his or her desk.) 1991 figures show that only 55 per cent of the total telephone stock was actually connected to the public telephone network (Campbell, 1995). The remaining 45 per cent was connected to a vast array of private or "branch systems" belonging to the USSR's All-Union State Ministries and large industrial conglomerates.¹⁷ Thus the Ministry of Railroads, Ministry of Energy and numerous military-industrial enterprises all possessed independent telephone systems. Although many could and did connect to the public telephone system, they nevertheless constituted an alternative to the Ministry of Communications (*Minsviaz*) monopoly over telephony in the USSR.

The scope and character of the Russian Net has been greatly affected by the low penetration rates and poor quality of basic telephony, and by multiple telephone networks. First and foremost, these features have acted as a brake limiting the expansion of Net services. Where no telephony exists, neither can the Net. Second, unlike the West, where the Net is largely defined by its rich array of on-line services,¹⁸ in Russia the poor state and limited quantity of local telephone lines

¹⁷ This figure (60 per cent) does not include highly secure systems operated by the KGB for the benefit of state and party organs (SPS or *sistema pravitel'svey svyazi*), nor does it include purely military systems.

¹⁸ In recent years, standard Internet services in the West include electronic mail, Usenet, Telnet, FTP and the World Wide Web. With the exception of e-mail and Usenet, these

constrain the ability to maintain an on-line connection, which in turn has limited the number of ISPs that are connected to the Internet on a full-time basis. In this respect, unlike their compatriots in the West, the majority of Russian users experience the Net through off-line e-mail and Usenet groups alone.

Third, the multiplicity of networks has had a dual influence on the development of Russia's Net. On the one hand, the lack of a telephone monopoly has given potential ISPs a large number of options through which to establish inter-regional and international connectivity (Flek, 1992).¹⁹ Thus, as enterprises have been liquidated and state and party offices have been sold or rented in order to generate revenue for their owners, their Soviet-era "independent" telephone networks (including long-haul and data services) have become available as alternatives to the existing local, regional and national telephone operators (themselves presently undergoing privatization).²⁰ The many network options have ensured thriving competition within Russia's fledgling ISP market, meaning that ownership of the Russian Net is diversified among a variety of local, regional and national operators. At present, Russia has more than 70 independent ISPs, many of whom act as upstream providers to a multitude of smaller local outfits.²¹ Significantly, this trend runs counter to the tendency found in the global Internet where consolidation of ownership among ever-larger conglomerates is the norm.

RUSSIA'S NETWORK SEGMENTS

The Russian Net can be roughly divided into four basic segments. Each segment represents, in both historical and technical terms, a different layer of the Russian Net. The largest and oldest segment belongs to the commercial network known as Relcom (deciphered as RELiable COMmunications) which emerged during the late 1980s. Between 1988 and 1990 the Relcom network (or Relcom/Demos²² as it was known until early 1992) became the first and most extensive e-mail network of the Soviet era. By the end of 1991, Relcom spanned more than 120 towns and cities, encompassing 20,000 users in over 1,000 organizations across the Soviet Union.²³

applications require a reliable on-line connection and, consequently, an ISP that is connected to the Internet full-time.

¹⁹ On a larger scale, the operators of some non-secure private systems (such as the former Communist Party telephone system, Iskra II) have effectively privatized their operations and actively compete against the main public operators (such as Rostelekom and Intertelekom) for a share of the long-haul market (Flek, 1992).

²⁰ This diversity also extends to the market for specialized data network services. Private "branch" data systems (such as the former military-industrial data network, ISTOK-K) provide an alternative solution to those services on offer from Rospac and other Minsviaz-operated data networks (Flek, 1992; Campbell, 1995).

²¹ Most of these ISPs remain in private hands or exist as joint stock companies, with only one exception—AO Relcom—which trades as a public company (Cook, 1992a; 1992b).

²² Demos is the acronym of the UNIX-like operating system developed by the team Dilogova Edinstvaya Monozadachnaya Operatsionaya Sistema (Unified Interactive Multitasking Operating System).

²³ In point of fact, so dominant and key was Relcom's role in popularizing electronic communications that, at least up to the end of 1995, most Russians used Relcom as a synonym of the Internet, an expression which only gained currency in the popular Russian press in late 1996.

Relcom's early emergence meant that it strongly influenced the Russian Net's unique organizational character, especially the franchise structure of much of the Russian ISP market, and its early commercial orientation.

In this respect, although many nodes on the Russian Net are described as "Relcom Nodes," Relcom itself has never represented a unified whole. Rather, Relcom is a generic name describing ostensibly private companies exchanging e-mail with the main Relcom node located in Moscow.²⁴ The central feature that defines the Relcom network is a contractual agreement wherein each "node" and "end-user" is charged for every byte of data they send or receive across the network. This scheme has allowed individual Relcom service providers to recoup the cost of capital expenditures and intercity (and international) telephony, while earning a small profit.²⁵ This tariff structure characterized the Relcom network as commercial from its inception. Thus a full three years before the question of commercialization of the Internet became an issue among the global Internet community, Russia's segment of the Internet (at that time represented by Relcom) was operating in accordance with commercial principles.

The effect of this early commercialization was twofold. First, unlike the Internet in the West, which weaned a generation of network users on a "free" service available at most universities, access to Relcom always incurred a cost to the end user. As a consequence, Relcom users have sought to recoup their costs, meaning that they tend to use Relcom to conduct business transactions of some kind or another, rather than for more eclectic pursuits. Second, since Relcom service providers made their money for each byte of data, they had little incentive to start providing on-line services, such as the Web, for which per-byte accounting is practically impossible.²⁶

The second segment of the Russian Net consists of a variety of ostensibly non-profit academic and research efforts, led by the Russian Academy of Sciences and a number of individual universities and institutes. For the most part, these efforts occurred later than Relcom and sought to operate on a purely non-profit basis, meaning that participating organizations (which were nodes on the network) did

²⁴ This main facility, located at the Kurchatov Institute of Atomic Energy (KIAE) provides network facilities (NOCC) to send and receive mail between all other Relcom nodes and abroad.

²⁵ The reasoning behind the per byte charge reflects the unreliability of Russian telephone lines, which preclude charging users for time spent on-line, and hence the real cost of intercity and international telephony.

²⁶ In 1992, Relcom/Demos split into two companies. This was the result of a disagreement among its directors concerning the full commercialization of the company. During the past six years, Relcom's successor companies (AO Relcom and SP Demos) remain Russia's dominant network providers and have diversified their operations to provide on-line Internet connectivity and backbone services to the new generation of ISPs. AO Relcom operates as a publicly traded company. Nevertheless, its base of operations remains the KIAE, a facility operated by the Russian Academy of Sciences, and its staff remain, at least nominally, employees of the Academy. This makes AO Relcom a rather unique entity. On one hand, Relcom's home at KIAE insulates it from the pressures of commercial competition in the volatile Russian marketplace. On the other hand, the dependence on KIAE has limited its ability for flexibility in redefining itself as a purely commercial entity. Consequently, in comparison to other providers, and in particular its former co-partner Demos, Relcom has not developed at the same rate.

not charge each other for services. Instead, network fees were used to secure international and inter-regional connectivity. In addition, the academic and research nets sought to develop a full range of on-line services (Telnet, FTP, WAIS and WWW).

Although these efforts received some state funding (primarily through the Russian Fund for Fundamental Research) they were also supported by a wide range of private and state-sponsored foreign funding. For example, the Soros-funded International Science Foundation²⁷ (ISF) financed the Moscow Backbone project, which aimed to create an Internet-type network among Moscow-based ISPs and the Russian Academy of Sciences by way of a city-wide fibre-optic loop (Cook, 1992a; 1992b). A unified Moscow backbone never materialized due to a series of increasingly acrimonious disagreements between ISF, the Academy of Sciences and Relcom over who, in the end, was to have responsibility for the network. As of 1998, the “backbone” remains “broken” into the Academy of Sciences-run Southern loop and the Relcom-operated northern segment.²⁸

A more successful attempt to build a Russia-wide academic and research network was the FreeNet²⁹ (deciphered as “For REsEarch Network”), a joint effort among non-profit networks designed to take advantage of Soros-funded infrastructure and state funding (Buben, 1995). To date, although a growing number of academic institutions and universities have joined FreeNet, it remains a loose coalition of networks rather than an “academic backbone” of the type represented by the old US NSFNet or the UK’s SuperJanet. In terms of both its geographic reach and number of users, FreeNet and the remainder of Russia’s academic and research networks are poor cousins to Russia’s commercial Net (Relcom/Demos).

The third segment of the Russian Net encompasses a variety of commercial and ostensibly non-commercial network providers who share two common characteristics: all are dependent on foreign support, and all offer services highly

²⁷ The ISF’s mandate was to provide assistance to Russian science during the tough years that followed the collapse of the Soviet system. Connecting Russian scientists to the Internet was seen as an important part of this mandate.

²⁸ In 1996, Soros pledged a further \$ 500 million to link 500 Russian universities to the Internet (the so-called Soros-Chernomyrdin Agreement). The Soros foundation is presently pursuing Metropolitan Area Network (MAN) projects in several cities, including Yaroslavl and Akademgorodok (Novosibirsk). While the primary beneficiary of these projects is “Russian science,” the agenda of the Soros-funded Open Societies Foundation is broader, including the provision of low-cost Internet access to a variety of civic groups, including non-governmental organizations (NGOs).

²⁹ FreeNet grew out of a stillborn effort by a group of Soviet institutions during the late 1980s to establish a network loosely modelled on the US Bitnet and the European Academic and Research Net (EARN). In 1990, institutions involved in this effort (then named SUEARN) received seed funding from a consortium of US and European institutions (including the Carnegie Foundation, EARN and IREX) to establish an international leased-line between Moscow and Copenhagen. However, by 1992 Bitnet was a dying technology; and after a year, foreign partners decided to stop funding the Copenhagen connection. Instead, they turned their attention the Moscow Backbone project and a variety of smaller projects. By mid-1992, SUEARN reinvented itself as FreeNet and began pushing for the creation of a Russian Academic and Research Internet (Cook, 1992a; 1992b; Mendkowicz, 1994).

centralized in Moscow.³⁰ Their services are entirely on-line and are similar in some respects to CompuServe and America On-Line. To date, the popular appeal of these ISPs (which include GlasNet and Sovam Teleport) is limited due to their lack of presence in the regions. Their clientele is largely Moscow-based and upscale, centring mainly on foreigners and the new class of rich Russians (*novoeye Russkie*). However, given the slowly increasing quality of the telephone infrastructure in the Russian regions, their highly centralized and content-driven approach may, as in the West, represent a business model for the future.

The fourth and final segment of the Russian Net—Fidonet—rarely, if ever, gets any serious attention in the West. Fidonet technology was developed in the early 1980s by a young American anarchist, giving birth to the first (and only) amateur computer network with global reach (Kochegarov, 1996). Unlike the Internet, which in the United States was the preserve of academic and military institutions up to the early 1990s, Fidonet has been more the preserve of talented computerphiles, run on a purely non-commercial, anyone-can-join basis. Although much smaller than the Internet (largely due to its technical characteristics), by 1996 the global Fidonet encompassed more than 33,000 nodes across five zones (North America, Europe, Africa, Latin America and Oceania) (Fido7, 1998). The Russian segment of the global Fidonet (known as Fido7 or Region 50) presently encompasses 4,469 nodes representing 90 separate Oblast-level networks and up to 100,000 users (Fido7, 1998).

In stark contrast to the West, where Fidonet communities are rapidly contracting, Fidonet's penetration of Russian society is considerable and growing. Fidonet's popularity in Russia is a function of several factors. First, Fidonet's "proletarian" accessibility stands in contrast to the relatively elite character of the other three segments of the Net. Unlike Relcom/Demos and the premium services offered by GlasNet and Sovam, Fidonet is cost-free to anyone with a computer, modem and the desire to communicate (Kochegarov, 1996).³¹ Moreover, unlike the academic Internet represented by FreeNet, one does not have to be a member of the Academy of Sciences or a university to gain access. Second, Fidonet offers roughly the same level of service as Russia's commercial network providers, particularly in the regions.³² Moreover, Russia's Fidonet is interconnected with the global Internet via numerous gateways, meaning that messages can move freely between the two Nets. In addition to these objective factors, Fidonet's popularity is a function of the Fidonet users themselves. *Fidoshniki* (Fidonet enthusiasts) form an active and cohesive community dedicated to Fidonet's maintenance and expansion. For reasons that I discuss shortly, Fidonet continues to attract a wide-ranging and loyal following, even among individuals with alternative ways to access the Internet.

³⁰ For example GlasNet, ostensibly the Russian spur of the non-profit global NGO network Association for Progressive Computing (APC), operates a CIS-wide network from a single cluster of Moscow-based nodes. Users in the regions dial into local Private Access Dial-up Service (PADS) to reach Glasnet's Moscow host. Sovam Teleport's "Russia On-line", another ISP in this category, takes a similar approach.

³¹ Fidonet software was written for an IBM-type PC around 1982. Nothing except a basic version of DOS and a modem is needed to make it run.

³² As the vagaries of Russia's telecommunications infrastructure limit most Net access to e-mail and Usenet, Fidonet's capacity to send mail, transfer files, and support a wide range of news groups provides the same kind of services on offer from most commercial providers (Paliev, 1998; Kochegarov, 1996).

This snapshot of the Russian Net has highlighted its technical characteristics, as well as its decentralized and differentiated structures. I now want to take a closer look at who, exactly, these various networks connect, and where.

DISTRIBUTION AND PENETRATION

Mapping the Net's penetration in Russia's regions presents a challenge. To date, there are no "yellow pages" or electronic guidebooks to the Russian Net, nor is there a simple or automatic way to generate an accurate picture of users. Technical tools can help to decipher the information that service providers register about their clients, but this is complicated given the Net's fragmentation among a number of technically differentiated networks.³³ Moreover, as a rule, Russian service providers stopped publishing data about their clients in 1994.³⁴ As a result, mapping the regional penetration of the Russian Net presents a multi-layered problem: how to accurately map technically differentiated networks; how to identify Net users and sub-segments without revealing potentially sensitive commercial information; and how to ensure that the resulting picture is relatively accurate.³⁵

For the purposes of this paper, I wish only to illustrate patterns of regional penetration. Fidonet offers a representative picture, mainly because where Fidonet exists, the Internet can exist. Similarly, if Fidonet cannot exist, then neither can the Internet.³⁶ So, using Fidonet as a baseline, several things are evident. First, the Net is overwhelmingly an urban phenomenon: 99 per cent of all nodes are located in major urban centres, usually the capital cities of the oblasts, republics or autonomous okrugs (see figure 2). Second, despite the existence of 90 regional network segments, nodes are not equally distributed across Russia's regions. Most are concentrated in a few urban centres. Three cities—Moscow, St. Petersburg and Ekatarinburg—account for more than 70 per cent of all nodes, with Moscow alone representing a 40 per cent share. It is clear that urban Russians, particularly those living in the major administrative, scientific and industrial enclaves, are more likely to be connected than those living in rural areas or the regions, a pattern not unlike the distribution of telephony. Third, despite the overall increase in Russia's

³³ The problems include a lack of correlation between the address of virtual networks and their actual physical location, the lack of consistency in geographic domain names, and the tendency of Moscow-based providers to delegate their net addresses to regional clients.

³⁴ This was partially a result of greater competition among ISPs, but also a matter of practicality as the mushrooming numbers and the share of clients held by regionally-based ISPs made compiling a unified directory impractical.

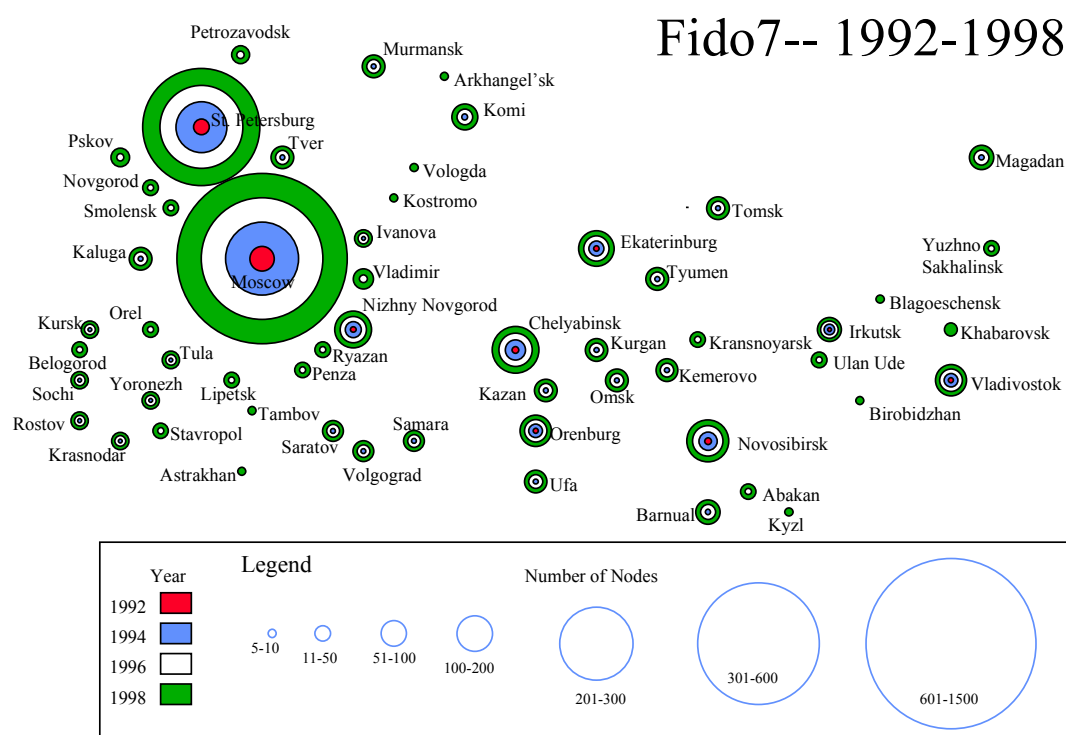
³⁵ I am presently compiling a detailed map taking into account all of these variables (Rohozinski, forthcoming).

³⁶ Fidonet offers a good measure of penetration for other reasons. First, since it is a non-commercial amateur network, the incidence of Fidonet nodes in any locale is a good indicator of the general level of computerization and knowledge of networking. Second, the absence of Fidonet is a good indicator of the Net's socioeconomic penetration. If a network other than Fidonet exists, it is safe to assume that access to it is more restricted by socioeconomic variables (like cost or membership in a university) (Dubovai, 1995; Paliev, 1998; Kochegarov, 1996). As there are no formal schools for the Internet, many professional *Setoviki* cut their teeth on the Fidonet and many continue to be Fidonet *aficionados*.

computerization levels and the increasing quality of telecommunications infrastructure in the regions, the disparity between the Moscow-St. Petersburg axis and the rest of the country appears to be increasing rather than narrowing.³⁷

Finally and overall, we see that under 40 per cent of the registered voting population have the remotest possibility of access to the Net. This is certainly an important figure to bear in mind when making pronouncements about the Net's ability to influence the society as a whole.³⁸

Figure 2
Fido7: 1992-1998
Regional distribution and penetration of Fidonet



This tour of the Russian Net has revealed a variegated terrain. The Net's outreach is limited and concentrated, bound by geography, infrastructure and other more subtle socioeconomic factors. This feature alone should make us sceptical about

³⁷ A thumbnail comparison of these results with preliminary figures for the Russian Internet appears to bear out the same pattern. While many regional urban centres are achieving Internet connectivity (as opposed to e-mail only), three cities—in this case, Moscow, St. Petersburg and Chelyabinsk—appear to account for more majority of all Russian Internet domains (Tutubalin, 1998).

³⁸ In another vein, technically derived inventories of Web presence on the Russian Net can allow us to see whether political parties, representative and administrative bodies are present on the Net. In this respect, it is clear that neither political parties nor representative bodies have made an overt effort to leverage the Net as part of their political or civic outreach. As of June 1998, only 19 of an estimated 180 registered political parties in Russia had a presence on the Web. Similarly, only 62 regional and city-level bodies (out of a total of several thousand) have done likewise. While these figures are rising, they represent a fraction of the 22,000 registered World Wide Web sites on the Russian Net (Rambler, 1998).

grand claims regarding the Net's democratizing potential. However, while the Net is not accessible across the whole of Russian society, it has played a role in defining a protected space for extending and facilitating components of civil society—including during the Soviet era, when civic space was tightly circumscribed by the state. It is to this issue—the Net as a social meeting place, as cyberspace—that I now briefly turn.

NETWORKS AND THE DIALECTICS OF CONTROL

The emergence of Russian cyberspace in the late 1980s (prior to the dissolution of the Soviet system) presents a fascinating puzzle. How is it that the concerted efforts of the Soviet state to build functioning computer networks—at a time when the state still wielded formidable control—failed rather abysmally, whereas the “private” networks, which were built outside state control, attracted thriving user communities? Framing a perspective on this question requires an appreciation of the Soviet social order within which Russian cyberspace emerged. In particular, it requires an appreciation of the dialectic between the Soviet state's pervasive pursuit of social control and the strategies of counter-control pursued by individuals.³⁹

Soviet ideology vociferously denied the market as a mechanism for exercising social, political and economic control. Unlike the United States (or most of Western Europe), the challenge of control⁴⁰—that is, *the need to develop organizational and technological solutions to address issues of management and governance in industrially complex societies*—was assigned to a single party, which assumed control over all aspects of political, social, and economic behaviour (and which supposedly represented the interests of the people). The Soviet system of social control assumed that non-state social space—“civil society”—was unnecessary and hence non-existent (Kaminski, 1992).

Of course, in reality Soviet society did not conform to this ideological blueprint.⁴¹ Rather, the often contradictory relationship between centralized state and party

³⁹ I see computer networks as fulfilling much the same function as social networks. As such, they are a mechanism for the exercise of social power. Like markets or hierarchies, they function to distribute, aggregate, and express different forms of control and counter-control. But unlike either markets or hierarchies, structures or formal rules do not necessarily bound networks. The power of networks lies in their flexible and amorphous nature, adapting to the needs of their changing membership (Mitchell and University of Zambia, Institute for Social Research, 1969; Thompson and Open University, 1991).

⁴⁰ Following Beniger (1986), Mattelart (1994) and Mulgan (1991), one can say that modern industrial societies struggle to manage and co-ordinate the flow of economic goods and services in an environment where technological means outpace the capacity for organizational change. This situation accentuates the need for mastering technologies of communication whose task it is to act as the medium through which information vital to management can be prioritized and acted upon. As Beniger contends, the “control revolution”—the phenomenon of new technologies of production leading to the creation of new technologies for managing and marketing production—underpins modern conceptions of the information society, in which information challenges industrial capital as the major motor of economic expansion.

⁴¹ Indeed, as some authors contend, the history of the Soviet Union can be seen as a series of cascading “*perestroikas*”. From the NEP through Stalin's war communism, Khrushchev's

control, and the needs of everyday survival as experienced by the Soviet population, resulted in two distinct spheres of existence: the public or official sphere that upheld (at least rhetorically) the proscribed norms of the institutional order; and the private or unofficial sphere that reflected the quite different norms of everyday life.⁴² We will look at these two spheres in turn.

NETWORKS OF CONTROL: THE PUBLIC SPHERE

The official or public sphere was dominated by the values and norms prescribed by Marxist-Leninist ideology as interpreted by the leadership and apparatus of the Communist Party of the Soviet Union (CPSU) and enforced by a “mighty complex of information and education.”⁴³ These ideologically derived norms and structures were embedded in a complex political and administrative hierarchy. At the state level, the apex of the central planning system was the Politburo of the Central Committee of the CPSU, which presided over the dense hierarchy of centralized political institutions and economic ministries (e.g., the Central Committee, the Cabinet of Ministers, Gosplan, Gossnab, the Presidium of the Academy of Sciences and the various constituent all-Union ministries and institutions). It was this mammoth impersonal bureaucratic centre that made decisions affecting all aspects of Soviet life, from determining where citizens could live, to prescribing the number of bobby pins produced by the national economy. At the social level, the ideological norms that were meant to buttress the state apparatus were conveyed to the individual citizenry through a number of channels: from the values and practices of educational and cultural institutions, children’s organizations and the military, to the “ideological syringe” of the centrally controlled mass media (Mickiewicz, 1997). At more elite levels, adherence to the system was reinforced by the privileges inherent in membership in the Communist party *nomenklatura*.

Co-ordinating the minutiae of administrative detail inherent to this vast, complex system represented a major challenge of control. As such, it is not surprising that Soviet leaders welcomed the advent of computerization, seeing it as the technological solution for a myriad of central planning needs. Thus, throughout the 1970s and 1980s, Soviet leaders proclaimed the need to harness science and technology in the service of developed socialism. From the Brezhnev-era call for a Scientific and Technological Revolution (STR) to Gorbachev’s programme of *uskorenie* (acceleration), science and technology were hailed as the solution to the future production and management challenges of the Soviet system (Hoffmann and Laird, 1985).⁴⁴ However, it seems that Soviet leaders never really developed a common vision concerning the role that information technologies were to play in

thaw and economic reorganizations, the Kosygin reforms of the mid 1960s, and Brezhnev’s “Little Deal” of the 1970s, systems of control have changed, alternating between continuity and reform (Castells, 1998; Castells and Kiselyova, 1995).

⁴² See, for example, Shlapentokh, 1986; 1989; Kaminski, 1992; Temkin, 1996; Ledeneva, 1998).

⁴³ Here I adopt Remington’s perspective, in which ideology is conceptualized as “an organized network of institutions imposing a measure of doctrinal coherence over communications”, rather than the more conventional view that sees ideology as a purely intellectual system (Remington, 1988).

⁴⁴ Indeed, to their credit, Soviet ideologues were among the first to recognize the critical importance of science and technology as productive forces (Hoffmann and Laird, 1985).

extending their ability to control and manage centrally (Judy and Clough, 1989). Thus, despite the vigour of official propaganda about the utility and centrality of computers and networks to the Soviet economic model, the history of the state's official computer networking achievements is surprisingly brief. The state did pursue several high-profile programmes aimed at catapulting the USSR into the information age, but most of these efforts came to naught. Certainly, the Soviet state never conceived of, or successfully developed, networks on the scale of the US Internet.⁴⁵

The failure of official computer networking efforts, despite the top-level priority and resources they received, is a function of several factors, including institutional competition, the resistance of line managers at all levels to increased control by the centre, and the pervasiveness of Soviet bureaucratic control.

For example, during the late 1960s the state planned to create the OGSPD, a unified, all-union data network. This network was to serve the needs of two different institutions with two different purposes: to unify the planning and supply organizations of the Soviet state (Gossnab and Gosplan); and to provide a system of unified national accounting for the Ministry of Statistics (Goskomstat).⁴⁶ Gosplan wanted a network with which to manage the operations of all branches of the economy; Goskomstat wanted a network to accumulate statistics from which future planning could be derived. The project was stymied from the outset. At the highest level, technical difficulties and administrative in-fighting between the two institutions—mostly over which one was to control the network—plagued the project. Further down the hierarchy, the project was resisted by line-level managers and directors who believed that the resulting network (with its increased transparency and control potential) would undercut their flexibility to “manage” (and control) their affairs (which often involved subversion of central prerogatives for personal gain). By the early 1970s, it was clear that the project was at an impasse. Consequently, the plans were scaled back and the delivery of the network postponed indefinitely. By the end of the Soviet era, only segments of the OGSPD were operational.⁴⁷

Official networking efforts were also stifled by bureaucratic control within Soviet institutions, at all levels. For example, by the end of the 1980s, two non-classified, state-run, all-union computer networks came into existence. The first network—*Akademset*—was designed to interconnect the Institutes of the Academy of Sciences. However, it was used at less than 4 per cent of its capacity and there is strong evidence that, despite official accounts to the contrary, the network never actually worked at all, except in what its managers termed “an experimental

⁴⁵ In point of fact, talk of creating an ARPANET-like network did appear in the early 1980s, with some Western analysts noting Soviet plans for the creation of an *Interiset* (literally translated as Internet), presumably a CMEA response to the Internet (McHenry, 1988). However, there are no traces that these plans ever amounted to anything.

⁴⁶ See Cave, 1980; United States Central Intelligence Agency, Office of Soviet Analysis, 1987.

⁴⁷ Later, during the mid 1970s, Gosplan attempted to go it alone and focused on trying to build a more limited network for managing certain branches of the economy, but again resistance by enterprise directors limited the success of this venture (United States Central Intelligence Agency, Office of Soviet Analysis, 1987).

regime”—a euphemism for the fact that no one used it.⁴⁸ Indeed, most of the people I interviewed from the Academy of Sciences claimed they were not aware that such a network had existed at all.⁴⁹ Others believed that the network had been meant “for administration of the Academy” and not “for researchers”, and that for this reason the nodes were located in secure offices, accessible only by “specially qualified cadres”.

The second official network—IASnet—was designed to give Soviet academics access to the databases held by the All-Union Centre for Data (VNITI) as well as Western databases and networks (including the Internet).⁵⁰ IASnet did establish a substantial internal network and several international connections; but Soviet academics who wanted to use this network were faced with a time-consuming prospect. First they had to pass their requests through a variety of bureaucratic gatekeepers—at their home institution and at VNIPAS—for basic approval. From there, the requests would be given to qualified “specialists” who would perform the needed research and pass the results back down to the researcher through the appropriate reporting chain.⁵¹ Thus, far from providing a quick and convenient method for conducting research and contacting colleagues, IASnet often involved extra work and bureaucratic headaches. Most academics could not be bothered, and IASnet languished.

In short, the official state-run networks that did emerge were analogues of the existing bureaucratic structure, subject to the same bottlenecks and controls, and

⁴⁸ Interview with Vladimir Serduik, former Deputy Director Institute of Automated Systems, November 1998.

⁴⁹ Including several former institute directors and deputy directors.

⁵⁰ IASnet (i.e., Institute for Automated Systems Network) was housed at the Moscow-based All-Union Institute for the Problems of Automated Systems (VNIPAS). By the late 1980s, VNIPAS was the most connected “open” institute of the Soviet era, with 11 international connections. Among its accomplishments, VNIPAS is credited with establishing the USSR’s first openly acknowledged connection to global data networks and the basis for Minsviaz’s X.25 service (Rospac) (Dizard and Swensrud, 1987). In the mid 1980s, VNIPAS was the focal point for a private US attempt to create a peace bridge between East and West. Largely through the efforts of Joel Schatz, a California-based businessman, a connection between VNIPAS and the United States was created, which later became the non-profit San Francisco Moscow Teleport (SFMT) and, later still, Sovam Teleport. Other, more “closed”, networks also possessed international connectivity, and invariably access to the Western Internet. The Institute for Space Research (IKI), a relatively open academic institution, for example, possessed a connection the European Space Agency in France; and from there, it had access to the NASA network at the Goddard Space Centre in Virginia. The Institute’s deputy director described to me how the system worked in practice. The physical line terminated in a special room that remained under lock and key at all times. When an IKI staff member needed to transmit or receive files from abroad the information was prepared on separate magnetic tapes. These tapes were then taken to the special room and loaded onto computers dedicated to securing the international connection. Only then did specially designated personnel effect the transfer.

⁵¹ Even when direct communications between Western and Soviet academics became possible during the late 1980s, the use of IASnet was often mediated by VNIPAS staff. Soviet researchers would bring their written communication to staff who would then send it to a Western partner. In turn, when a message was received, the Soviet researcher would be notified to pick the message up from VNIPAS (Cole, 1994). In this respect, IASnet is not comparable to the early Internet, or any other Western academic network, where access was relatively unrestricted (at least to those working in the institutions where connectivity existed).

even more stultified than other, more established, communications channels. In the final analysis, official Soviet-era computer networks failed to attract users because they reflected and reproduced the ossified structures of the larger Soviet “public sphere”.

While state-directed initiatives withered, privately run networks flourished, often with the tacit agreement of the same line managers and directors who resisted official networking efforts. By 1991, it was these hidden networks—born out of private interests and existing outside of the official sphere—that formed the largest and fastest growing segment of Russia’s emerging Net. Understanding how and why these private networks came into being requires exploration of the space that they provided to individuals. This space—cyberspace—allowed social actors to leverage individual power against the over-controlling institutions of state, and thus to reclaim some of the civil space precluded in the Soviet model of governance.

NETWORKS OF EVERYDAY LIFE: THE PRIVATE SPHERE

The Soviet official sphere of life had its antithesis in the private or informal sphere of everyday life—the “reverse-side of an over-controlling centre, the reaction of ordinary people to social constraints they faced” (Ledeneva, 1998). Despite the ideologically prescribed efficiency of the centrally planned system, real life was characterized by shortages, conflicts and other failings. As such, individuals needed to develop strategies to redress grievances and to subsist professionally, socially and economically. These strategies involved the exploitation of social contacts and professional positions to build up informal social networks—or *blat* as they are known in Russian—through which they expanded their personal power within and against the dominance of institutions.

On an individual level, *blat* networks allowed people to leverage and use personal *positional power* to facilitate the process of obtaining “all-too-everyday goods and services” (Ledeneva, 1998:1). On a systemic level, *blat* acted as an “elaborate and all pervading old-boys network” (Crankshaw cited in Ledeneva, 1998). that facilitated the workings of the otherwise paralysing bureaucracy and catalysed co-ordination across the various functionally distinct institutional hierarchies of the Soviet party and state system. Thus, while *blat* actually helped the system to function, it also gave individuals some measure of control over the “who-gets-what” decision making that was supposed to be the sole prerogative of the state.

An important aspect of *blat* was the value it attributed to good information. Information was far more valuable than money in the Soviet Union, mainly due the possibilities it opened to those had access to it. Good information could range from the best time to queue for bread at a particular store, to advice about when an institute director should invite an important superior to ensure support for a pet project.

In fact, information manipulation is present in all societies—used as a mechanism to buttress the status quo and to further individual interest. However, its importance was greatly accentuated and distorted in the USSR for a number of

reasons. First, the sheer geographical enormity of the country and its relatively underdeveloped communications infrastructure caused considerable isolation of communities. Information could not travel easily, and this increased its value. Second, and more important, the overwhelming importance of administrative decisions, and the relative unimportance of money, meant that information and access to information became, in effect, the “currency” of the system—a commodity in an economic system where money existed as a unit of account rather than a unit of allocation.⁵²

Seen in this context, the unofficial Net that emerged in the closing years of the 1980s was an important facilitator in the exchange of informational currency among colleagues and friends. The Net provided those who had access to it with the ability to benefit from information, unfettered by the hierarchical filters of the “public sphere” order, or by geography.

Although the unofficial Net was built by cyber-entrepreneurs in order to accomplish their own private aims, its nodes were actually housed in public institutions, using public funds and infrastructure. As such, it represents a graphic example of the private subversion and re-colonization of the public sphere: the same institute directors and senior managers who viewed *Akademset* and other official networks with suspicion (and subtly subverted their functioning), supported the efforts to establish unofficial network nodes within their institutions. In part, and especially after 1991, this was driven by the recognition that these nodes could provide a much needed source of revenue, and in some cases a *raison d’être* for the institution. More importantly, unofficial networks were a means to leverage informational capital. Thus, for example, scientists and academics recognized that the Net allowed them to bypass the formal bureaucratic hierarchy to access colleagues, funding and provided a means to organize travel and publication that had been hitherto unthinkable. Similarly, enterprise directors and entrepreneurs of all kinds recognized the enormous value of knowing local prices of goods and leveraging the local shortages inherent in the Soviet system to realize huge profits. On another level, access to the Net permitted people to extend their circle of acquaintances across a broad community, yet within what effectively constituted the “private” or informal sphere, freed from the constraints of time, space and hierarchy.

The deeply personal and informal aspect of Russian cyberspace was reflected in the pattern of growth exhibited by Relcom/Demos during its early years. Relcom began as part of a “private” effort between a group of Moscow programmers from the Kurchatov Institute of Atomic Energy (KIAE) and the physics faculty of the Moscow State University who were trying to develop a Russian version of the UNIX operating system. The first triangle of nodes was set up between professional acquaintances who worked, respectively, at the Demos Lab, the Kurchatov Institute, and a joint venture called “Dialog”.⁵³ Throughout 1990/91, as

⁵² See, for example, Bellows, 1993; Shmatko, 1995; Temkin, 1996; Ledeneva, 1998.

⁵³ Relcom’s first connection to the Internet follows a similar “personal script.” In August 1990, a computer engineer, Leo Tomberg, visited some colleagues at Demos in Moscow. His colleagues had just purchased a new modem and were in the midst of testing it. They decided to try to connect to a server in Finland because a colleague of Leo’s had recently been there as a visiting academic and still had his password and account on the University Internet server. Within a few hours, the assembled team had poked around the Finnish server enough to arouse the attention of its administrator. Shortly thereafter rapport was

Soviet-era institutions began their decline, the Relcom networks spread through personal contacts among colleagues, encompassing an ever-expanding range of institutions, linked by personal or professional circles of interest. So clubby was this environment that Relcom did not start using a second-level domain system (i.e., one that reflects the geographic location of a node) until after the 1991 coup, when the number of nodes expanded exponentially. Even as late as 1992/93, knowledge of Relcom spread primarily through personal contacts rather than more public channels such as advertising.

By 1992/93, state funding began to dry up and Relcom became a pay-as-you-go network.⁵⁴ This commercialization gave further importance to the Net, and also began to transform the nature of its “space,” away from a purely private channel among professional colleagues, to a more “virtual” forum that increasingly took on market-like characteristics.

Commercialization opened up Relcom’s access to a new generation of Net users—entrepreneurs who recognized its power to fill the vacuum caused by the collapse of Soviet-era economic planning and distribution mechanisms. The end of central planning meant the collapse of the old hierarchical contacts between central ministries and regional enterprises, which had previously determined the allocation of raw materials and the disposal of finished products. In the absence of a functioning market, Relcom helped to fill the void, as it hosted newsgroups dedicated to the sale and trade of commodities and goods, which acted as a virtual electronic commodities exchange (*elektronaya birzha*) (Interviews with Relcom staff, 1992).

Commercialization also moved Relcom “upscale”, with its user fees placing it beyond the reach of many potential users, even those with the means to own or use a computer. As a consequence, those potential users whose interests remained more social than entrepreneurial sought out a different network system: Fidonet.

Fidonet was built entirely upon contacts between acquaintances.⁵⁵ But unlike Relcom, Fidonet remained decidedly non-commercial, built upon a desire to network with colleagues rather than by any commercial or institutional motives.⁵⁶

struck, and this culminated, on 13 September 1990, with Demos registering the domain <.su> (Soviet Union) as the “official” address of the (then) Soviet segment of the Internet. All of this, needless to say, occurred without the knowledge or agreement of anyone outside of the Demos team.

⁵⁴ In the early years, Relcom nodes subsisted on “privatized” public funds. That is to say, they were located in state institutions which paid for the computers and telephony charges, but the nodes themselves serviced the private needs of their operators.

⁵⁵ Interestingly enough, unlike Relcom, which spread from Moscow outwards, Fidonet first appeared in Novosibirsk during 1990 and spread to Moscow through Chelyabinsk (Fido7, 1998).

⁵⁶ There are several possible reasons for this. First, Fidonet represents a primitive computer technology—designed to operate on the most primitive of PCs—and does not require knowledge of UNIX or any other hardware-hungry software. Consequently, unlike Relcom’s dependence on facilities available only at state institutions, Fidonet could exist anywhere there was a PC and modem. Second, Russia’s Net is largely an off-line phenomenon. Consequently, the differences between the kinds of service available from Relcom and Fidonet are marginal. Messages from Fidonet can be sent to the Internet and vice versa. In contrast to Relcom’s commercial services and to the relatively elite status of Russia’s academic and research networks, Fidonet is “proletarian” in nature, giving anyone

That Fidonet is a social network is clearly evidenced by comparing Relcom and Fidonet newsgroups. At present Relcom carries 169 newsgroups, a minority of which possess a social character. By contrast, Fido7 carries between 1,569 and 1,737 newsgroups (depending on the regional net) encompassing a vast array of interests ranging from discussion of beer, science fiction, collections of anecdotes, to serious academic meditations.

The reasons for Fidonet's success go beyond a simple reaction against Relcom's commercialization. Undoubtedly, its technical simplicity, free cost and type of services are attractive. In addition, however, Fidonet appears to have taken over the role once fulfilled by Relcom prior to its commercialization, namely, as a back-channel for social networking. Interestingly, many institutions appear to have both a Relcom and a Fidonet connection: the Relcom network tends to be used for institutional and business needs, while Fidonet is used more for informal social networking.

In part, Fidonet's informality is reinforced by the manner in which one becomes a member of the Fidonet community, which is rather like becoming a member of a secret society.⁵⁷ The following narrative is an amalgam of those told to me by several inducted *Fidoshniki*.

Typically, you would find out about Fidonet through a friend or colleague who was a user, sometimes even indirectly. You would call the *Fidoshniki* and ask him if you could join. Usually, you would arrange to meet for a beer or coffee somewhere and he would give you the diskettes containing the Fido programme and the telephone number of a few nodes. You would then struggle for a few days trying to get the software to work and start calling the nodes whose number you were given. As a visitor, your "privileges" would be limited, so you would have to contact the nodemaster for permission to become either a sub-node or a point. Everything would be done informally, especially the rules and conflicts of life in Fido. Your willingness to participate and contribute time to maintaining the Net would determine over time whether you could become either a newsgroup moderator or a co-ordinator of several nodes.⁵⁸

Fidonet's communal feel is enhanced by the fact that, unlike the Internet, Fidonet users and node operators must follow certain rules. While these rules are not draconian, the consequences of not following them are excommunication from the

with an inclination the opportunity to use it. Third, language is another possible factor. Although in recent years great strides have been made in supporting foreign language content on the global Internet, it remains heavily dominated by the English-speaking world and, more specifically, by its "America-centric" culture. This was particularly true in the early 1990s, when both Fidonet and Relcom made their appearance in the USSR. The relative absence (until recently) of Russian language content, and the simple fact that the majority of Russian Net users are not English readers, limited the appeal of the Internet's global reach. The fact that the Internet is global makes it no less inaccessible for those who have no need or desire to learn English. Fidonet, from the outset, was entirely a Russian language phenomenon and remains to this day a linguistically bounded community.

⁵⁷ Fidonet remains unadvertised, and there is no readily accessible public server providing the software and rules needed for Fido membership. An exhaustive search of the Russian press has only yielded three references to Fidonet over the past eight years.

⁵⁸ See also Dubovai, 1995.

network.⁵⁹ Overall, Fidonet demands greater personal investment by its users than other computer networks. At the same time, the community of *Fidoshniki* has expanded from its initial core of professional computer aficionados to a wide range of users, including artists, musicians and scientists. In short, it involves a good cross-section of professional Russian society itself.⁶⁰

SUMMARY AND PERSPECTIVE: THE SOCIAL SIGNIFICANCE OF RUSSIAN CYBERSPACE

Our exploration of Russian cyberspace suggests that, in the Soviet era, the Russian Net provided a space in which individuals could exercise some modicum of power against Soviet Russia's ossified bureaucratic order. The Russian Net—built upon the cultural tradition of personal *blat* networks—served to extend and empower those social networks by “routing around” the hierarchical dominance of the institutional order, while providing a mechanism for the exchange of much-coveted private information. In this sense, the virtual space that the Net created—cyberspace—acted as a kind of surrogate civil society, a space that allowed for the unfettered pursuit of personal contacts and group interests outside the strictures of the Soviet institutional order.

The Net's role in countering the 1991 coup represented a “Big Bang” of sorts, by exposing the latent power of this networked civil society and its previously submerged social networks. In this sense, the significance of the Net's mobilization in 1991 was less political than it was a practical demonstration of social empowerment. Members of Russia's cybercommunity actively mobilized against the coup because they perceived it as a threat to their communal space—cyberspace. The scale of the threat was augmented by the coup-makers' immediate takeover of most communications media, and the perceived risk that a successful coup would reimpose a return to hierarchical orthodoxy and communications control.⁶¹ The cybercommunity's mobilization—circulating vital information between Moscow and the regions and thereby helping to organize the opposition—circumvented the very factors that the coup plotters had counted on for imposing the state of emergency, namely their control of the media, the hierarchical ordering of Soviet society, and the social isolation imposed by Russia's immense geography.⁶²

⁵⁹ The rules of Fidonet are embedded in its guiding policy document and include the following: member nodes are to actively participate in the operation of the network, meaning that they have to be available at set times to receive and send onward mail; node operators are not allowed to read transiting mail; newsgroups, the most popular method of communication, are moderated; and a Fidonet member can be excommunicated for any activities judged excessive or inappropriate by the duly elected co-ordinators of the network.

⁶⁰ Information based on interviews with past and present *Fidoshniki*, including several past co-ordinators of Fido7, November 1997.

⁶¹ This information is based on interviews with the Net's operators and users. For an extended discussion, see Rohozinski, forthcoming.

⁶² Another consequence of the Net's successful “surfacing” in 1991 was to attract more Russians into cyberspace, thereby extending and deepening the boundaries of Russia's cybercommunity.

Since 1991, Russia has undergone several political spasms of greater or lesser importance: the 1993 constitutional crisis, the 1995 war in Chechnya, and the 1996 Russian presidential elections. However, in none of these crises has the Net community mobilized with the spontaneous single-mindedness that occurred in 1991, because the more recent crises have not been perceived to threaten the very space that the Net inhabits. As such, the use of the Net for subsequent political actions has focused on specific issues, with subsections of the Net community mobilizing around a plethora of individual issues. For example, Russia's ISPs have begun to organize a political lobby around the issue of regulation, while Fidonet users in Moscow have organized demonstrations in opposition to the imposition of per-minute telephone charges.⁶³ I take this as a sign of normalization, representing a confident networked community and reflecting the heterogeneity of opinion inherent in Russian society itself.

In the post-Soviet period, several factors would seem to suggest a decline in the importance of the social functions of Russian cyberspace. For example, the dissolution of the Soviet system of state control would seem to devalue the Net's role as a civic space for circumventing the strictures of a proscriptive institutional order. Moreover, the monetization of the economy would suggest a decline in the overarching importance of *blat* networks as means for exchanging informational currency. However, it is clear that Russia's cybercommunity, and the outreach of its Net, has continued to expand. The Net's ongoing development, I would suggest, is a testament to its continued social utility as a "back channel" for informal social and professional networking. Thus, while the administrative power of the unitary party-state has disappeared, it has been replaced by the concentrated economic and political power of a new post-communist capitalist class.⁶⁴ Moreover, while Russia remains a geographically vast and relatively underdeveloped country, its regional imbalances have increased in the post-Soviet period, fuelled by the decline of all-Russian institutions and new economic disparities. Geography, money and access to infrastructure have become new obstacles, limiting the ability of Russia's citizens to participate freely in society. In this context, the Russian Net—despite its limited penetration of Russian society—continues to allow its users to "route around" the old and new obstacles of Russia's geographic enormity, its relative underdevelopment, and its post-Soviet economic and political disparities.

In a different vein, a new factor potentially affecting Russian cyberspace is the Russian state's recent interest in asserting a measure of control over the Net.⁶⁵ For example, a recent Presidential Decree has banned the use of encryption algorithms or devices unless they are certified by FAPSI (*Federalnoye Aгенstvo Pravitel'svey Sviazi i Informatiki*), Russia's version of the US National Security Agency.⁶⁶ In addition, FAPSI has tried to own a section of cyberspace by positioning itself as a provider of secure network services through a joint venture with Relcom. To date, neither effort has yielded any significant results: the Presidential Decree has been mostly ignored and unenforced, while the FAPSI-Relcom venture fell victim to political scandal (Borisov, 1997). Nevertheless, both initiatives are indicative of

⁶³ See, for example, Gosduma, 1996.

⁶⁴ See, for example, Voronkov, 1993; Medushevskii, 1995; Shlapentokh, 1995; Shmatko, 1995.

⁶⁵ See, for example, Markomenko, 1997; Ruchkin, 1997.

⁶⁶ See, for example, Lorent, 1997; Yeltsin, 1995.

the state's interest in defining, dividing and controlling a corner of Russian cyberspace.

Overall, Russia's network segments continue to expand along specialized lines, each adding to the texture of Russian cyberspace without fragmenting the totality of the Net, and supported by the diffuse nature of ownership. In this respect, although Russian cyberspace is a more crowded and less collegial place than during the Soviet era, its various segments continue to act as a means for redressing the imbalance between the newly dominant social actors and ordinary individuals, at least those who are connected. Given the relatively elitist state of Russian cyberspace, it would be misleading to draw any direct relationship between democracy and the Net. Nevertheless the Net continues to provide a space where connected individuals and civic groups can communicate and, at times, organize themselves against certain of post-Soviet Russia's anti-democratic tendencies.

This paper began with a revolt against what I termed the "Barney Syndrome"—the analytical tendency to assume that the existence of connectivity implied some sort of social impact across the whole society. This grounded analysis of the limits of the Russian Net, and the social forms of its cyberspace, has demonstrated the need to develop a carefully nuanced and contextualized perspective on what we mean by "the Net" before we can begin to extrapolate about its transformative potential for any society. But from a broader perspective, does the Russian case provide any lessons for the study of the Net worldwide? I would argue that the answer is a qualified yes. On one hand, the Russian case appears to bear out John Perry Barlow's oft-quoted observation that the Net routes around obstructions. That is, it can facilitate the exercise of social agency that would otherwise be circumscribed by dominant social actors. In this sense, we could suggest that cyberspace may represent a forum for a civil society adapted to the peculiarities of the information age—a civil society that leverages the technological infrastructure of modern industrial societies. On the other hand, the Russian case also highlights the factors that preclude membership in a virtual civil society—education, socioeconomic means and underdevelopment. In a very real sense, the global Net, like its Russian segment, remains a relatively elitist phenomenon, more the preserve of large and often privileged interest groups than of society writ large. Finally, like previous technological artefacts, the Russian Net's scope and character, and that of its attendant cyberspace, are strongly embedded in its specific socio-cultural context, bounded by language and the specific needs of its users. The Russian case reminds us to be cautious in our tendency to conceptualize networks as a universal social technology, unbounded by the norms of human societies and behaviour. Perhaps we need to adopt an anthropological approach to cyberspace, which is as much defined by culture, language and circumstance as any other area of human endeavour.

BIBLIOGRAPHY

- Bellows, H. (1993)
“The challenge of informationalization in post-communist societies”,
Communist and Post-Communist Studies, 26(2):144-164.
- Belsie, L. (1991)
“Technology thwarted coup leader success”, **Christian Science Monitor**,
9.
- Beniger, J.R. (1986)
**The Control Revolution: Technological and Economic Origins of the
Information Society**, Harvard University Press, Cambridge,
Massachusetts/London.
- Borisov, G. (1997)
“FAPSI: connection with the mafia?”, **Novoya Gazeta**, Moscow.
- Buben, M. (1995)
“Russian internet through the eyes of Russian science”, **Posik**, Moscow, p.
3.
- Cairncross, F. (1997)
**The Death of Distance: How the Communications Revolution will
Change our Lives**, Harvard Business School Press, Boston.
- Campbell, R.W. (1995)
**Soviet and Post-Soviet Telecommunications: An Industry Under
Reform**, Westview Press, Boulder, Colorado.
- Castells, M. (1998)
End of Millennium, Blackwell Publishers, Malden, Massachusetts.
- Castells, M. and E. Kiselyova (1995)
**The Collapse of Soviet Communism: A View from the Information
Society**, International and Area Studies, University of California,
Berkeley.
- Cave, M. (1980)
Computers and Economic Planning: The Soviet Experience,
Cambridge University Press, Cambridge.
- Cole, M. (1994)
**An Experiment in Computer-mediated Co-operation Between Nations
in Conflict**, Laboratory of Comparative Human Cognition, University of
California, San Diego.

- Cook, G. (1992a)
Russian Telecommunications After the Revolution: New Perspectives on Infrastructure Creation, Cook Network Consultants, Ewing, New Jersey.
- _____. (1992b)
Russian Telecommunications: Crisis Creation of Infrastructure in 1992, Cook Network Consultants, Ewing, New Jersey.
- Dizard, W.P. and S.B. Swensrud (1987)
Gorbachev's Information Revolution: Controlling Glasnost in a New Electronic Era, Westview Press, Boulder, Colorado.
- Dubovai, L. (1995)
"The telecommunications game has become an example of life", **Computer World Kiev**, 24(47):10 (interview with Sergie Gulchuk).
- Fido7 (1998)
Fidonet. History FAQ, (<http://www.fido7.com/doc/fpol4xx.txt>).
- Flek, F. (1992)
Russia's Parallel Phone Lines Open Subscribers, Reuters Information Services.
- Gosduma, 1996
Parliamentary Hearing on the Topic of "Russia and the Internet: The Choice of the Future", Russian House of Parliament.
- Goskomstat (1997)
Regions of Russia: Official Statistical Handbook, Goskomstat Russia, Moscow.
- Graham, S. and S. Marvin (1996)
Telecommunications and the City Electronic Spaces, Urban Places, Routledge, London.
- Groves, M. (1991)
"Crisis in the Kremlin: Computers help U.S. firms track coup", **Los Angeles Times**, Los Angeles, p. 3.
- Hoffmann, E.P. and R.F. Laird (1985)
Technocratic Socialism: The Soviet Union in the Advanced Industrial Era, Duke University Press, Durham.
- Hogan, B.T. and M. (1991)
Computer Networking in the USSR: Technology, Uses and Social Effects, School of Information Studies, Syracuse University, Syracuse.
- Judy, R.W. and V.L. Clough (1989)
The Information Age and Soviet Society, Hudson Institute, Indianapolis.

- Kaminski, A.Z. (1992)
An Institutional Theory of Communist Regimes: Design, Function, and Breakdown, ICS Press, San Francisco.
- Kedzie, C. (1995)
Democracy and Network Connectivity, available on-line on <http://www.isoc.org/HMP/PAPER/134/html/paper.html>
- Klimov, V. (1995)
“Sprint or octopus?” **Rossiyskaya Gazeta**, Moscow, p. 4.
- Kochegarov, M. (1996)
“Fido: Internet’s older brother”, **Izvestia**, Moscow.
- Lawton, G. (1993)
“The end of the party line”, **Wired (Infobot)**, wired magazine.
- Ledeneva, A. (1998)
Russia’s Economy of Favours: Blat, Networking, and Informal Exchanges, Cambridge University Press, New York.
- Lorent, E. (1997)
“Keep out! Censorship has not yet been introduced into the computer network, but criminal punishment has already been foreseen”, **Novoye Vremya**, Moscow, pp. 36-37.
- Markomenko, V. (1997)
“Invisible, long drawn out war: Federal government communications and information agency meets its challenges”, **Nezavisimoye Voyennoye Obrazovaniye**, Moscow, pp. 1-7.
- Marvin, C. (1988)
When New Technologies Were Old: Thinking about Electronic Communications in the Late Nineteenth Century, Oxford University Press, Oxford.
- Mattelart, A. (1994)
Mapping World Communication, War, Progress and Culture, University of Minnesota Press, Minneapolis.
- McHenry, W. (1988)
“Computer networks in the Soviet scientific community”, **Computer Networks and Soviet Civil Science**.
- Medushevskii, A. (1995)
“The formation of ruling class”, **Sociological Research**, 36(2):31-51.
- Mendkowicz, A. (1994)
FREEnet/UNICOR: The Experience of Co-operation, NATO Advanced Networking Workshop, NATO, Golitsyno.

- Mickiewicz, E.P. (1997)
Changing Channels: Television and the Struggle for Power in Russia, Oxford University Press, New York.
- Mitchell, J.C. and University of Zambia, Institute for Social Research (1969)
Social Networks in Urban Situations: Analyses of Personal Relationships in Central African Towns (published for the Institute for Social Research, University of Zambia), Manchester University Press.
- Mulgan, G. (1991)
Communication and Control: Networks and the New Economies of Communication, Polity, Oxford.
- Network Wizards (1998)
<http://www.nw.com/>
- OECD (1992)
Telecommunications Indicators of the Former Soviet Union, ITU, Geneva.
- Paliev, B. (1998)
“Networking among friends”, **Fidonet—nekomercheskaya telekommunikatsyonaya set'dlya neformalno obshchestva**, Aktsyonarnoe obshchestvo “IKE.
- Press, L. (1991)
Relcom, an Appropriate Technology Network, California State University, Los Angeles.
- Rambler (1998)
Rambler Index of Russian WWW Sites, Demos.
- Remington, T.F. (1998)
The Truth of Authority: Ideology and Communication in the Soviet Union, University of Pittsburgh Press, Pittsburgh.
- Rohozinski, R. (forthcoming)
Mapping Russian Cyberspace: A Perspective on the Sociology of Networked Communities, Cambridge University Press, Cambridge.
- Ruchkin, A. (1997)
“Star wars being replaced by information wars”, **Rossiyskaya Gazeta**, Moscow, p. 6.
- Shlapentokh, V. (1986)
Soviet Public Opinion and Ideology: Mythology and Pragmatism in Interaction, Praeger, New York.
- ____ (1989)
Public and Private Life of the Soviet People: Changing Values in Post-Stalin Russia, Oxford University Press, New York.

- ____ (1995)
Privatisation and Illegalisation of Social and Political Life, NATO, Special Advisor for Central and East European Affairs, pp. 1-44.
- Shmatko, N.I. (1995)
“The formation of the Russian entrepreneurial system and bureaucratic capital”, **Sociological Research**, 6:23-41.
- Temkin, G. (1996)
“Information and motivation: Reflections on the failure of the socialist economic system”, **Communist and Post-Communist Studies**, 29(1):25-41.
- Thompson, G. and Open University (1991)
Markets, Hierarchies, and Networks: The Co-ordination of Social Life, Sage Publications, Newbury Park, London.
- Tutubalin, A. (1998)
Russia Internet Domain Survey, 3-5 May.
- United States Central Intelligence Agency, Directorate of Intelligence (1987)
The USSR Confronts the Information Revolution: A Conference Report, proceedings of a conference held at Airlie House (Virginia, 12-13 November), Washington, D.C.
- United States Central Intelligence Agency, Office of Soviet Analysis (1987)
Enterprise-level Computing in the Soviet Economy: A Contract Study, Washington, D.C.
- Voronkov, V.I. (1993)
“The formation of the ruling elite during the transition to democracy”, **Sociological Research**, (2):7-21.
- Yeltsin, B. (1995)
Russian Federation Presidential Edict No. 334 “On measures to ensure legality in the development, production, sale, and operation of encoding equipment as well as in the provision of information-encoding services”, **Rossiyskaya Gazeta**, Moscow, p. 5.