FIIA REPORT 35

Russian critical infrastructures

Vulnerabilities and policies

Katri Pynnöniemi (ed.)

ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

FIIA REPORT 35

Russian critical infrastructures

Vulnerabilities and policies

Russian critical infrastructures

Vulnerabilities and policies

Katri Pynnöniemi (ed.)

ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

WWW.FIIA.FI

FIIA REPORT 35

Reports can be ordered from the Finnish Institute of International Affairs.
+358 9 432 7707
erja.kangas@fiia.fi

All FIIA reports and other publications are also
available on our website at www.fiia.fi.

Language editing: Lynn Nikkanen
Graphic design: Nordenswan & Siirilä Oy / Tuomas Kortteinen
Layout: Tuomas Kortteinen
Printed by: Suomen Yliopistopaino Oy –
Juvenes Print, Tampere 2012

The Finnish Institute of International Affairs
Ulkopoliittinen instituutti
PL 400
00161 Helsinki
Finland

www.fiia.fi
firstname.lastname@fiia.fi

ISBN 978-951-769-364-6 (print)
ISBN 978-951-769-365-3 (web)
ISSN 1458-994X

The Finnish Institute of International Affairs is an independent research institute that produces high-level research to support political decision-making and public debate both nationally and internationally. The Institute undertakes quality control in editing publications but the responsibility for the views expressed ultimately rests with the authors.

Contents

PREFACE 7

1. Introduction:
   The framing of the critical infrastructure policies 13
   Katri Pynnöniemi

2. The evolution of Russian policy on critical infrastructure protection 31
   Katri Pynnöniemi

3. Threats to critical infrastructure and state responses:
   The case of the 2010 forest fires in Russia 57
   Irina Busygina

4. Re-reading critical infrastructure
   — A view from the indigenous communities of the Russian Arctic 79
   Tero Mustonen

5. Conclusions and policy recommendations 105
   Katri Pynnöniemi

BIBLIOGRAPHY 109

PREVIOUSLY PUBLISHED IN THE SERIES 117

Preface

Telephones, airplanes, express trains, elevators, rotary presses, sidewalks, factory smokestacks, stone monstrosities, soot and smoke – these are the elements of beauty in the new urban environment…the rhythm of life has changed. Everything now has become lightning quick, rapidly flowing like on a film strip.
Vladimir Mayakovsky[1]

Futurists, and among them the Russian poet Vladimir Mayakovsky, envisioned the beginning of the twentieth century as the advent of the age of speed. It was a time when new inventions from telephones to tramways "transformed modern society's sense of space by connecting people in ways previously unimaginable".[2] Today, a hundred years later, the futurist vision has become reality at the global level. International business practices, information technologies and the modern way of life are all interconnected and form a space of flows.[3] The emergence of the critical infrastructure (CI) concept in the political lexicon is one aspect of this overall change. The paradox is that infrastructures that were identified as "elements of beauty" at the beginning of the twentieth century are now increasingly viewed

[1] Cited in T HARTE, *Fast Forward: The Aesthetics and Ideology of Speed in Russian Avant-Garde Culture, 1910–1930*, University of Wisconsin Press, Wisconsin, p. 3.

[2] HARTE, op. cit., p. 11.

[3] M CASTELLS, *The Information Age. Economy, Society and Culture. Vol I The Rise of the Network Society*, Blackwell Publisher, Oxford; M Aaltola, J Sipilä and V Vuorisalo, Securing Global Commons: A Small State perspective, *FIIA Working Paper,* June 2011.

in terms of trauma, chaos and unpredictability.[4] Speed is no longer everything, resilience is.[5] The collapse of the Soviet Union and the subsequent political and economic turmoil in Russia can be viewed against the background of this overall change.

Russia's "troubled transformation" has been studied extensively during the past twenty years. Indeed, it is difficult to pinpoint a theme or subject that has not been touched upon. Yet, the Russian policies on CI and on critical infrastructure protection (CIP) seem like a good candidate. Previous research has viewed infrastructures as a critical problem for economic development in Russia – something that prevents the country from realizing its economic potential and from taking full advantage of Russia's role as a major regional power.[6] At the same time, it is acknowledged that energy infrastructures such as oil and gas pipelines, refineries, and ports play a key role in Russia's bid for great power status in world politics and maintenance of its dominant role vis-à-vis neighbouring countries.[7] In the framework of business literature, the human and economic costs of bad institutions and the degeneration of physical infrastructures are offered as explanations for regional disparities in the business climate.[8] In each case, infrastructures are framed as something external – as one among many instruments required to achieve the purported goal.

The emergence of the critical infrastructure concept in general, and within the framework of Russian politics in particular, is closely related to specific infrastructure installations (such as the aforementioned pipelines), and can be linked to certain political events or phenomena (such as terrorism), but cannot be fully explained with reference to the critical state of physical infrastructures or the

[4] J BRASSET, N VAUGHAN-WILLIAMS, 'Governing Traumatic Events', *Alternatives: Global, Local, Political*, vol. 37, no. 3, pp. 183–187.

[5] Resilience refers to the ability of the economy and society to withstand catastrophes with little or no damage at all.

[6] See eg. A ÅSLUND and A KUCHINS, *The Russian Balance Sheet*, Peterson Institute for International Economics and Center for Strategic and International Studies, Washington, DC, April 2009.

[7] P AALTO (ed), *Russia's Energy Policies: National, Interregional, and Global Levels*, Edward Elgar Publishing Ltd., Cheltenham, 2012.

[8] OECD, *Infrastructure to 2030: Telecom, Land Transport, Water and Electricity*, Secretary-General of the OECD, Paris, May 2006. Accessed 3 November 2012, http://www.inst-informatica.pt/servicos/informacao-e-documentacao/biblioteca-digital/gestao-e-organizacao/0306011E.pdf; A Plekhanov and A Isakova, 'Region-specific Constraints to Doing Business: Evidence from Russia', EBRD, *Working Paper*, no. 125, March 2011, Accessed 3 November 2012, http://www.ebrd.com/downloads/research/economics/workingpapers/WP0125.pdf.

fluctuating security situation in Russia's southern borderlands. The difference has to do with the way in which infrastructures are framed as (potentially) 'dangerous', and thus 'critical'.

The argument put forward in this report[9] is that we should view the Russian policies on CI(P) against the general puzzle briefly outlined above (the age of speed giving way to the search for resilience), but also as an issue that is closely linked to the internal dynamics of Russia's hybrid regime.[10] The forest fires of 2010 are a case in point. During the fire season in 2010, it was estimated that between 5 and 15 million hectares were consumed by forest and peat fires.[11] The impact of the (peat) fires was especially severe in Moscow, where the number of additional daily fatalities was in the hundreds. Russia has suffered severe fire seasons before, but the summer of 2010 is remembered for being particularly catastrophic. As will be argued in this report (Chapter 3), there is a clear connection between regime type and vulnerability to catastrophic events.

Our purpose in this report is not to assess what a 'dangerous place' Russia actually is, nor to estimate when and where we are likely to witness the next major CI failure in the country. Instead, the report will scrutinize the situational and conceptual factors underlying Russian policies on CI. First, it will explore the evolution of the Russian policies on CIP in the context of the national security policy. Second, the report will assess the political implications of critical infrastructure vulnerability in Russia. Given the hybrid nature of the current regime, it is pertinent to ask whether the political environment in Russia actually produces rather than helps to mitigate infrastructure-related risks and vulnerabilities. Third, the report provides insights into the complex grassroots realities of CI and resilience in the face of all-out system shocks in the human societies of the Russian North – focusing on indigenous people living in two regions, Murmansk and Sakha-Yakutia.

[9] This research was funded by the Scientific Advisory Board for Defence (MATINE). The authors would like to thank Teija Tiilikainen and Arkady Moshes for their comments on the manuscript, Mika Aaltola for inspiration and Veera Laine for research assistance in compiling the research materials.

[10] R SAKWA, *The Crisis of Russian Democracy. The Dual State, Factionalism and the Medvedev Succession*, Cambridge, Cambridge University Press.

[11] O YANITSKY, 'The 2010 Wildfires in Russia. An Ecosociological Analysis', *Sociological Research*, vol. 51, no. 2, 2012, pp. 57–75; J GOLDAMMER, 'Preliminary Assessment of the Fire Situation in Western Russia', The Global Fire Monitoring Center, 15 August 2010. Accessed 3 November 2012, http://www.fire.uni-freiburg.de/intro/about4_2010-Dateien/GFMC-RUS-State-DUMA-18-September-2010-Fire-Report.pdf.

1

1. Introduction: The framing of the critical infrastructure policies

Katri Pynnöniemi

BACKGROUND: NORMAL ACCIDENTS IN A RISK SOCIETY

The emergence of the 'critical infrastructure' (CI) concept in the political lexicon in the West has been explained with reference to changes in threat perceptions and the increasing interconnectivity that make societies more vulnerable to external attacks or internal malfunction of critical nodes in the network. What has changed in recent years is the way the CI vulnerability has been reframed – from a problem emergent in the functioning of high-risk technologies – to an issue of paramount importance in the framework of national security. In this introduction we will firstly provide an overview of this wider pattern of change, and secondly, explicate our research hypothesis regarding CI vulnerabilities in Russia. The section starts with an introduction to the 1980's discussion on ecological catastrophes and risk society that provides the background to the CI conceptualization. This is followed by a brief discussion on the framing of CI as an issue of national security (in the US), concluding with a presentation of the research hypothesis regarding Russian policies on CI.

In a book first published in 1984 Charles Perrow introduced the concept of "normal accidents", which refers to the systemic vulnerability of high-risk technologies, including for example airplanes, nuclear plants, and genetic engineering. The argument put forward by Perrow was that the management of complex technologies can be improved by taking into account human- and technology-generated safety risks, but at the end of the day, accidents and major catastrophes are unlikely to be avoided due to the immense complexity of the task. Written at the time of the Cold War, the book aims to demonstrate that high-risk technologies have systemic attributes, they are "human constructions as *systems*, not collections of individuals or representatives of ideologies".[1] Perrow's critical inquiry into the nuclear power industry, DNA engineering and air traffic control systems calls into question "layers upon layers of accommodations and bargains that go by the name of tradition", that is, unintentional results of political bargaining coupled with privatization and negligent attitude to "externalities", the social costs of high-risk technologies.[2]

German sociologist Ulrich Beck's research into the risk society, first published in German in 1986, provides important insights into the implications of high-risk technologies for social and political dynamics. Beck argues that risks are an all-encompassing part of life and a paradigmatic feature of thinking about the future. In turn, the practice of mapping risks and vulnerabilities is a symptomatic feature of risk societies. Later, Beck elaborates this notion further and asks "how is the presence of future catastrophes 'manufactured'?" He draws attention to practices and techniques that have been introduced and implemented in *anticipation* of global risks. This has led to a situation where risk *assessments* and *forecasts* have become an integral part of public policy. This phenomenon has been addressed in the Foucauldian studies on biopolitics and governmentality, where "the first objects of knowledge and the targets it seeks to control are 'aleatory' and 'unpredictable', and knowable through techniques such as forecasts, statistical estimates, and overall measures that take into account both their uncertainty and their patterns over a population, rather than their reality at the level of individuals".[3]

The concept of *risk colonization* is also used to explicate a process whereby "we are no longer simply concerned with the governance *of* risk, but we are now in an era of governance *by* risk". But governance can never be complete, Henry Rothstein argues, as "inherent uncertainties, fragmented organizational settings, constrained resources, ungovernable actors and unintended consequences [...] create institutional risks that can threaten the legitimacy of

[1] C PERROW, *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, Princeton 1999, p. 351.

[2] PERROW, op.cit., p. 351.

[3] S COLLIER, 'Topologies of Power: Foucault's Analysis of Political Government beyond 'Governmentality', *Theory, Culture & Society*, vol. 26, no. 6, p. 83.

governance organizations and their practices in managing societal risks". Furthermore he points out that "the emergence of risk is not so much related to a real, or falsely imagined, change in objective threats to society, but is more related to governance systems framing and managing threats to society as risks in response to pressures to account for governance failure".[4]

Indeed, after almost thirty years, Perrow's insights into systemic vulnerabilities and Beck's research into the risk society are perhaps more topical than ever. In an afterword to the 1999 edition of the book, Perrow notes that "the accidents (Bhopal, Chernobyl, *Challenger*) we have added to our lives are a melancholy certification that nothing much has changed in the industrial world since 1984, but the publications indicate that, while we do not seem to have made any progress in preventing accidents, we have made great progress in interpreting them".[5] Today it is commonplace to think that accidents and major catastrophes are a result of multiple causes. Some of the catastrophes could be foreseen, prevented even, other mishaps emerge from the functioning of complex systems, and are just waiting to happen, as Perrow argued back in 1984. What has changed is the general framework in which accidents and catastrophes are viewed. This paradigm shift in framing certain infrastructure objects as more critical than others is due to the reinterpretation of risks and vulnerabilities with reference to national security.

'BARBARIANS AT THE GATE':
CI AND THE PROTECTION OF OUR WAY OF LIFE

In 1997 the US President's Commission authorized one of the first reports on CI where it identified eight infrastructures as "vital structures". These infrastructures were telecommunications, electric power systems, natural gas and oil, banking and finance, transportation, water supply systems government services and emergency services.[6] The report concluded that "the US was so dependent on

[4] U BECK, *World at Risk*, Polity Press, Cambridge, 2009, p. 3; H ROTHSTEIN, 'The Institutional Origins of Risk: A New Agenda for Risk Research', *Health, Risk & Society*, vol. 8, no. 3, 2006, pp. 216–217.

[5] PERROW, op.cit., p. 353.

[6] C PURSIAINEN, 'The Challenges for European Critical Infrastructure Protection', *European Integration*, vol. 31, no. 6, 2009, p. 723.

these infrastructures that the government had to view them through the lens of a national security focus".[7] Since then, this definition has been broadened and the list of critical infrastructures and related Key Resources currently includes sixteen sectors.[8] The definition of CI, offered by the OECD in 2008, includes in this category a set of infrastructures and functions that "provide essential support for economic and social well-being, for public safety and for the functioning of key government responsibilities".[9] According to the definition applied in the European Union, '"critical infrastructure" means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'.[10]

Myriam Dunn Cavelty, Head of the New Risks Unit at the Center for Security Studies in Zurich, argues that the conceptualization of critical infrastructures as part of *national security* is one aspect of the overall change in the security discourse where "aggressive intentions of states" are replaced with more "diffuse risks and the difficulties of locating and identifying enemies". She also argues that the US military has been the driving force for change in the discourse. This is mainly due to two factors, first, the expansion and diffusion of the threat spectrum after the Cold War, and consequently, a shift in thinking about possible targets, from mainly military to the 'soft spots' listed above.[11] However, we may draw a parallel between the Cold War paradigm of 'mutually assured destruction' and the CIP, whereby the latter is seen as a continuation of the previous paradigm in a new form.

During the Cold War years, the nuclear deterrence worked upon the assumption of 'mutually assured destruction'. In the 1960s, the US Strategic Air Command had 25 military targets on its radar, and

[7] E M BRUNNER, ELGIN M. and M SUTTER, *International CIIP Handbook 2008/2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, Center for Security Studies, ETH Zurich, 2009, p. 37.

[8] PURSIAINEN, op.cit., p. 723.

[9] K GORDON and M DION, 'Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security', OECD, May 2008, p. 3.

[10] Council Directive 2008/114/EC, On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, *Official Journal of the European Union*, 23 December 2008, L 345/75–L 345/82.

[11] M CAVELTY, 'Critical Information Infrastructure: Vulnerabilities, Threats and Responses', *UNIDIR Disarmament Forum*, no. 3, 2007, pp. 15–22.

151 urban-industrial centres in the Soviet Union were targeted, including steel and cement factories, nuclear factories, radio stations, oil refineries and cargo shipping and passenger transport hubs.[12] Although the possibility of unintended attack due to the malfunction of nuclear weapons or other critical sites was not altogether dismissed, the basic assumption was that 'mutually assured destruction' was a controlled action of the state.[13] As Cavelty argues above, the threat perception has changed radically whereas the critical sites have remained the same.

However, the storyline that ties the new threat perception(s) to specific infrastructure installations seems rather traditional. An editorial published in the first volume of the *International Journal of Critical Infrastructure Protection* in 2008 illustrates this point. The editorial recalls an event that led to the destruction of ancient Rome: "In 537 A.D. the Goths besieged Rome and destroyed principal aqueducts, the main component of the city's critical infrastructure". This, as the text suggests, should be seen as a forewarning as "it is possible for a malevolent entity – *from the other side of the world* – to bring down the Internet and telecommunications systems". And to make the message even clearer, it is noted that "Modern barbarians do not have to reach the city gates to wreak havoc".[14] More than any other event, it was the terrorist attacks of September 2001 ("9/11") that helped to cement critical infrastructure protection (CIP) as a part of the US, and later European security landscape.[15] 9/11 served as a starting point for preparation of the US 'national strategy for the physical protection of critical infrastructure and key assets' that was published in February 2003. The policy programme frames the issue in terms of protecting the *homeland* from "the terrorist enemy" and securing "the foundations of our Nation and *way of life*".[16]

The way in which CI is conceptualized as something that provides a basis for the Western-type *way of life* has captured the attention of critical security scholars. They point out that "critical

[12] J RISLAKKI, *Paha Sektori. Atomipommi, Kylmä Sota ja Suomi.* Juva, WSOY, 2010, p. 61.

[13] A recent article lists the known accidents in the US. See J LEWIS, 'Nightmare on Nuke Street: Twelve Terrifying Tales from the Nuclear Crypt', *Foreign Policy Journal*, October 30, 2012.

[14] S SHENOI, 'Editorial', *International Journal of Critical Infrastructure protection*, vol. 1 no. 1–2, 2008, p. 1. Emphasis added.

[15] PURSIAINEN, op. cit.

[16] *The National Strategy for Physical Protection of Critical Infrastructures and Key Assets*, The White House, February 2003. Emphasis added. http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

infrastructures perform vital roles in securing the liberal way of rule and its vision of what 'quality of life' must mean". As Michael Dillon and Julian Reid put it:

> The defence of critical infrastructure is not about the mundane protection of human beings from the risk of violent death at the hands of other human beings, but about a more profound defence of the combined physical and technological infrastructures which liberal regimes have come to understand as necessary for their vitality and security in recent years.[17]

A similar logic is recognized as playing a role in the argumentation on 'dangerous climate change'. As noted by Kevin Grove, the current discourse on this issue is "an attempt to secure Western ways of life against the effects of environmental change".[18] Studies that present climate change as 'dangerous' reproduce risk management and catastrophe insurance practices that "sustain the forms of social and political order that Western-led 'development' has produced".[19] Grove's argumentation echoes debates in the framework of *world ecology* or *world risk society* concepts from the late 1980s.[20]

However, as suggested above, 9/11 changed the security landscape, and with it the "doomsday accounts of environmental degradation as a security threat" were pushed aside.[21] The heightened sense of vulnerability and the perception of the threat from terrorism linked to it, have resulted in a quantitative proliferation of security discourse and in the "erosion of distinctions such as civil/military, legal/illegal, domestic/international, private/public and – above all – internal/external", Sven Opitz notes. Opitz refers to the targeted killing of individuals suspected of terrorism and the transformation

[17] Cited in T LUNDBORG and N VAUGHAN-WILLIAMS, 'Resilience, Critical Infrastructure and Molecular Security: the Excess of Life in Biopolitics', *International Journal Political Sociology*, vol. 5, no. 4, p. 375.

[18] K GROVE, 'Insuring 'Our Common Future?' Dangerous Climate Change and the Biopolitics of Environmental Security', *Geopolitics* vol. 15, no. 3, 2010, p. 539.

[19] For example, see C M BRIGGS, 'Climate Security, Risk Assessment and Military Planning', *International Affair*s, vol. 88, no. 5, 2012, p. 1049. See also M. BRZOSKA, 'Climate change and the military in China, Russia, the United Kingdom, and the United States', *Bulletin of the Atomic Scientists*, vol. 68, no. 2, 2011, pp. 43–54.

[20] I MASSA, 'Yhteiskuntatieteellisen ympäristötutkimuksen paradigmat ja keskeisimmät suuntaukset', teoksessa *Vihreä Teoria: Ympäristö Yhteiskuntateorioissa*, I Massa (ed), Gaudeamus, Helsinki, 2009, s. 28.

[21] GROVE, op. cit., p. 537.

of public spaces from football stadiums to city centres into surveillance sites by security companies that are granted the right to take measures against potential dangers.[22]

The focus on critical infrastructures stems from what is valued in liberal democratic societies: "the ability to keep people, services, and goods constantly on the move".[23] A traumatic event, such as a crisis, an emergency or a catastrophe, is an interruption that breaks the normal pattern of movement. However, it is a trauma that is "fast becoming a paradigmatic lens through which the dynamics of contemporary international politics are framed, understood, and responded to".[24] At the same time, research on critical infrastructure protection is framed as a "problem-solving exercise" and the questions concerning power relations sustained or produced by the "spectacle of particular events" are often not even asked.[25]

However, what has been emphasized in recent research is an understanding of critical infrastructures as *assemblages* of things that comprise human and non-human components. A port, railway line, or electric grid is a complex system composed of physical objects, the data required to run the system, and finally, practices and norms that guide the persons managing them. In other words, the 'cyber-space' consists of tangible things in a physical space, including long-haul fiber optic lines, operation centres and backup centres that control financial information flows, electric transmission lines, power plants, gas compressor stations, and so forth.[26] In general, the policies on critical infrastructure protection tend to present such complex systems as "closed, totalizing and inevitable successful biopolitical apparatuses". Instead of this totalizing view, Lundborg and Vaughan-Williams argue, the complex systems should be seen for what they are: "open, vulnerable, and often absurd systems that continually falter and backfire, and are often undermined according to their own logics".[27]

In fact, the debate among practitioners of CIP and IR scholars has evolved in this latter direction, and hence CI vulnerability is no

[22] S OPITZ, 'Government Unlimited. The Security dispositif of illiberal governmentality', In *Governmentality. Current Issues and Future Challenges*, U BRÖCKLING, S KRASMANN and T LEMKE, Routledge, NY, 2011.

[23] LUNDBORG and VAUGHAN-WILLIAMS, op. cit., p. 373.

[24] J BRASSET, N VAUGHAN-WILLIAMS, 'Governing Traumatic Events', *Alternatives: Global, Local, Political*, vol. 37, no. 3, p. 183.

[25] BRASSET and VAUGHAN-WILLIAMS, op. cit. p. 183.

[26] COLLIER, op. cit.; LUNDBORG and VAUGHAN-WILLIAMS, op. cit., p. 373.

[27] LUNDBORG and VAUGHAN-WILLIAMS 2011, 369.

longer conceptualized only as protection against external disturbance but as a search for *resilience* — the ability of the system to function in all circumstances. For example, studies on cybergeography, namely the mapping of the physical coordinates of cyber-space, search for the points of vulnerability and subsequently try to improve the resilience of the system as a whole.[28] As has been noted by Christer Pursiainen, "while critical infrastructures were perhaps earlier understood as something very stable and concrete, either physical or information and communication technology systems, there seems to be a trend towards a broad, holistic understanding of critical infrastructure, where it is understood as networks or systems of vital functions of the society as a whole or the infrastructures embedded in these functions".[29]

A survey published by the OECD in 2008 concluded that, in general, definitions of what constitutes critical infrastructure tend to be broad, and include both physical and intangible assets. What is also typical is that the government programmes that were studied "tend to take an 'all hazards approach'", meaning that they consider threats towards critical infrastructures that originate from natural disasters, from accidents or deliberate attacks.[30] Whereas differences in the conceptualization of CI are based on differing security and threat perceptions, differences in geographical and historical preconditions and socio-political factors explain the variations in definition.[31] In the following, we will outline our initial hypothesis in examining Russian policies on CI and the political implications of CI failure.

POST-SOVIET RUSSIA AND THE CHALLENGE OF DE-MODERNIZATION AND INFRASTRUCTURE COLLAPSE

In his 2005 Annual Address to the Federal Assembly President Vladimir Putin famously defined the collapse of the Soviet Union as "the greatest geopolitical catastrophe of the century". This was a "genuine drama" that left millions of "co-citizens and compatriots" outside of Russian territory, destroyed "old ideas", made mass

[28] S P GORMAN, Networks, *Security and Complexity: The Role of Public Policy in Critical Infrastructure Protection*, Edward Elgar, Cheltenham, 2005, pp. 2–4.

[29] PURSIAINEN, op. cit., p. 723.

[30] GORDON and DION, op. cit., p. 5.

[31] BRUNNER and SUTTER, op. cit.

poverty a “norm” and infected the country with “an epidemic of disintegration”. The catastrophe metaphor used in this context singled out the collapse of the Soviet Union as an event that explained subsequent hardships and challenges. Later in the same speech, Putin refers to the same metaphor again and argues that “clearing the debris” has now been completed successfully and thus, the degradation of state and public institutions of the country has been prevented.[32] Consequently, the ‘state of emergency’ in which Russia found itself in the 1990s has come to an end. The catastrophe metaphor is used here to reinforce the status of contemporary Russian politics as a time of return to normalcy constituted by an efficient state, a free society and a competitive economy.

An alternative interpretation of the current situation, and something that we would like to elaborate on in this report, views the dissolution of the Soviet Union not simply as a single systemic crisis that has been overcome, nor the inception of a “transition”[33] to another era, but rather as an event that brought to the fore the actual state of decomposition of the Soviet polity. A plane crash metaphor, used earlier by Sergei Medvedev to argue for a regional interpretation of post-Soviet developments, clarifies the difference in our approach. “When a plane in the air runs out of fuel, or loses control, or its engine catches fire – this is a crisis”, writes Medvedev, “but when the plane hits the ground, it ceases to exist as a subject of crisis, and one needs to apply different terms to describe the fate of the debris”. [34]

Indeed, in the mid-1990s, regionalization offered a plausible frame for interpreting this process. During the 2000s, the regional frame has been replaced by conceptualizations of Russian politics as “authoritarian modernization” or a “hybrid regime”.[35] The research

[32] The speech was made at the beginning of Putin’s second presidential term in April 2005 and was intended to be read as a programme for state policies in the forthcoming decade. V Putin, Annual Address to the Federal Assembly of the Russian Federation, the Kremlin, 25 April 2005, accessed 13 October 2012, http://archive.kremlin.ru/eng/speeches/2005/04/25/2031_type70029type82912_87086.shtml

[33] On the unintended consequences of transition, see e.g. L POLISHCHUK, ‘Misuse of Institutions: Lessons from Transition’, UNWIDER, Working Paper no. 2010/75, June 2010; On the impact of tradition to transition, see S HEDLUND, *Russian Path Dependence*, Routledge, London and NY, 2005; T CAROTHERS, ‘The End of the Transition Paradigm’, *Journal of Democracy*, vol. 13, no. 1, 2002.

[34] S MEDVEDEV, ‘Post-Soviet Developments: A Regional Interpretation (A Methodological View), in *Post-Soviet Puzzles. Mapping the Political Economy of the Former Soviet Union*, vol. II, Nomos Verlagsgesellschaft, Baden-Baden, p. 5.

[35] SAKWA, op. cit.

undertaken in this framework has brought to the fore the formal and informal practices of Russian state administration, as well as elaborated on the ideological contours of "Putin's power vertical'. The research hypotheses embedded in these conceptualizations tend to see the dissolution of the Soviet Union as a one-time, accomplished event. As an alternative to this interpretation, one hypothesis is to regard this process as an open-ended one, where catastrophes and disasters have become *a part of the normal functioning of the polity*. A metaphor that captures our hypothesis is borrowed from the former first secretary of the presidential administration, Vladislav Surkov, who argued in a 2010 interview for *Vedomosti* daily:

> Today the Russian economy resembles an old armoured train without a locomotive. On the train sit people with computers, wearing ties and with glamorous ladies at their side. The armour has virtually disintegrated and it [the train] is decelerating. A little bit further and it will stop altogether.[36]

Surkov's 'old armoured train' symbolizes Russia's capital stock, which is rapidly deteriorating. The average age of industrial equipment in 2009 was 13.0 years, compared with 10.8 in 1990. Just 9.7% of industrial equipment in 1996 was less than five years old. By 2009 the share of up to 5 years old machinery and equipment has increased slightly to 14%. Half of this stock is between 5 and 15 years old.[37]

In the official policy documents, the continuing regeneration of the public infrastructure base – the roads, electricity network, pipelines, housing and other public facilities – is regarded as a factor that undermines not just economic growth prospects, but the perception of Russia as one of the great powers and the country's position as a regional hegemony. This is particularly the case since Russia's position as a major 'energy superpower' is concretely dependent on the very same crumbling infrastructure base.[38] The previous

[36] M GLINKI and N KOSTENKO, 'Nazad v buduschee', *Vedomosti*, 18, 2536, 3 February 2010.

[37] E LENCHUK, 'EU-Russia Programme partnership for modernization and its role in the technological upgrade of the Russian Economy', presentation at the seminar on *Industrial modernization: Is it possible to boost innovation in Russia?*, 27 October 2011, Moscow, The Moscow State University; A LYNCH, 'Roots of Russia's Economic Dilemmas: Liberal Economics and Illiberal Geography', *Europe-Asia Studies*, vol. 54, no. 4, 2002, p. 33.

[38] K PYNNÖNIEMI, *New Road, New Life, New Russia: International transport corridors at the conjunction of geography and politics in Russia*, Acta Universitatis Tamperensis, Tampere, 2008.

analysis of this situation, particularly if conducted in the framework of the economic or business literature, presents the current Russian infrastructure system as an example of previous 'mis-investments', due to which the country's economic geography is incompatible with the principle of the free movement of capital.[39] What is common to these otherwise diverse interpretations is that they are embedded in the framework of the development paradigm. This means that the regeneration of Russia's infrastructure system is viewed as a problem that can be fixed by improving the (state) governance of these critical assets. For example, it is hoped that the practice of public-private partnerships will mitigate the risks to long-term investments in terms of a turbulent business environment.

An argument put forward in this report is that understanding the present-day challenges for Russia only in the context of the development paradigm is inadequate and, worse, misleading. What is required is an analysis that is oriented at understanding the complex systems as inherently vulnerable and open for disasters. In formulating the initial hypothesis of this report, we took note of environmental sociologist Oleg Yanitsky's definition of Russia as "a society of all-encompassing risk". According to Yanitsky:

> In a society of all-encompassing risk the risk production and dissemination become omnipresent and ex-territorial. People in Moscow, Irkutsk and at Sakhalin are equally exposed to risk. In such a society risk production embraces in equal measure the industrial system, everyday life and nature. Risk production encompasses all functional spheres and penetrates into all life-supporting systems. The environment, which is at the same time a risk producer and a risk distributor, turns out mostly to be a risk producer because its carrying capacity has been exceeded many times over.[40]

The normal accident theory, presented briefly above, as well as the risk society concept, provide a conceptual basis for understanding the (negative) development dynamics in Russia in the past twenty years. However, it should be emphasized that the conceptualization of developments in Russia on these terms does not set Russia apart

[39] LYNCH, op. cit., p. 39; see also F HILL and G CLIFFORD, *The Siberian Curse. How Communist Planners Left Russia Out in the Cold*, Brookings Institution Press, Washington, 2003.

[40] O YANITSKY, 'Sustainability and risk. The case of Russia', in *Russian Environmentalism. The Yanitsky Reader*, Taus, Moscow, 2010, p. 61.

as an anomaly of the (Western) development path. On the contrary, present-day Russia can be regarded as a (dystopian) future where the vulnerabilities typical of modern societies are a part of normal, everyday life.

The initial hypothesis of our research is that it is plausible to compare the use of the CI concept in the Russian policy context to that of the US or European context. In fact, we may note a close resemblance between Russian and general Western discourse on CI and CIP. This relates in particular to the threat of terrorism, which has become more pronounced at the level of Russian government policy on CI, although it does not dominate it as in the US.[41] However, the Russian policies on CI are evolving against the background of massive de-modernization of the Russian economy and de-legitimization of the political system – processes that generate rather than help to mitigate infrastructure-related risks and vulnerabilities.

Exactly one month after President Putin's speech, where he described the Russian nation as surviving a "geopolitical catastrophe", a sudden blackout paralyzed several districts of Moscow city as well as Tula, Kaluga, Ryazan and the Moscow regions, affecting more than two million people. Four years later, with the major accident at Sayayanno-Shushenskoi power station, the whole Eastern Siberian electricity network was, momentarily, on the verge of collapse. In July 2010, the wildfires in several regions resulted in substantial economic and human losses. According to data provided by the Ministry of Health and Social Development, the mortality rate rose by 50.7 per cent in the Moscow and Tula oblasts, and by 16.6 per cent in the Republic of Tatarstan.[42] The following year, in August 2010, a hurricane with thunderstorms caused blackouts in 1,500 built-up areas in the northwest of Russia.[43] Reports about massive explosions in the arms storage facilities, the collapse of apartment buildings caused by the gas leakage and the slow but irreversible degeneration of the flora and fauna of the Russian north appear regularly in the Russian press.

[41] In the US, non-intentional risks to infrastructure (poor design, accidents and natural disasters) are regarded as a secondary priority, whereas the primary focus is "on hostile attempts to damage, misuse, or otherwise subvert" the infrastructures. PURSIAINEN, op. cit. p. 731.

[42] O YANITSKY, 'The 2010 Wildfires in Russia. An Ecosociological Analysis', *Sociological Research*, vol. 51, no. 2, 2012, pp. 57–75.

[43] 'Hurricane causes blackouts in Russia's northwest', *The Voice of Russia*, August 16, 2010, accessed November 3, 2012, http://english.ruvr.ru/2010/08/16/15875344.html.

The latest Russian government programme on mitigating the risks to CI indicates several factors that make these sites vulnerable. According to the programme:

> An analysis of information about emergency situations that takes into consideration the structure and dynamics of threats indicates that natural disasters (related to hazardous natural phenomena and fires), accidents on water, as well as anthropogenic accidents and terrorist acts are the main sources of emergency situations and present a substantial threat to the security of citizens and the national economy, and are consequently a threat to sustainable development and ensuring the national security of the Russian Federation.[44]

The three individual chapters of this report will discuss the situational and conceptual background against which certain infrastructures are categorized as critical. The question is, in part, about threat (and risk) perceptions that can be opened up by looking into the Russian discussion on national security. However, and this is what we intend to show in this report as well, the question also concerns the type of political regime Russia currently has and how it copes (or does not cope) with the challenges posed to critical infrastructures. The chapter on the resilience of the northern territories in Russia aims to bring to this discussion yet another aspect, namely the question of the sustainability of the resource-extraction-based policies in the context of global climate change. By explicating the use of the CI concept in these three different cases, we may understand the underlying assumptions of the Russian state policies as well as changes in concrete practices. In the following section we will outline in more detail the three individual research projects conducted for this report.

THE RESEARCH TASK AND STRUCTURE OF THE REPORT

The report presents an empirically oriented research analysis of the Russian government policy on CIP. First, the report aims at understanding the situational and conceptual factors that influence the evolution of the policy. Second, through examining the Russian state policies in

[44] Postanovlenie Pravitelstvo RF, 'O Federal'noi Tselevoi Programme Snizhenie Riskov i Smyatsenie posledstvii Tsrezvytsainyh situachii prirodnogo i tehnogennogo haraktera v Rossiiskoi Federatsii do 2015 goda', 7 July 2011, no. 555, p. 8.

the case of the wildfires in 2010 and the development of the northern territories, the report discusses the political implications of potential natural or technological catastrophes for the current political regime. The emphasis is on understanding the ways in which the de-modernization and de-legitimization processes figure in the background to the conceptual and concrete discussion on critical infrastructure protection in Russia. It should be highlighted that the task is not to assess the level of critical infrastructure protection in Russia nor the major problems in mitigating the risks in this field in the country (as compared to other countries). Further to this, modelling the risks to critical infrastructures and the preparedness of these infrastructures for cyber or physical threats are outside the scope of our research.

The report starts with Katri Pynnöniemi's article (Chapter 2), which discusses the formation of the CIP policy in Russia, first in the framework of the so-called 'winter preparedness' practice, and later in the context of the national security policy, and as an administrative-political category. The Foucauldian notion of governmentality provides a loose framework for the inquiry, as it helps to direct attention away from 'state' or 'politics' to "the formation and transformation of theories, proposals, strategies and technologies"[45] that underlie and thus form what constitutes governance. Accordingly, the analysis does not try to establish a correspondence between certain practices and rationalities, nor between plans and their actual implementation. Rather, the question is about rationalities embedded in the practices and techniques of critical infrastructure protection.[46]

A complementary research analytical framework is discussed by Irina Busygina (Chapter 3). The initial hypothesis of her analysis is that political regimes demonstrate principally different reactions and different levels of state capacity for threats to critical infrastructure, the main lines of division here being between democratic, authoritarian and hybrid regimes. The hybrid regimes, such as Russia, find themselves in the most vulnerable situation since they lack the leverages of both government and control that "pure" types of political regimes are able to use. Therefore, threats to critical infrastructure (natural and man-triggered catastrophes) are important not only *per se* but could serve as good tests for state and regime capacity.

[45] N ROSE, *Powers of Freedom: Reframing Political Thought*, Cambridge University Press, Cambridge, 1999, p. 3.

[46] See also T LEMKE, 'Foucault, Governmentality, and Critique', in *Rethinking Marxism*, vol. 14, no. 3 2002, p. 8.

Busygina analyses the reactions and behaviour of the Russian state during and after the forest fires of 2010, which are considered to be the most disastrous in national recorded history. Her analysis focuses on the mode of control, channels of communication and coordination, the problem of open and credible information and, finally, on the preparedness of local/regional communities for disasters. In general, with regard to the 2010 forest fires, the Russian state has demonstrated a "one-man control" model (instead of an all-agencies approach), which implies a logic of subordination in terms of command and communication (which in practice, however, often led to chaotic and incoherent actions), and which "plays" with information of different kinds, demonstrating serious discrepancies between the official rhetoric and the real state of affairs.

The final section of the report (Chapter 4) takes up the issue of resilience, and focuses on societies living in the extreme north of Russia. Tero Mustonen analyses the knowledge produced at the local community level in relation to official discourses and, as the empirical material will show, proves that people on the ground possess the critical memory and capacity to review and form their own relationships to the administrational discourses and the decisions that ensue. The case study materials will be derived from two northern provinces – the Murmansk region and the Republic of Sakha-Yakutia. Both are along the Northern Sea Route, which will be one of the new "engines" of trade and economy in the geopolitical plans of Russia.

The insights from each of the interlinked but separate research projects presented in this report are summarized in the conclusion (Chapter 5), which is formulated as policy recommendations for decision-makers in Russia and in the EU member states.

2

2. The evolution of Russian policy on critical infrastructure protection

Katri Pynnöniemi

INTRODUCTION

Little research has been conducted into Russian policies on critical infrastructure vulnerabilities, apart from studies has touched upon this issue from the viewpoint of studies on resilience of complex information systems and case studies on crisis management at the Baltic Sea Region.[1] Previous studies on Russian national security policies have mainly focused either on *capabilities* (reform of the Russian army and modernization of the military-industrial complex) or *interests* (explained in reference to foreign policy, strategic culture, the economy, and so forth).[2] Yet, Russia does appear frequently in the

[1] P YUSUPOV and V SHISHIN, 'Informatsionno-kommunikatsionnye tekhnologii i natsionalnaya besopasnost –protivorechivaya realnost', *Informatizatsiya i Svuaz'*, no. 1, 2010; T THOMAS, 'Russia's information warfare structure: understanding the roles of the security council, Fapsi, the state technical commission and the military', *European Security*, vol. 7, no.1, 1998, pp.156–172; T HELLENBERG and P VISURI (eds), *Preventing Terrorism in Maritime Regions: Case Analysis of the Project Poseidon*, Aleksanteri Institute, Aleksanteri Papers, no. 1, 2009; T HELLENBERG, 'Energy security and transportation risks in the Baltic Sea Region', *Aleksanteri Series*, 2007; analysis of Russian national security strategy from the viewpoint of comprehensive security paradigm see A-L HEUSALA, 'Kokonaisturvallisuus-käsite Venäjän turvallisuuspolitiikan tutkimuksessa', *Kosmopolis* vol. 41, no. 4, 2011, pp.23–38.

[2] The impact of Russian domestic developments, especially the rise of so-called *siloviki*, on threat perceptions and practical policy-making, has been studied extensively. Six consecutive reports prepared by the Swedish Defence Research Agency (FOI), provide a comprehensive account of developments that broadly encompass both capabilities and interests. V PALLIN (ed.), *Russian Military Capability in a Ten-Year Perspective — 2011*, Swedish Defence Research Agency (FOI), June 2012; see also A SAVELYEV, *Russian Defense Doctrine*, in S BLANK, (ed.) *Russian Military Politics and Russia's 2010 Defense Doctrine*, Strategic Studies Institute (SSI), March 2011, pp.153–180.

Western debates on cyber threats. In this context, the country is considered "home to some of the most competent cybercriminal networks in the world"[3], and a place where the intelligence service operates a "terrifying monitoring system, which goes under the suitably totalitarian name of SORM-2".[4] The first Chechen war in 1994–1996 and the world's "first real cyber war" between Russia and Estonia in 2007 are cited as examples of Russia's ability and willingness to fight a cyber war.[5] At the same time, in the Russian public debate the vulnerability of the country's own industries and critical assets is used in arguing for better IT security.[6] Yet focusing on the cyber aspect alone is inadequate, even misleading, if the purpose is to understand Russian *policies* on critical infrastructure protection (CIP).[7]

A report published by the Rand Corporation titled *Assessing Russia's Decline* provides another, no less controversial starting point for such an inquiry. The report was published in 2002 and it captures the general line of thinking in the West on Russia's transformation during the last ten-year period. The basic assumption of the report is that Russia is a declining power and this situation "may evolve into challenges and dangers that extend well beyond its borders".[8] The report underlines that Russia does not possess a "traditional threat"

[3] M GLENNY, 'The Cyber Arms Race Has Begun', *The Nation*, October 31, 2011, p. 18; see also the recent report on Russia's cybercriminal underground, M CONCHAROV, *Russian Underground 101*, Research Paper, Trend Micro Incorporated, 2012, viewed 06 November 2012, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf.

[4] SORM-2 is a system operated by the FSB, which collects all data that run across the Runet. M GLENNY, op.cit. p. 18.

[5] R KAISER, 'Estonia and the Birth of Cyberwar', Presentation at Aleksanteri Institute, 4 October 2012; H BERGER, *Venäjän informaatio-psykologinen sodankäyntitapa terrorismintorjunnassa ja viiden päivän sodassa*, Julkaisusarja 1, Tutkimuksia no. 5, 2010, Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos.

[6] A MIHAILOV, 'Kriticheskaya infrastruktura okazalas' v kiberopasnosti', Business FM, 17 November 2010, viewed 14 November 2012, http://www.bfm.ru/articles/2010/11/17/kriticheskaja-infrastruktura-okazalas-v-kiberopasnosti.html; 'Bolee poleviny rossiiskih objektov kriticheskoi infrastrukturu ne obespetsivajut dolzhnyh mer informatsionnoi bezopasnosti', 22 March 2011, viewed 7 February 2012, http://www.antivirus43.ru/news/222; Researchers Yusupov and Shishkin report that modern data centres appeared in Russia in early 2000. The centres were built upon imported technologies and are heavily concentrated (90%) either in Moscow or St. Petersburg. P YUSUPOV and V SHISHIN, op.cit.

[7] Russia is currently formulating a cyber strategy that will replace the information security doctrine from 2000. M IVANOV, 'Sovet federatsii zanyalsya tsifrovym suverenitetom', Kommersant, 6 November 2012, viewed 12 November 2012, http://www.kommersant.ru/doc/2060832/print.

[8] O OLIKER, Assessing Russia's Decline: Trends and Implications for the United States and the US Air Force, Santa Monica, CA: Rand Corporation, 2002.

rooted in its military capability, but is an important factor in US calculus due to a set of "amorphous dangers presented by military, political and social decline".[9] The conflict propensity, together with the infrastructure deterioration, "increase the likelihood of a humanitarian catastrophe, whether from war itself, from an industrial or nuclear accident, from a health crisis, or from physical and economic isolation of parts of the country", the report argues.[10] At the time of writing, the report captured the sense of doubt in the West on the dynamics of change in Russia, although the mainstream view on the country's development was rather positive.

The basic problem of CIP in Russia is expressed with reference to "over 45,000 potentially dangerous objects located in the country and over 90 million people living in high-risk zones".[11] The argument put forward in this chapter is that by examining the Russian policies on critical infrastructure, we may better understand the kind of challenges Russia faces, and also how the country intends to deal with them. This chapter explores the evolution and underlying assumptions of Russia's policies on critical infrastructure protection (CIP). The initial hypothesis of the research is that Russian policies do resemble those outlined in the US or European context, yet the way in which the key ideas presented in the policy "hang together" reveals underlying differences in the policy fields.

To open up the discussion on the political horizon of CIP policies in Russia, the first section discusses "winter season" practices, namely the preparedness of public utilities for winter and the delivery of energy to the northern territories. It is argued that "winter preparedness" can best be understood as a political spectacle that captures what is considered "normal" in the present-day Russian political context: a vertical (top-down) approach to the governance of mundane things, coupled with the regular use of "exceptional measures" to get things done. The second section will review the evolution of the Russian policy on CIP and clarify the criteria applied in determining which infrastructures are considered critical. The last section

[9] O OLIKER, op.cit., p. 1.

[10] O OLIKER, op.cit., p. 7.

[11] P TSALIKOV, V.A. AKIMOV, K. A. KOZLOV, Otsenka prirodnoi, tehnogennoi i rkologicheskoi besopasnosti Rossii, FGU VNII GOTCS, MChS Rossii, 2009; President RF, 'Osnovy gosudarstvennoi politiki v oblasti obespecheniya besopasnosti naseleniya RF i zashchishchennosti kriticheski vazhnyh i potentsialno opasnyh ob'ektov ot ugroz prirodnogo, tehnogennogo kharakteri i terroristicheskih Aktov na Period do 2020 goda', 15 November 2011, utv. no. Pr-3400.

introduces the main government agency responsible for implementing the CIP policy, and also describes the recent changes in the reporting and monitoring of emergency situations. The conclusion summarizes the main findings of the analysis and discusses ideas for further research. It should be underlined that the analysis presented in this chapter is intended as an introduction to this subject and not as a comprehensive account of it.

The main body of research material consists of official documents that are intended to frame government actions towards the phenomenon and the infrastructures considered *critical* for national security. The most important of these is the federal target programme on CIP that was first accepted in 1999 and which has been revised twice since then, in 2006 and 2011 respectively. It outlines the main principles of the government policy on critical infrastructure protection. The news reports, official speeches and interviews published in the Russian press between 2000 and 2011 are used as secondary material to trace the evolution of the policies on CIP.

THE SPECTACLE OF "WINTER SEASON" PREPAREDNESS

Every autumn at around the same time, the Russian government holds a series of meetings with the regional authorities that all deal with the same problem: the winter preparedness (*podgotovku k zimu*) of the country. There are only two issues on the agenda: the functioning of the northern supply system[12] that provides the northernmost regions of the country with energy and other resources for the winter period, and the functioning of the heating systems in the rest of the country. The Federal Grid Company's (RAO UES) announcement of October 2012 illustrates what "winter preparedness" is concretely about and how it is presented to the public. According to the press release below, the company has completed its preparations for the winter period in the North-West Russian region, including:

> Reconstructed 354 bedding of pillars, and reinforced 182 pillars, 174 distance bars and more than 43,000 insulators, changed lightning

[12] The northern supply system emerged during the Soviet Union as a response to the need to supply remote regions of the Russian Arctic and sub-Arctic with fossil fuels, mainly diesel and coal, as well as foodstuffs. I OVERLAND, 'The Siberian curse: a blessing in disguise for renewable energy', *Sibirica*, vol. 9, no. 2, Summer 2010, pp. 1–20.

> guard cables along 24 km length, cut down 19,000 trees that presented risk of falling on power line. Repaired 15 transformers and autotransformers on substations, which is more than two times the results of the previous year. In case of emergency, 1,061 specialists of the regional grid company will be available for help, as well as 387 pieces of special equipment and 760 other specialists from other organizations.[13]

The functioning and overall resilience of these life-support systems (*system zhisneobespecheniya*) is subject to federal-level regulation, so implementation of the planned reconstruction works is consequently controlled, at least in principle, by the state inspectors. In the public discussion, however, the inspectors are not even mentioned as a rule, or if they are, this is made with reference to the implied corruption of inspectors (or regulators, or both). In fact, the public discussion on the winter season is best understood as a performance whereby the regional leader expresses his or her loyalty towards his superiors by submitting carefully orchestrated pieces of information to the head of the state.

For example, in October 2009 the governor of the Kamchatka region, Alexey Kuzmitsky, confirmed to Prime Minister Vladimir Putin that “92 per cent of communal buildings had been prepared for the winter”, and with this, the spectacle of “winter preparedness” had been accomplished.[14] The regional news reports complement and consolidate the original spectacle by showing that the “actual state of preparedness” is far lower than the reported level. For example, in August 2001, a regional Moscow newspaper reported that the task of “preparing for winter” was only 11 percent complete.[15] Although critical towards the official performance, this information consolidated the original representation of “winter preparedness” as a series of indicators and percentage points.

It is the practice of designating certain objects as “strategic” that undermines the integrity of this spectacle. The notion “strategic object” is used with reference to those infrastructures and functions that are considered strategically important for the state. This status

[13] ’Vse energopredpriyatiya Severo-Zapada poluchili pasporta gotovnosti k zime 2012–2012’, IA REGNUM, 10 October 2012, viewed 13 October 2012, http://www.regnum.ru/news/polit/1579772.html.

[14] ’V Putin provel selektornoe soveshchanie po voprosu podgotovki organizatsii elektroenergetiki i predpriyatii ZhkH k prohozhdeniyu osenne-zimnego perioda 2009–2010’, 5 October 2009, viewed 11 October 2012, http://www.government.ru/docs/5100/.

[15] E ZVEREVA, ’Zimnyaya Skazka’, *Moskovsky Komsomolets*, 10 August 2001.

has been granted to specific industrial objects, nuclear plants, the Moscow metro, as well as hospitals and other communal infrastructures that are guaranteed access to electricity even in the event that the companies or organizations operating these vital systems are unable to pay for the electricity.[16] In some cases, however, this notion is used in legitimizing direct control and surveillance of these objects.

For example, in 2001, the mayor of the city of Norilsk in Northern Russia argued that in order to increase the security of "strategic objects" (the Messoyha-Norilsk gas pipeline), Norilsk should be reinstated as a "closed town", a status that it had lost in 1991.[17] The immigrants from the South were identified as a security threat, which, in turn, was used in arguing for the monitoring and even possible closure of the public space to certain categories of people. In the aftermath of the August 1999 explosions in Moscow apartment blocks, the "unidentified hallway" was also named as a "strategic object" that should be safeguarded against a possible terrorist threat.[18] The privatization of the public domain, coupled with an extensive but unaccountable regulative regime, raiding practices and the overall criminalization of society are factors that render public spaces vulnerable. Yet, as these examples also show, the practice of designating certain objects as strategic is far from uniform, and effectively contributes to a blurring of the distinction between normal and emergency, open and closed, or public and private spheres.

What is argued here is that practices related to the "winter season" are regarded as a part of the normal functioning of the state governance, rather than something that requires a declaration of a state of emergency. Russia's physical geography is the most obvious explanation for this, as the permafrost area comprises over half of the total area of the country.[19] However, the political spectacle that revolves around the "92 per cent" fulfillment of the winter preparedness plan actively overlooks this "natural" background. Instead, what is reinforced is a political culture whereby the political leadership is expected to control and personally take part in solving political, social and economic problems at every level of the state administration,

[16] N ANDREEVA, 'Puteshestvie tuda, kuda vas ne pustyat', *Saratovskie Vesti*, 10 January, 2001.

[17] 'Sergei Shoigu poprosili zakryt Norilsk', *Kommersant* 14 March 2001. Norilsk regained the status of a closed town in October 2001, restricting the access of foreign travellers to the town (except citizens of Belorussia).

[18] 'Ohrana Pod'ezdov', *Petrovka*, Moskva 20 June 2001.

[19] E PETROVA, 'Critical infrastructure in Russia: geographical analysis of accidents triggered by natural hazards', *Environmental Engineering and Management Journal*, vol. 10, no. 1, 2011, p. 58.

including the heating supply for residential buildings, for example. However, the repeated failure to prepare for winter contributes to the de-legitimization of the political regime.[20] (See Chapter 3 for a detailed discussion on the link between de-legitimization and catastrophes).

Another point, reflected in the above discussion on winter preparedness, concerns the powers vested in the act of designating an object as *critical*. For example, when institutionalized (as an institutional fact), applying the notion of 'strategic object' may provide for certain privileges over others for communities/owners of that specific infrastructure installation.[21] The object may be considered strategic for the Russian economy, such as an oil pipeline, or it may acquire privileged status as part of a specific practice such as 'winter season preparedness'. Other variations of the theme also apply. For example, 'strategic object' status can be bought or imposed, and in both cases the fact of having the status does not necessarily imply the *strategic nature* of the object for the community or country as a whole. This reflection is, in fact, the very locus of the policies on CIP as it touches on the question of the criteria by which certain infrastructures (or functions) are regarded as critical and why. In the following section I will first outline the general framework of the discussion on critical infrastructures, as it emerged in the late 1990s and early 2000s, and then focus in more detail on the actual definition of critical infrastructures.

DEFINING RUSSIA'S 'CRITICAL INFRASTRUCTURES'

CI vulnerability in the framework of national security

The National Security Concept of Russia was approved by a presidential decree on 11 January 2000, shortly after President Boris Yeltsin had suddenly resigned and appointed Vladimir Putin as his designated heir. The Concept emphasizes the emergence of a multipolar world, Russia's status as one of the great powers, and finally, attempts by other states to "weaken Russia politically, economically, militarily and in other ways".[22] This marks a clear change in articulation, for the earlier

[20] For more on this, see S HEDLUND, 'Such a beautiful dream: how Russia did not become a market economy', *The Russian Review* vol. 67, April 2008, pp. 187–208.

[21] On the construction of institutional facts, see J SEARLE, *The Construction of social reality*, Penguin Books, London, 2005.

[22] 'Concept of National Security of the RF', approved by Presidential decree no. 24, 10 January 2000, pp. 1–2.

version of the Concept, approved by President Yeltsin in late December 1997, speaks about economic instability as the "primary threat to Russia", and mentions internal sources, rather than other states or alliances, as a challenge to Russia's territorial integrity.[23]

Although the main source of vulnerability in the concept approved in January 2000 is identified as being outside of Russia, other factors are identified as well. The "deteriorating environmental situation in the country and depletion of its natural resources" are mentioned among the factors that have a negative influence on the "state of the economy and society's willingness to grasp the globality and importance of these issues". In connection with this, it is noted that "the erosion of state oversight and the insufficient effectiveness of the legal and economic mechanism for averting and relieving emergencies are bound to increase the risk of man-made disasters in all sectors of economic activity".[24] Accordingly, the priority areas of government activity include "ecologically safe and non-hazardous storage and/or utilization of decommissioned arms, nuclear ammunition, chemical weapons stocks", and "urgent environmental protection measures" that are called for to protect ecologically dangerous regions of the country. To implement these tasks, a "qualitative improvement of the unified state system of disaster warning and relief" should be established, including its further "integration with similar systems of foreign states".[25]

Not long before the publication of the national security concept in September 1999, the first government programme 'on the reduction of risks and moderation of the consequences of emergency situations caused by natural or technological disasters in the Russian Federation until 2005' was approved. It outlined the basic principles and objectives for the establishment of the above-mentioned unified state system of disaster warning and relief.[26] The ten-page document does not identify specific infrastructure objects as critical, but rather speaks about 'population' and 'territory' as being vulnerable to

[23] 'Concept of National Security of the RF', approved by Presidential decree no. 130, 17 December 1997; See also J J KIPP, 'Russian Military Doctrine: Past, Present, and Future', in S BLANK, *Russian military politics and Russia's defence doctrine*, Strategic Studies Institute, SSI Monograph, 2011, p. 95.

[24] 'Concept of National Security of the RF', p. 8.

[25] Ibid., p.16.

[26] Pravitelstva RF, 'O federalnoi tselevoi programme "Snizhenie riskov i smyagchenie posledstvii chrezvytsainyh situatsii prirodnogo i tehnogennogo kharaktera v RF do 2005 goda', Postanovlenie no. 1098, 29 September 1999.

emergency situations caused by "disasters of a natural or technological character". The objective of the policy is to improve the complex system relating to the prevention of emergency situations, to allow for a 40 to 50 per cent decrease in the risk to the population 'living in the regions affected by the impact of a dangerous natural or technological phenomenon'.[27]

At that point, Russian policy was not focused on *critical infrastructures* but was based instead on thinking along the lines of an 'all-hazard approach'.[28] The basis for this was established in the federal law on "protection of population and territory from natural catastrophes and technology- generated emergency situations" that came into force in November 1994. It defines "organizational-legislative norms" for the protection of the population and the environment, as well as the protection of water, air space, and objects of industrial or social significance against emergency situations of a natural or technological character. [29] The fact that the first federal-level programme on the prevention of emergency situations was approved only a few weeks after the deadly apartment explosions in Moscow and the southern Russian cities of Volgodonsk and Buynaksk, seems to underline the low priority of this rather abstract programme and also it *not being* considered in the framework of national security.[30] This situation began to change two years later.

In July 2003 Vladimir Rushailo, the secretary of the Security Council, came forward with an idea that Russia should formulate the principles of the state policy in the sphere of environmental and technological security. According to Rushailo, the aim of the new policy would be to "unite work and other resources of the state administration, improve current legislation, develop the technological basis and create a modern unified system of physical protection for the (strategic) objects".[31] Tambov was later chosen as a pilot

[27] Ibid. The budget for this government programme was around 6 billion roubles (at 1999 rates), of which 4.5 billion were earmarked from the regional budgets.

[28] See discussion on the all-hazard approach versus critical infrastructure protection policy e.g. C PURSIAINEN, 'The Challenges for European Critical Infrastructure Protection', *European Integration*, vol. 31, no. 6, 2009.

[29] Federalnyi Zakon, 'O zashchite naseleniya i territorii ot chrezvychainyh situatsii prirodnogo i tehnogennogo haratera', no 68-FZ, 21 December 1994.

[30] The three consecutive explosions between 4 and 13 of September 2009 killed over 200 people and paved the way for the second war in Chechnya.

[31] R. POLYAKOV, 'Vladimir Rushailo obsudil problemy natsional'noi bezopasnosti Rossii', *Kommersant* (Voronezh), 7 July 2003.

region in which to conduct a project on protection of the "critically important infrastructure".[32]

The joint session of the Security Council and the State Council in November 2003 can be considered as the starting point for the formulation of the Russian policy on critical infrastructure protection. In his opening statement at the meeting, President Putin emphasized that the protection of "critical to national security objects from technological, nature-generated or terrorist threats" is an acute task and requires the joint action of the state authorities and "economic organisms".[33] The new policy is required because Russia's run-down infrastructures are prone to malfunction, and the risk of technology-generated catastrophes is further aggravated due to widespread indifference to safety rules and norms, Putin explained. In addition, each year more and more natural catastrophes, such as hurricanes, earthquakes and forest fires are reported in Russia. To tackle these problems, state policy needs to be reshaped, Putin argued.[34]

The first set of documents explicating state interests and objectives in terms of critical objects was outlined soon after, in December 2003. The state policy on the improvement of chemical and biological, as well as nuclear security paved the way for a re-formulation of the policy away from largely unidentified 'emergency situations' to the protection of critical sites from terrorist acts and other threats to "vital human activities, national security and socio-economic development".[35] With the concept of the "federal system of monitoring the critically important infrastructure objects and/or dangerous goods" introduced in August 2005, the policy was tied to "critically important objects" whose malfunction may lead to "un-manageability of the economy and administrative-territorial

[32] The project focused on improving security in the chemical industry and improving the monitoring systems in major population centres (in the Tambov region). 'Novaya sistema bezopasnosti Rossii rozhdaetsya v Tambove', Tambovskaya Zhizn' (Tambov), 10 August 2004.

[33] V PUTIN, 'Vstupitel'noe slovo na sovmestnom zasedanii Soveta Bezopasnosti i preziduma Gosudarsvennogo soveta po voprosu o povyshenii zashchity kriticheski vazhnyh dlya natsional'noi bezopasnosti ob'ektov infrastruktury i naseleniya strany v usloviyah obostreniya ugroz prirodnogo, tehnogennogo, i terroristicheskogo haraktera', 13 November 2003, Moskva, Kreml, viewed 15 May 2012, http://archive.kremlin.ru/text/appears/2003/11/55532.shtml.

[34] Ibid.

[35] 'Osnovy gosudarstvennoi politiki v oblasti obespecheniya khimicheskoi i biologicheskoi bezopasnosti RF na period do 2010 goda i dal'neishuyu perspektivu', Prezident RF V PUTIN, ukaz Pr-2194, 4 December 2003; 'Osnovy gosudarstvennoi politiki v oblasti obespecheniya yadernoi i radiatsionnoi bezopasnosti RF na period do 2010 goda i dal'neishuyu perspektivu', *Rossiiskaya Gazeta*, 7 April 2004.

unity of the country" and "affect the security and general well-being (*zhisnedeyatel'nosti*) of the population over a long period of time".[36]

Finally, in September 2006, a concept paper was published entitled "Conceptual basis of the state policy on protection of population and critically important and potentially dangerous objects from emergency situations caused by natural or technological disasters and terrorist acts".[37] The state policy on CI is legitimized with reference to the following dangers and threats:

- increasing danger and intensity of technology-generated and naturally occurring emergencies,
- increasing number of potentially dangerous objects, many of which are located in big cities and densely populated areas,
- physical depletion and technological backwardness of systems and complexes designed to improve safety of dangerous objects,
- low level of education and training of the personnel (working with dangerous objects, K.P.), weak technological discipline, low level of safety culture,
- inadequate level of financing of measures aimed at improving the safety of the population and management of the dangerous objects,
- increasing danger of international and internal terrorism, increasing level of criminality and the narcotic business in society.[38]

The federal target programme, and the preceding government policy documents, reinforce a "regime of rationality"[39] which, in turn, legitimizes a specific constellation of security, state governance and power. This triangle is emergent in the criteria for identification of the 'critically important objects'.

[36] Rasporyazheniem Pravitelstva RF, 'Kontseptsiya federal'noi sistemy monitoring kriticheski vazhnyh ob'ektov i/ili potentsial'no opasnyh ob'ektov infrastruktury RF i opasnyh gruzov', no. 1314 p. 27 August 2005.

[37] 'Osnovy gosudarstvennoi politiki v oblasti obespecheniya bezopasnosti naseleniya RF i zashchshchennosti kriticheski vazhnyh i potenchial'no opasnyh objektov ot ugroz tehnogennogo, prirodnogo kharaktera i terroristicheskih aktov', Prezident RF, 28 September 2006, Pr-1649.

[38] Ibid.

[39] Foucault cited in T LEMKE, 'Foucault, Governmentality, and Critique', paper presented at the *Rethinking Marxism Conference*, University of Amherst (MA), 21–24 September 2000, p. 7.

Criteria for the definition of critically important objects

The notion of 'critical infrastructure protection' is rarely used in the Russian media. Instead, this phenomenon is discussed using various other terms, such as 'strategic object' (*strategicheskii obj'ekt*), 'dangerous industrial object' (*opasnyi proizvodstvenniyi ob'ekt*), 'very important object' (*osobo vazhnyi ob'ekt*), 'very dangerous technically complex object' (*osobo opasnyi i tehnicheski slozhnii ob'ekt*), and 'potentially dangerous objects'.[40] These terms are used interchangeably with the concept of 'critically important objects' (*kriticheski vazhnyh ob'ektov*, KVO) that emerged in the official policy context after 2006. The critically important objects are identified in accordance with three criteria: the type of threat, the scale of the catastrophe, and the importance of the object.[41]

Starting with the first – type of threat – the revised version of the federal target programme on CIP from 2006 clarifies that in Russia there are "2,500 chemically dangerous objects[42], over 1,500 nuclear sites, 8,000 fire-sensitive and explosive-prone objects, and over 30,000 hydrotechnical systems", a majority of which have great "economic, military and social significance for the country, but also present potential danger for the health and life of the population and the natural environment".[43] The industrial development projects in ecologically vulnerable areas (presumably including the Arctic), are regarded as particularly hazardous:

> Nature-related risks which occur as a consequence of the processes of economic activity and represent a potential threat source for people's vital activity and economic potential, include risks of damage to the natural environment which, as a result, threaten the activity of existing industrial and other facilities, and the implementation of new industrial development projects, including those in regions that are especially sensitive to the anthropological influence of ecosystems,

[40] The analysis is based on a search that was conducted through the Integrum search engine and listed articles that appeared in major federal newspapers in Russia between 2000 and 2010.

[41] Emercom, 'Metodicheskie rekomendatsii po provedeniyu inventarizatsii kriticheski vazhnyh i potentchial'no opasnyh ob'ektov RF i formirovaniyu oerecheniya kriticheski vazhnyh ob'ektov na regional'nom urovne', administrative order no. 2-4-60-10-14, 19 June 2008.

[42] See assessment of biotechnology sector in Russia today at R ROFFEY, *Biotechnology in Russia: Why is it not a success story?*, Swedish Defence Research Agency, User Report, 2010.

[43] Postanovlenie Pravitelstvo RF, 'O Federal'noi tselevoi programme snizhenie riskov i smyatsenie posledstvii tsrezvytsainyh situachii prirodnogo i tehnogennogo haraktera v Rossiiskoi Federatsii do 2010 goda', 6 January, 2006, no. 1.

> technological accidents and other causes which, under normal circumstances, would bear no ecological or other threat. [44]

The Ministry of Emergency Situations, which coordinates the implementation of government policies on emergency prevention and response, also includes in this first criterion objects with a high fire security requirement (*pozharovzriyvoopasnye ob'jekti*), as well as government, finance and banking sector, information and telecommunications infrastructure and other non-identified objects.[45]

The scale of the catastrophe is another important reference point in the categorization of critically important objects. The Russian government order in September 1996 defined the scale based on three criteria: the human, material and spatial impact of the catastrophe. The six-scale ranking identified local, municipal, territorial, regional, federal, as well as disasters on a trans-border scale. *Local disasters* are situations where there are less than 10 casualties, no more than 100 persons' vital activities (*zhiznedeyatelnosti*) are disrupted, material costs are not extensive and the (spatial) impact of the disruption does not exceed the specific industrial or social object.[46] At the other end of the scale are t*rans-border disasters*, which are not defined in concrete terms but with reference to their *cross-border* significance. The 1996 order was reviewed in May 2007 and the six-scale ranking currently includes: local, municipal, inter-municipal (previous municipal and territorial categories), regional, inter-regional and federal, whereas the trans-boundary scale is excluded.[47] The critically important objects are defined in accordance with the last three scales: regional, inter-regional and federal.[48]

The last criterion defines the importance of critically important objects in terms of three spheres (of action): impact of the object on the regional economy, possible damage caused to state prestige (that is, governance, the banking sector and military security) and possible threats to population and territory (namely the impact from the interruption of vital systems on the local population).[49] These

[44] Postanovlenie Pravitelstvo RF 2006, p. 9.

[45] Emercom, op. cit., 2008.

[46] Postanovlenie Pravitelstvo RF, 'O klassifikatsii chrezvychainyh situatsii prirodnogo i tehnogennogo haratera', no. 1094, 13 September 1996.

[47] Postanovlenie Pravitelstvo RF, 'O klassifikatsii chrezvychainyh situatsii prirodnogo i tehnogennogo haratera', no. 304, 21 May 2007.

[48] Emercom, op. cit., 2008.

[49] Emercom, op. cit., 2008.

three criteria provide a basis for identification and registration of the critically important objects, a status that can be granted by the head of the region.[50] This discussion has clarified the basis on which certain infrastructures (understood broadly) are considered critical. In the next section I will briefly introduce certain aspects concerning the reporting and monitoring of CI vulnerabilities, although it should be emphasized that the purpose here is not to assess the level of protection.

GOVERNANCE THROUGH THE REPORTING AND MONITORING OF CI VULNERABILITIES

As discussed in the previous section, the Russian policy on CIP was formulated in 2006 in a series of documents, including the concept paper published in September 2006 that also provided the basis for the formulation of the criteria for the identification of critically important objects, and the federal target programme that outlined tasks to prevent emergency situations in the country. The latter programme ran until 2010 and was replaced in July 2011 by a new programme that will run until 2015.[51] This last section will focus on these latter developments, particularly on the shift from identification of the critical objects to systems of monitoring and reporting emergencies and threats.

The point of departure is the argument put forward in the latest edition of the catastrophe prevention state programme from July 2011.[52] As stated in the document:

> The resolution of tasks for guaranteeing national security in emergency situations can be achieved through improving the effectiveness of the implementation of the government and local self-government authority in the sphere of security control of the population's vital activity, renewal of the technical equipment base, production technologies for potentially hazardous facilities and life-support facilities, the introduction of modern technical means for informing

[50] Ibid.

[51] Postanovlenie Pravitelstvo RF, 'O federal'noi tselevoi programme "Snizhenie riskov i smyagchenie posledstvii chrezvychainyh situatsii prirodnogo i tehnogennogo haraktera v RF do 2015 goda'.

[52] Ibid., pp. 10–11.

> populations in places of mass gatherings, as well as the development of measure-taking systems in order to reduce risks and mitigate the consequences of natural and anthropogenic emergency situations and terrorist acts.[53]

The programme calls for the development of a scientific-methodological basis for risk management, and a set of "long-term strategies and organizational-financial mechanisms" that enhance the "interaction", "coordination" and "targeting" of resources.[54] The improvement of the monitoring and emergency prevention systems is legitimized by reference to the fact that the *risk* of natural disasters and major technological catastrophes in the territory of Russia is constantly increasing. At the same time, recent statistics show that the economic and human costs of emergency situations are decreasing.

According to official statistics, 238 emergency situations were reported in Russia in 2011, compared with 360 cases in 2010. In 2009, 429 emergency situations were registered.[55] (See Table 1.) The number of individuals reported to have died or sustained injuries due to natural or technological disasters is steadily decreasing as well. According to a report on the implementation of the CIP programme in 2010 (the base year for calculations used in the new programme), the number of fatalities in accidents decreased by 15.1 per cent and the number of injured decreased by 10.2 per cent. The economic costs of catastrophes are reported to have decreased by 8 per cent.[56] A closer look at the statistics reveals a number of contradictions, however. For example, official statistics report 429 emergency situations in 2009, whereas information provided by the Ministry of Emergency Situations of Russia (MCHS) includes 424 cases. This is, however, a minor flaw compared with the drastic change in the total number of emergency situations as reported in 2008 compared to 2009. There are several plausible explanations for this change. It may relate to

[53] Ibid., p. 9.

[54] Postanovlenie Pravitelstvo RF, 'O federal'noi tselevoi programme "Snizhenie riskov i smyagchenie posledstvii chrezvychainyh situatsii prirodnogo i tehnogennogo haraktera v RF do 2015 goda', no. 555, 7 July 2011, p. 13.

[55] Edinaya mezhvedomstvennaya informatsionno-statisticheskaya sistema, informatsiya o chrezvychainyh situatsiyah, accessed 23 October, 2012, http://www.fedstat.ru/indicator/data.do?id=41317&referrerType=0&referrerId=947198.

[56] Ministry of Emergency Situations of RF, 'Otchet ob itogah realizatsii federalnoi tselevoi programmy" Snizhenie riskov i smyagchenie posledstvii chrezvychainyh situatsii prirodnogo i tehnogennogo haraktera v RF do 2010 goda', accessed 15 October 2012, upload/FCPriski2010.doc.

the overall decrease in industrial production in Russia during the economic crisis in 2008–2009. What also seems possible is that the reporting technique or actual definition of a technological disaster has been reformulated and, as a consequence, the total number of emergency situations has drastically declined.

Emergency situations**	2011	2010	2009	2008	2007	2006
in total, of which	297*	360*	429*	2154	2693	2847
Technological disasters	185	178	270	1966	2248	2541
Natural catastrophes	65	118	133	152	402	261
Biological–social catastrophes	42	43	21	36	43	44

Table 1. Annual statistics of emergency situations in Russia between 2006 and 2011
* Source: Russian Statistic Agency http://www.fedstat.ru/indicator/data.do.
** Source: Information provided on MCHS website, http://www.mchs.gov.ru/stats/index.php?section_id=253.

It is also notable that the first report published in 1992 by MCHS records 1,242 emergency situations, of which 1,004 were "technological", 144 "natural disasters", and 94 of a "biological-social character". In all, 6,800 people were injured and 947 people died as a result of these disasters.[57] In comparison, in 2006, 2007 and 2008, the reported number of deaths is almost equivalent to those injured in 1992.[58] In later years, the statistical evidence of the human cost is counted in hundreds rather than in thousands. Further research would be required to clarify the reasons for these changes.

However, the conclusion drawn in the above-mentioned federal target programme from 2011 is that the reduction in the number of emergency situations and their human and economic costs "speaks for the efficiency of the preventive measures and effectiveness of the measures conducted during the crisis situation".[59] The establishment of a National Crisis Management Center[60] in 2006 and the development of similar centres at the federal district level are cited as examples of an improvement

[57] The Ministry of the Russian Federation for Civil Defence, Emergencies and Limitation of Consequences of Natural Disasters, EMERCOM, *Report on implementation of the tasks in 1992–1993*, accessed 27 May 2012, http://www.mchs.gov.ru/eng/ministry/?section_id=591.

[58] EMERCOM, *Report on implementation of the tasks in 2005–2006*, accessed 27 May 2012, http://www.mchs.gov.ru/ministry/index.php?section_id=298.

[59] Ibid., 8.

[60] EMERCOM, 'National Crisis Management Center', accessed 14 November 2012, http://www.mchs.gov.ru/eng/powers/?section_id=609.

in the situation. Other examples of efficient crisis management mentioned in the text include "the military conflict between Georgia and South-Ossetia", "the technological accident at Sayano-Shushensko hydroelectric plant in 2009"[61], "the forest fires in 2010" (see Chapter 3), and other technological disasters.[62] In connection with the third anniversary of the Sayano-Shushenskaya catastrophe, the Russian government widened the scope of the monitoring and control of dangerous industrial objects and the hydro-electric systems regulatory authorities. Since July 1, 2012, the Russian Federal Mining and Industrial Inspectorate (Rostechnadzor) has been granted wide supervisory powers over the owners and managers of these specific objects.[63]

The reporting and monitoring of CI-related vulnerabilities and threats puts *risk* at the centre of the analysis and further legitimizes policies on CIP. The objective set in the federal target programme is to improve the monitoring and forecasting capacities to the extent that they cover 80 per cent of technology- and nature-generated risks.[64] A new culture of emergency response is required to achieve this objective. This new culture is a "culture of informing and alerting about emergency situations" which, in turn, is formed on the basis of next-generation systems of emergency situation monitoring and forecasting, wider use of new information technologies for these purposes, and the implementation of a system of measures for ensuring the comprehensive security of population and territory by 2015.[65]

> The development of informational security systems for the population in places of mass gathering, and the monitoring of critically important and potentially hazardous facilities and cargo, as well as

[61] The official investigation into the causes of the accident revealed serious flaws in the management of the power station, including deficiencies in safety procedures that date back to the late 1970s. F MAKSIMOV and N SKORLYGINA, 'Tri goda sputstya vodu', *Kommersant* 17 August 2012.

[62] Pravitelstva RF, 'Kontseptsiya federalnoi tselevoi programmy 'snizhenie riskov i smyagchenie posledstvii chrevytsainyh situatsii prirodnogo i tenogennogo kharaktera v RF do 2015 goda', *rasporyazhenie* no. 534-p, 29 March 2011.

[63] MAKSIMOV and SKORLYGINA 2012.

[64] Postanovlenie Pravitelstvo RF 2011, pp. 25–26.

[65] Postanovlenie Pravitelstvo RF 2011, p. 13. After the Moscow metro bombing on 29 March 2010, President Medvedev ordered the establishment of a new monitoring system for public transport in Moscow and other cities by 2014. President Rossii, Ukaz 'O sozdanii kompleksnoi sistemy obespecheniya bezopasnosti naseleniya na transporte', 31 March 2010, accessed 12 May 2012, http://news.kremlin.ru/news/7295/print.

> the development of mechanisms of control coordination, form the technological basis of the all-Russian system of informing in the sphere of the complex provision of security for the population and critically important infrastructural facilities against natural and anthropogenic hazards.[66]

Back in 2006, the establishment of the National Crisis Management Center was presented as an answer to the growing need to improve the "optimization of emergency response activities with the use of modern technologies". However, a special unit responsible for monitoring and forecasting emergency situations has already been in existence since 1998, and it publishes an annual report on risks related to technological and natural catastrophes.[67]

CRITICAL INFRASTRUCTURE PROTECTION AND PUTIN'S 'POWER VERTICAL'

The flood catastrophe in Southern Russia in the Krasnodar region in early July 2012 demonstrated just how fragile the practices of "monitoring and forecasting" actually are.[68] Not long after the catastrophe, Dmitry Rogozin, a vice-prime minister in Dmitry Medvedev's government, who is in charge of the development of the military-industrial complex and civil mobilization, announced that a "national catastrophe prevention service" will be formed on the basis of a new committee that had been established earlier under the personal supervision of vice-minister Rogozin.[69] Professor of mathematics Georgy Malinetsky from the Keldysh Institute was appointed head of the working group overseeing the formation of the new agency. Malinetsky gave several interviews to the Russian media

[66] Postanovlenie Pravitelstvo RF 2011, p. 15.

[67] MChS Rossii, 'Prognoz chrezvychainoi obstanovki na territorii RF na 2012 god', Tsentr "Antistihiya", Moskva 2011, accessed 15 November 2012, http://www.mchs.gov.ru/forecasts/detail.php?ID=701495.

[68] Almost 200 hundred people died in the floods. The authorities have been criticized particularly for their failure to inform the local population. 'Te, kto pridet posle nas, vy zhe v dva raza huzhe', *Kommersant Vlast*', 20 August 2012.

[69] According to news reports, the main task of the new committee is to provide scientific and political analysis that will help in the re-modernization of the Russian military-industrial complex, and in addition, to propagate information in favour of the military-industrial complex. 'Pri glave Voenno-promyshlennoi komissii bidet sozdan obshchestvennyi sovet', *Kommersant*, 2 July 2012, accessed 17 August 2012, http://www.kommersant.ru/news/1971998.

where he emphasized the need to step up the efforts to monitor and prevent critical infrastructure-related catastrophes in Russia. The capacity of the Russian state to act upon technology-generated risks and natural catastrophes had not improved over the decade, the professor argued.[70]Although too broad a topic to be discussed in more detail here, the administrative reforms conducted in the 2000s are a factor that should be taken into consideration when we try to explain this situation.

For example, the government order on scales of catastrophe from 2007 does not identify the administrative agencies responsible for catastrophe prevention and post-crisis response, as the previous version of the order did. The revision of the law on Security, originally passed in 1992 with changes inscribed by President Dmitry Medvedev in December 2010, should also be mentioned in this context. The law from 1992 listed the customs authorities, firefighters, environmental protection units and so forth as agencies responsible for actions in the sphere of security, whereas in the new edition of the law reference is made only to federal as well as "regional and municipal state organs". What is emphasized instead is the need for coordination and organization of the state actions under a system termed "strategic planning".[71] (See Chapter 3 for a more detailed discussion on changes in the forestry sector.)

During the last twenty years, administrative and financial resources for emergency prevention have been consolidated under the Ministry of Emergency Situations of Russia. The Ministry was formed on the basis of the Russian civil-military agency (MO RSFSR) in July 1991. The first head of the agency (and later Ministry) was Sergei Shoigu, who served in this position until May 2012 when he became a governor of Moscow region.[72] Today, the Ministry has over 200,000 employees, organizing international and domestic rescue services and having responsibility for civil mobilization in Russia. After the forest fires in 2010, the Ministry was promised

[70] 'Vladimir Putin schitaet, sto budushchee Rossii dolzhno byt svyazano s vysokimi tehnologiyami, a ne s energosistelyami', *ITAR-TASS*, 3 December 2001.

[71] K PYNNÖNIEMI, 'Securing Russia? New security law raises more questions than it answers', 14 February 2011, accessed 15 November 2012, http://www.fiia.fi/en/publication/168/securing_russia/.

[72] On November 6, 2012 President Putin replaced Defence Minister Anatoly Serdyukov and appointed Shoigu to this post.

new resources, especially new equipment from airplanes to smaller devices aimed at fighting fires.[73]

The multiple ways in which the changes in the state governance structures have influenced critical infrastructure protection are beyond the scope of this brief analysis. However, previous analysis of Putin's 'power vertical' has suggested that the current Russian administrative system is far from effective, being weakened by systemic corruption and patrimonialism. The role of technocratic administration in the politics is also considered extensive, that in turn, may facilitate authoritarian rule in Russia.[74]

Unlike in the early 2000 policy documents, the inherent vulnerabilities are not reflected at the conceptual level. The current version of the National Security Concept (renamed Strategy) was published in May 2009 and it sets an entirely new tone for the CIP policy. The first sentence of the Strategy makes it clear that "Russia has overcome the consequences of the systemic political and socio-economic crisis of the end of the 20th Century, [...] restored the country's potential to enhance its competitiveness and defend its national interests as a key player within evolving multipolar international relations".[75] The statement reflects the general understanding that despite the major impact of the 2008 global financial crisis on the country's economy, the Russian political system will withstand the major crisis and is even able to pursue modernization within specific sectors of economy.[76]

The scale of threat has shifted from a predominantly environmental sphere or vaguer 'weakening of the state capacity', to "state and public security". The source of vulnerability identified in the text is:

[73] 'Predsedatel' pravitels'tva RF V.V. Putin provel soveshchanie po ukrepleniyu materialno-tehnicheskoi bazy MCHS', 12 November 2010, accessed 15 November 2012, http://government.ru/docs/12895/.

[74] R SAKWA, *The Crisis of Russian Democracy. The Dual State, Factionalism and the Medvedev Succession*, Cambridge, Cambridge University Press; C PURSIAINEN and M PEI, 'Authoritarianism or Democracy?', in C PURSIAINEN (ed.), *At the Crossroads of Post-Communist Modernization. Russia and China in Comparative Perspective*, Palgrave Macmillan, London, 2012, p. 134; E HUSKEY, 'Nomenklatura Lite? The cadres reserve in Russian public administration', *Problems of Post-Communism*, vol. 51, no. 2, 2004, pp. 30–39.

[75] 'Russia's National Security Strategy', approved by Presidential decree no. 537, 12 May 2009, p.1.

[76] K PYNNÖNIEMI, 'The political constrains on Russia's economic development: the visionary zeal of technological modernization and its critics', *FIIA Working Paper*, The Finnish Institute of International Affairs, Helsinki, 16 June 2010, viewed 19 November 2012, URL: http://www.fiia.fi/en/publication/127/the_political_constraints_on_russia_s_economic_development/.

> The activity of terrorist organizations, groups and individuals that aim at the disruption of the normal functioning of state bodies, or the destruction of military or industrial sites, enterprises and institutions providing vital social services, and the intimidation of the population by means including nuclear and chemical weapons or dangerous radioactive, chemical and biological substances.

In contrast to most other definitions of critical infrastructure, the text does not make reference to the cyber sphere and the interconnectivity of complex systems as points of vulnerability. However, as in the US or European definitions of CIP, the idea of a "way of life" as an object to be protected is present in the text. Reference is also made to the task of "improving the quality of life of Russian citizens" and a "healthy lifestyle". Food security, high quality medicine and healthcare are mentioned separately and allow for stylistic as well as conceptual comparison to policies adopted in the US and in the EU. The evolution of the Russian policy on CIP towards terminology used in the West is completed with the current reformulation of the country's cyber strategy.[77]

While it is possible to recognize a resemblance at the terminological and conceptual level, this does not yet indicate that the actual risk management practices are the same. Further research is required to open up the underlying discursive (and concrete) practices that influence the implementation of Russia's CIP policy. What can be observed, however, is a general shift at the policy-planning level, indicated in the following list of the main policy documents on the protection of Russia's critical infrastructures (Table 2). Before 2000, the policies focused on emergencies in general. This changed between 2000 and 2003 when the policies were re-formulated towards 'critical infrastructures'. Recent attention is being focused on cyber-related vulnerabilities.

[77] M IVANOV, 'Sovet federatsii zanyalsya tsifrovym suverenitetom', *Kommersant*, 6 November 2012, accessed 12 November 2012, http://www.kommersant.ru/doc/2060832/print.

Year	Focus on emergencies	Focus on critical infrastructures
1994	*The Federal Law* on “Protection of population and territory from natural catastrophes and technology-generated emergency situations”	
1996	*Government Order* on Classification of Emergency Situations	
1999	*Federal Target Programme* on mitigation of risks and consequences from emergency situations caused by natural or technological disasters	
2000	National Security Concept	National Security Concept
2003		*The state concept* on improvement of chemical, biological and nuclear security
2005		*Government Order* on the establishment of the federal system of monitoring critically important objects
2006		*Conceptual basis* of the state policy on protection of population and critically important and potentially dangerous objects from emergency situations caused by natural or technological disasters and terrorist acts (until 2010)
2007	*Government Order* on classification of emergency situations (revision of Gov Order from 1996)	
2009		National Security Strategy
2011		*Conceptual basis* of the state policy on protection of population and critically important and potentially dangerous objects from emergency situations caused by natural or technological disasters and terrorist acts (until 2020)

Table 2.
The main policy documents on the protection of Russia’s critical infrastructure.

CONCLUSION

While each new catastrophe seems to carry traces of past disasters within it, the same can be said about attempts to mitigate such risks. However, as suggested in the introduction to this report, even if our techniques of coping with complex systems have not radically improved during the last twenty years, interpretations of the phenomenon have changed significantly. We have become more aware that complex systems rarely have a single cause that renders them vulnerable.[78] Perrow singles out greed, or more eloquently put – private gain versus public good – as a factor that multiplies the complexity of the situation through such mundane practices as corporate downsizing or shifting resources from inspection to reinsurance.[79]

Russia is no exception in this regard, although the mechanisms that render public space vulnerable may appear to be different from the viewpoint of a "normal market economy". The analysis shows that the conceptualization of CI in Russia has actually evolved along lines similar to those adopted in the US and Europe, from something discussed mostly in the framework of ecological security to a phenomenon that is understood as a part of the protection of national security against the threat of terrorism. However, if compared to the discussion in the US, the conceptualization of CI in the Russian context has more variations and is still a rather marginal topic in the national security context.

The winter preparedness practice is an example of the state response to potential risks arising from (extremely) cold weather. It is plausible to argue that this is, in fact, an example of political spectacle more than anything else. Further research is required that focuses on the monitoring techniques for emergency situations on the one hand, and on the discourse(s) on critical infrastructure security on the other. This type of research would contribute to a better understanding of critical infrastructure vulnerabilities in Russia and, hopefully, to facilitating international cooperation on mitigating them.

[78] C PERROW, *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, Princeton 1999, p. 353.

[79] C PERROW, op. cit. pp. 340 and 360.

3

3. Threats to critical infrastructure and state responses: The case of the 2010 forest fires in Russia

Irina Busygina

INTRODUCTION

The concept of critical infrastructure (CI) is being used more and more widely both by experts and practitioners.[1] As was discussed in previous chapters, the term critical is used for any large and important infrastructure object whose destruction causes significant damage to a national economy and the life of its citizens. Political scientists, however, are interested in the *political implications* of the threats to CI, and particularly in how different types of states and different political regimes would respond to these threats and to what extent they are capable of maintaining CI resilience.

The complete protection of critical infrastructure can obviously never be guaranteed by any state, even an "ideal" one. However, it has been observed that the way in which states respond differs greatly, and it is not just about potential risk minimization but about levels of preparedness and resilience. As state institutions play a major role in disaster management, the consequences of a catastrophic event are perceived as indicators of the state's capability and decisiveness.

[1] While investigating the situation in Russia, Shibin, Shibina and Kuklin came to the conclusion that "A situation may arise where a significant number of infrastructures drops out of consideration as "critical" because they have not had the required influence on the social and economic position of the region. The role of such infrastructures can suddenly increase in conditions of world crisis. These circumstances necessitate revealing such "latent" potential infrastructures and have prompted the present research." (See SHIBIN, SHIBINA, KUKLIN 2011.) A further interesting project devoted to CI and public attitudes towards the government in rural Russia was recently conducted in the Higher School of Economics. (See LAZAREV et al. 2012.)

Thus, the threats to CI (natural and man-triggered catastrophes) could serve as good tests for state and regime capacity. Open democratic states would give albeit different but nevertheless effective and mostly adequate responses, while authoritarian ones will demonstrate principally different reactions, showing (yet actually veiled with excessive secrecy in the case of certain regimes) the capability of quick mobilization of resources in order to eliminate the consequences of a catastrophe. States with hybrid political regimes where democratic institutions are combined with authoritarian norms and practices (such as Russia) will be in the most vulnerable situation, while in the short term those most directly affected by the disaster can demonstrate even more support for the regime.[2] Every subsequent catastrophe can serve as a catalyst for street protests, whipping up the negative feelings of various societal groups towards the state (the Internet speeds up this process enormously) and resulting in these groups coming forward with political demands.[3]

The state authorities would, however, prefer to focus on technological aspects and solutions (improving surveillance and installing video cameras) instead of introducing political change. It is quite obvious that in a democratic state the unpreparedness of state authorities to deal with disasters and catastrophes, their mistakes and miscalculations, could motivate citizens to start demonstrations. However, the people would hardly demonstrate for political change, but for policy changes and against the activities of certain officials and politicians.

The forest fires in the summer of 2010 provide an excellent case for studying how the Russian government behaves in emergency situations. The Russian wildfires in 2010 were the most disastrous in national recorded history. The fires consumed more than 500,000 hectares of land. More than 50 people died and over 1,200 houses were destroyed. President Dmitry Medvedev declared a state of emergency in seven regions and Prime Minister Vladimir Putin personally participated in the fire-fighting operations.

[2] Y LAZAREV, A SOBOLEV, I SOBOLEVA, and B SOKOLOV, 'Trial by Fire: A National Disaster's Impact on Attitude Towards the Government in Rural Russia'. *HSE Working Papers* WP BRP 04/PS/2012.

[3] V BARASH, and J KELLY, 'Salience vs. Commitment: Dynamics of Political Hashtags in Russian Twitter', *Berkman Center Research Publication, no. 2012-9*, April 4, 2012, Available at SSRN: http://ssrn.com/abstract=2034506; K ALEXANYAN, V BARASH, B ETLING, R FARIS, U GASSER, J KELLY, J.G. PALFREY, and H ROBERTS, 'Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere' (March 2, 2012). *Berkman Center Research Publication No. 2012-2.* Available at SSRN: http://ssrn.com/abstract=2014998

The remainder of this chapter is divided into the following sections. The first section deals with the reactions of different political regimes with regard to disasters and threats to critical infrastructure. The second section briefly examines the case of Chernobyl as an example of the notion that changes in the political regime are essentially reflected in the way in which the political regime copes with threats to CI. Section three is devoted to the causes of the 2010 forest fires in Russia, including institutional factors. Section four examines the various dimensions of Russian state behaviour towards forest fires, while the final section sums up the main arguments of the research.

ON DIFFERENT TYPES OF INCENTIVES AND STATE REACTIONS TO EMERGENCIES

As recent analysis shows, countries with higher income, lower inequality, lower corruption, and more democratic regimes have been found to experience less fatalities in disasters.[4] The effects of catastrophes and disasters are strongly moderated by political institutions. As Quiroz Flores and Smith show, "the same strength earthquake that takes the lives of tens of people in a rich democracy, will kill hundreds of thousands in a poor autocracy as a comparison of the 1989 San Francisco and the 2010 Haitian quakes illustrates. Wealth certainly provides resources with which to mitigate the effects of disasters. But the more important factor for determining the impact of disasters is how political institutions shape the incentive of leaders to use these resources to protect their citizens."[5]

In democratic political systems leaders are quite sensitive to the consequences of disasters, yet the very occurrence of these events has little effect on either the level of anti-government demonstrations or on the survival of political leaders. Democracies are large coalition systems where citizens evaluate the performance of a leader by the amount of public goods he or she provides. These public goods include disaster preparedness, education, prevention, and prompt

[4] See, for example, S COSTA, 'Government Repression and the Death Toll from Natural Disasters' (January 23, 2012). *CESifo Working Paper No. 3703*. Available at SSRN: http://ssrn.com/abstract=1990191

[5] QUIROZ FLORES, A. and SMITH, A., *Surviving Disasters*. Unpublished manuscript, 2010 (New York: New York University, 2010), p. 2. Available at: http://politics.as.nyu.edu/docs/IO/14714/Surviving_Disasters.pdf.

relief efforts once disaster strikes. If a large coalition leader cannot adequately deliver these goods, then citizens will turn to a political rival who can.[6] Therefore, leaders in democracies do have incentives to demonstrate a high level of preparedness, coordination work and resilience. The most useful and effective situation for the society in question is when the state has sufficient decision-making autonomy at its disposal, but when politicians and officials are placed under conditions of accountability and strict responsibility for the decisions they make.

In contrast, in more autocratic systems leaders are beholden only to a small segment of the population. Small coalition systems are marked by a lack of disaster preparedness and resilience. Disaster-related fatalities do not threaten the tenure of a leader in these systems. The survival of a small coalition leader depends upon maintaining the loyalty of a small number of core supporters. Nevertheless, the occurrence of mass disasters *could* threaten the survival of autocratic leaders because it serves as a coordination device among citizens who are already dissatisfied with their government.[7] In his research David Szakonyi comes to the compelling conclusion that electoral institutions not only matter to both citizens and regimes under autocracy, but that these institutions provide an indirect mechanism of accountability to call poorly performing authorities to task. As he shows after studying the political implications of the 2010 forest fires, voters punished the ruling party in subsequent elections for its incompetent response to the natural disaster. Furthermore, United Russia itself removed incumbents from electoral slates in burned areas in order to win back voters.[8]

States with effective economic policies are not only accountable to citizens and the private sector but they are decisive and have administrative capacity. In other words, such states are both *motivated* to provide (state accountability) and *capable* of providing good governance (state capability). The literature seems to increasingly recognize the importance of state capacity as a fundamental ingredient for effective governance.[9] A recent major work by Besley and Persson

[6] Ibid., p. 3.

[7] Ibid., pp. 3–4.

[8] D SZAKONYI, '*You're Fired!: Identifying Electoral Accountability in a Competitive Authoritarian Regime*'. New York: Columbia University, Department of Political Science. April 29, 2011.

[9] See A SAVOIA, and S KUNAL, 'Measurement and Evolution of State Capacity: Exploring a Lesser Known Aspect of Governance'. *Effective States and Inclusive Development Research Centre Working Paper 10*, April 2012. Available at SSRN: http://ssrn.com/abstract=2141901.

defines state capability (capacity) in terms of two major characteristics that enable the state to act effectively.[10] The first focuses on the state's capacity as an efficient tax collector, and the second on its capacity as an effective provider of public services (such as security, law, transportation, and education). Such effective states represent a minor fraction of modern nations, however.

As Bäck and Hadenius argue, the administrative capacity of the state comes as a result of two types of government and control: from the top (where authoritarian political regimes perform better due to their hierarchical structure and repressive apparatus), and from the bottom (where democracies prove to be more successful due to wide electoral participation and freedom of the mass media). Those states with weak democratic institutions find themselves in the most vulnerable position: they lose the control leverage that works from the top down (the erosion of authoritarian order naturally leads to the loss of its advantages), while democratic institutions of government and control from the bottom up do not work effectively.[11]

Thus, research findings suggest that democratic and autocratic political regimes would give principally different responses to CI challenges. However, here we face a significant problem: certain regimes are extremely difficult to classify. More regimes take the *form* of electoral democracy with regular, competitive and multiparty elections. However, these regimes do not correspond with the substance of true democracy. Some regimes with regular elections are, in fact, competitive authoritarian regimes or hybrid ones.[12] Independent observers consider Russia to be an elective authoritarian regime. Many countries fall into this "grey zone" between true democracies and explicit autocracies. In other words, elections exist, but their freedom and fairness are so doubtful that the results differ significantly from the real preferences of the voters, or their civil and political rights are limited to the extent that some (or many) political interests are unable to find channels for representation. In effect, elective authoritarianism creates unfair conditions for competition

[10] T BESLEY, and T PERSSON, *Pillars of Prosperity: The Political Economics of Development Clusters*. Princeton University Press, Princeton, 2011.

[11] H BÄCKAND A HADENIUS, 'Democracy and State Capacity: Exploring a J-Shaped Relationship'. *Governance* 21, 2008, pp. 1–24.

[12] In this article I use the term "hybrid political regime" as an umbrella term for those regimes that could neither be described as democratic nor as authoritarian. Examples of such regimes include Russia and most of the post-Soviet states.

for the government and the opposition, as the ruling party possesses and realizes the advantages of incumbency.[13]

Thus, based on these findings, we suggest that political regimes in the "grey zone" (hybrid regimes) will cope with CI challenges least well: they do not have the affordances of an open democratic state (free information flow, active involvement of citizens, all agencies working cohesively, and so forth) nor the mechanisms of an authoritarian regime (secrecy, repression, strict hierarchy). During and directly after a disaster, hybrid political regimes would presumably show incoherence, chaotic reactions, and loss of credibility.

CHERNOBYL: THE SOVIET LEGACY AND THE PRICE OF SECRECY

Empirical evidence from Russia's recent past supports the idea that changes in a political regime are essentially reflected in the way in which that regime copes with threats to critical infrastructure. The Soviet state was obviously not immune to catastrophes but up to the 1980s, under strict authoritarian rule, it did manage to keep them a closely guarded secret from the population living outside the area. However, the situation changed along with a weakening and "softening" of the regime, as exemplified by the Chernobyl accident.

The accident on 26 April 1986 at reactor number 4 of the V. I. Lenin atomic power station near Chernobyl in the USSR has had an extraordinary effect on both technology and politics. The catastrophe affected the health of many, and experts are still disputing the long-term consequences of the disaster. As Shlyakhter and Wilson argue, the Chernobyl accident was the inevitable outcome of a combination of bad design, bad management and bad communication practices in the Soviet nuclear industry. It appears that the secrecy that was endemic in the USSR had profound negative effects on both technological safety and public health.[14]

It is worth stressing that Chernobyl was not the only large radiation accident in the Soviet Union. In the late eighties, data were released on previous radiation accidents and incidents in the USSR,

[13] L DIAMOND, 'Thinking About Hybrid Regimes', *Journal of Democracy*, vol. 13, no. 2, 2002, pp. 21–35.

[14] A SHLYAKHTER, and R WILSON, 'Chernobyl: the inevitable results of secrecy'. *Public Undestand. Sci.* N1, 1992, pp. 251–259.

specifically concerning the effects of high occupational doses at Chelyabinsk military installation in 1947–1960, and the Kyshtym accident in 1957. The common thread running through all of these accidents is the complete failure of the Soviet system to manage modern technology in a safe manner.[15]

Chernobyl certainly triggered some changes in the policy of the Soviet state. On 25–29 August 1986 the Soviet Union took the extraordinary step of sending experts to the International Atomic Energy Agency in Vienna to describe to their foreign colleagues their understanding of the accident and its consequences. However, despite a certain openness towards the external expert community, the report by Soviet experts to the 1986 Vienna meeting was designated secret in the USSR.

Secrecy about the consequences of the accident had an extraordinarily negative effect on public trust towards the state. By this time the ideological pressure of the state had already weakened.[16] The Chernobyl accident struck a powerful blow to the Soviet state's capacity, causing a crisis of trust towards the state. The Soviet state leadership concealed information about the explosion for about a week following the accident. As a result, tens of thousands of unsuspecting people were on the streets during the May Day demonstrations in Kiev, Minsk, Bryansk, and many other cities, exposing themselves to the risk of getting a serious dose of radiation. In the absence of reliable information, vague rumours caused an unprecedented panic.[17]

Excessive secrecy is characteristic of all totalitarian regimes and is one of their principal weaknesses. All in all, the Chernobyl catastrophe constituted a significant threat to the Soviet state, not due to economic damage, but due to the inability of the regime to react adequately to the emergency.

[15] See G. N. TOMANOV, L. A. BULDAKOV, and V. L. SHVEDOV, 'Irradiation of the population and medical consequences of the accident'. Priroda, May 1990. 63–67.

[16] The events in Novocherkassk in 1962 are a stark reminder of the Soviet leadership's tough stance against civil activism, even during the time of the "thaw". The Novocherkassk tragedy started with a peaceful demonstration by hundreds of workers from the local factory against falling salaries and rising food prices and resulted in twenty dead, seven sentenced to death, and almost a hundred sentenced to lengthy imprisonment in correctional hard-labour camps. A YAKOVLEV, *A Century of Violence in Soviet Russia*, Yale University Press, New Haven and London, 2002.

[17] D KONCHALOVSKY, 'Chernobyl tragedy: the last "gift" from the Soviet regime'. *Moscow Times*, Apr 26, 2012.

THE FREQUENCY OF NATURAL AND MAN-TRIGGERED CATASTROPHES: WHAT CAUSED THE 2010 FOREST FIRES IN RUSSIA?

Disasters have increased in frequency over the past century. A number of high-profile disasters have also dominated news headlines in the past decade, raising media and public awareness of the issue.[18] In other words, this is a global trend and the number of catastrophes, possibly due to technological and climate changes, will only increase in the future. According to Ebert, we have entered a veritable Age of Catastrophes, which have grown both larger and more complex and are now routinely very widespread in scope. Indeed, the old days of geographically isolated industrial accidents, such as the sinking of the Titanic, together with their isolated causes and limited effects, are over. Today, disasters on the scale of Hurricane Katrina, the BP oil spill or the Japan tsunami and nuclear reactor accident threaten to engulf large swaths of civilization.[19] Territorially large countries would naturally have a higher probability of such disasters occurring.

Russia is the most territorially extended country in the world, so taking into account this huge territorial expanse, the condition and variation of the territory, and the distribution of CI objects, natural and technical disasters of differing genesis and scale are to be expected in the country every year. To quote Petrova, "electric power, heat, and water supply systems are most vulnerable to natural impacts among other infrastructure facilities in Russia. The influence of natural events on the critical infrastructure is stronger in the North-Western and Central parts of European Russia, in Krasnodar Territory and the Far East of Russia that are more exposed to hurricanes, snowstorms, rainfalls, icing, landslides, and other natural hazards".[20] According to Malinetzky, Russia's budget for coping with troubles, crises and catastrophes is comparable with the budgets of very weakly developed countries, while the set of risks is the same as in a highly developed country – Russia has 50,000

[18] P AITKEN and P LEGGAT, Considerations in Mass Casualty and Disaster Management. In: *Emergency Medicine – An International Perspective*. Ed. by MICHAEL BLAIVAS. InTech, 2012.

[19] D EBERT, *The Age of Catastrophe: Disaster and Humanity in Modern Times*, North Carolina: McFarland and Company Inc, 2012.

[20] E PETROVA, 'Critical infrastructure in Russia: geographical analysis of accidents triggered by natural hazards'. *Environmental Engineering and Management Journal*, vol. 10, no. 1, 2011.

dangerous and 5,000 especially dangerous objects.[21] (See the previous chapter for more details.)

There were two reasons for the 2010 fire catastrophe in Russia. The first and natural one was the large-scale drought (droughts of such a scale occur in the European part of Russia two or three times a century, occurring in the 20th century in 1936 and 1972). On each occasion, the droughts are followed by extensive forest and peat fires. In many regions the forests and peat are so dry that the tiniest spark will be enough for the forest underlay to start smouldering and quickly go up in flames.[22]

The second reason lies in inadequate institutional changes. Until 2007, there was one administrative agency responsible for forest fire safety, namely the State Forest Guard (Goslesohrana), which had 70,000 professional forestry crawlers. In 2007, when the new Forest Code entered into force, Goslesohrana was abolished and its functions were distributed among regional authorities and private tenants. In fact, the new Forest Code was introduced as a result of the United Russia project “Russian Forest”. As a consequence of this change in the legal basis of forest management, forestry has suffered from degradation and a decline in employment, with the best specialists leaving the sector, and an unprecedented growth in corruption.[23]

Forestry experts have argued that due to these institutional changes, forests are more prone to massive wildfires than before. The expert view is supported by the citizens, who gathered 42,000 signatures in 2009 demanding the reinstatement of Goslesohrana. The demand was relayed to the Presidential Administration, but no response was forthcoming. In April 2010 Greenpeace organized an expedition following the first wave of spring fires: its main conclusion was that the country is completely unprepared for the fire season, so if the weather favours the forest and peat fires, there is no practical way to prevent and control them. Greenpeace issued a special letter to this effect, warning the Russian leadership.[24]

[21] ‘Sistemy Preduprezhdeniya Katastrof v RF Mnogim Meshayut’, Interview of Prof. G Malinetskii, TV-Doshd, 24 July 2012, accessed 10 October, 2012, http://www.newsland.ru/news/detail/id/1001911/.

[22] See e.g. O YANITSKY, ‘The 2010 Wildfires in Russia. An Ecosociological Analysis’, *Sosiological Research*, vol. 51, no. 2, 2012, pp. 57–75.

[23] Ibid.

[24] Greenpeace Press release, ‘Grinpis podvel itogi protivopozharnoi ekspeditsii’, 14 May 2010, accessed 3 November 2012, http://www.greenpeace.org/russia/ru/press/releases/4695583/.

In the above sections I have put forward certain theoretical hypotheses to explain the behaviour of the "grey zone" regimes when their CI is under threat. In the following, I will discuss how the practical reactions of the Russian state during the 2010 forest fires corresponded with these insights. I will start by discussing some important framework conditions for coping successfully with the threats to CI presented by previous research on this subject.

"ONE-MAN CONTROL" OR AN ALL-AGENCIES APPROACH?

In its 2006 report, the United States National Research Council linked disaster resilience to the concept of social capital and emphasized the importance of both horizontal integration (within the community) and vertical integration (across different scales) among entities participating in loss-reduction activities. Stronger networks provide a greater opportunity for creating interpersonal trust. Intracommunity ties thus constitute the fundamental building blocks of a disaster-resilient society. However, there is also the need to link communities vertically to other external entities. External ties – for example, among local communities and state and federal governments, local companies and their parent corporations, and local chapters of non-profits and their national headquarters – bring benefits that cannot be realized through intracommunity linkages alone. The benefits include connections to broader societal institutions, expansion of trusted networks, and greater access to funding, expertise, and other resources.[25] Both types of integration – intracommunity ties and external ties – are necessary to maximize the ability of communities to mobilize, learn, and innovate. Emphasizing the importance of vertical ties between community networks and external entities does not imply that communities relinquish their decision-making authority to outside control.

These positions correspond with the "all-agencies approach" that emphasizes the multiple agencies that come together in disaster management. Nobody responds alone and preparations should ensure

[25] *Facing Hazards and Disasters: Understanding Human Dimensions.* United States National Research Council, 2006.

the ability to work together and ‘play happily together in the sandpit’. For this to occur, organizations need to come together in advance as a part of preparedness. It is not just a common language and the interoperability of systems that is important. A common finding in post-incident reviews is that the pre-incident development of networks, relationships and trust between individuals is an important determinant of successful outcomes.[26]

The Russian state demonstrates a principally different approach that could be described as “one-man control”. Thus, during the summer 2010 fires, Prime Minister Vladimir Putin was the most active, or at least the most visible, government leader in the media, even at the expense of Sergei Shoigu, the popular and long-serving minister of emergency situations. Governmental communications at the time presented good government as an exercise in personal control by the prime minister, supported by the use of specific communication tools and regulatory instruments during reconstruction.[27]

During the 2010 fires, governmental communications focused on the prime minister’s role (field visits, official meetings). Throughout these communications, and in the Russian mass media’s interpretation of the disaster and its management, the concept of personal control (in Russian, *lichnyi kontrol*) is omnipresent.The concept portrays Vladimir Putin as *monitoring all regulatory activities during the disaster*.

COMMUNICATION, COMMAND, COORDINATION

Communication is the most common problem identified in most disaster reviews.[28] It is also essential to remember that communication is not simply disseminating information but is a two-way

[26] AITKEN and LEGGAT 2012.

[27] E BERTRAND, ‘Constructing Russian Power by Communicating During Disasters The Forest Fires of 2010’, *Problems of Post-Communism*. Volume 59, Number 3, 2012, p. 33.

[28] J L ARNOLD et al., ‘Information sharing in out-of-hospital disaster response: The future role of information technology’. *Prehospital and Disaster Medicine*, vol. 19, no. 2, pp. 201–7; M BRAHAM et al., 5th Asia-Pacific conference on disaster medicine. Theme 7. Sharing international experiences in disasters: Summary and action plan. *Prehospital and Disaster Medicine*, vol. 16, no. 1, 2001, pp. 42–5; T C CHAN et al., ‘Information technology and emergency medical care during disasters’. *Academic Emergency Medicine*, vol. 11, no. 11, 2004, pp. 1229–36; R V GERACE, ‘Role of medical teams in a community disaster plan’. *Canadian Medical Association Journal*, 120, 1979, pp. 923–8; D A MCENTIRE, ‘Balancing international approaches to disaster: rethinking prevention instead of relief’. *Australian Journal of Emergency Management*, 13(2), 1998, pp. 50–55.

street, and as much care needs to be taken over ensuring the ability to receive messages and information as when disseminating them. Command, control and coordination arrangements became a point of emphasis after the California wildfires in the 1970s. This approach recognized that there are limited spans of control and a need for clear lines of command within organizations and communication across organizations. Failure to implement this may lead to difficulties over an integrated response and either task omission or task duplication.

Coordination brings together organizations and elements to ensure an effective response, and is mainly concerned with the systematic acquisition and application of resources in accordance with threat or impact.[29] Some may argue that a coordinating function is not consistent with the committee's suggestion that decision-making should remain decentralized. The committee would counter that decentralized decision-making is possible within an organized structure. Rules and guidelines exist to direct the structure, but the structure does not direct the outcomes of decision-making processes. As long as there is consensus regarding the rules of collaboration and the actions of a coordinating person or body, and as long as those rules are regularly evaluated for their relevance, decentralized decision-making is possible.[30]

That does not imply that collaborative efforts should be driven by federal regulations and requirements or that collaboration should be approached in a uniform fashion in communities around the country. As with any programme designed to address national problems, successful solutions developed to improve disaster resilience reflect the diversity of local communities around the nation. As the US experience shows, because of the importance of local-level buy-in to sustain the effort, it can be counterproductive for higher organizational levels in both the private and public sectors to provide more than technical, logistical, or financial support unless requested and coordinated with local leadership.[31]

During the summer 2010 fires, the prime minister's communications defined power in just this way: as an exercise in federal leaders' control of regional ones. This logic of subordination corresponds to

[29] AITKEN and LEGGAT 2012.

[30] *Building Community Disaster Resilience Through Private-Public Collaboration*. The National Academies Press, Washington D.C., 2011, p. 66.

[31] Ibid., p. 67.

the system that Putin revived as the "power vertical" in the 2000s.[32] During the 2010 fires, the videoconferences portrayed the political action as regional actors (governors, in the first instance) reported their regional situation to the prime minister and the government made a decision, subsequently transferring the necessary resources from the federal centre to the regions, which implemented the decision. A meeting on August 2, 2010, which brought together Vladimir Putin and federal and regional representatives of various state structures in charge of disaster management, illustrates this top-down cycle. (See previous chapter and discussion on 'winter preparedness'.)

THE PROBLEM OF OPEN AND CREDIBLE INFORMATION

One of the crucial conditions indicating the capability of a state to cope with the threats to CI is related to information – how and through which channels it is disseminated, and how reliable it is. In this respect we can observe different scenarios in different societies. For example in the US a major trend is the dramatic change in the mechanisms through which information about crises is disseminated among the American public. The crises, although they may be triggered by natural phenomena, are not themselves natural phenomena. Rather, a community must agree, through some process of information-sharing and deliberation, that an event constitutes a crisis: that is, that the event profoundly threatens some valued state of affairs and demands an urgent response by specific actors.[33]

The premise is that profound changes in information and communication technologies transform events into crises more rapidly. Moreover, this technological transformation has the effect of federalizing the problem of crisis management insomuch that more pressure is put on the US national government to take the lead in managing the response to major crises. In other words, a technological change is shifting opinion on the constitutional question of where the primary responsibility for crisis management should lie. This technological transformation is a distinctly post-millennial trend. However, it collides with a second reality of contemporary governance: that

[32] BERTRAND 2012, p. 36.
[33] SCHNEIDER 1985.

the US central government is ill-suited to respond authoritatively to crises because of a combination of ideological and institutional constraints on federal action.[34]

Russia is facing its own trend with regard to the dissemination of information. Thus, during the summer of 2010, the use of the Internet by Russian citizens to inform and to become informed spread largely through independent websites or blogs. This was not the case previously and it drastically changes the conditions in which federal and regional authorities currently operate.

Indeed, there is no way for the central and regional authorities to completely conceal information about the catastrophe from the general public.[35] In fact, this "informational dimension" is one of the most important ones separating democratic, authoritarian and "grey zone" political regimes. In democracies, the authorities could not intentionally conceal information about a disaster since this could cost politicians and officials their career. An authoritarian state would rely (albeit with less success due to the "CNN effect") on secrecy, however, to try to minimize the spread of information. This leads us to ask what kind of strategies the "grey zone" regimes might adopt. As the 2010 forest fires in Russia have shown, the political regime demonstrated several ways of "playing" with information. The example below shows that information was strictly regulated, shaped, or at least influenced by the government.[36]

A) *Understatement about the scale of the disaster, the damage caused by it and hence the degree of its "criticality".*
In general, according to data from the Global Fire Monitoring Center, the competent international organization, the area ravaged by forest fires in Russia between January and August 2010 was more than 15 million hectares. However, according to data issued by Rosleskhoz and the Ministry of Emergency Situations, the area was estimated at

[34] A ROBERTS, 'Building Resilience: Macrodynamic Constraints on Governmental Response to Crises'. *In: Designing Resilience for Extreme Events: Sociotechnical Approaches*, A. BOIN, L. COMFORT, C. DEMCHAK, eds., Pittsburgh, PA, University of Pittsburgh Press, 2009. pp. 84–105.

[35] 'Zaklyuchenie Obshchestvennoi Komissii po Rassledovaniyu Prichin i Posledstvii Prirodnyh Pozharov v Rossii v 2010 godu', 14 August, 2010, Yabloko Party, accessed 3 November, 2012, http://www.yabloko.ru/mneniya_i_publikatsii/2010/09/14.

[36] BERTRAND 2012, p. 32.

10 times less.[37] The evaluation of the scale of the damage caused by the forest fires published in official sources is based on two indicators: the cost of timber and the cost of standard reforestation works. In other words, the statistics take into consideration neither the costs of cultivation during the first 5–10 years after implantation nor the non-timber losses: loss and recovery of fauna and flora. Moreover, official evaluations do not consider basic ecological services — the production of oxygen, clean water, recreational services, protecting the soil against erosion, and so on, as a part of these calculations.[38]

B) *Information gap*
Although wildfires began in some regions in early May 2010 and continued to spread into July, the government did not begin communicating about the disaster until late July 2010.

C) *Filtering the information*
During the 2010 forest fires, government communications focused mainly on those consequences of the disaster that could be brought under control.

D) *Playing with the terms*
The state's emergency management agencies officially defined "forest fires" as an "uncontrolled (natural) burning that covers a forest area".[39] This definition seems to fit the summer 2010 disaster perfectly. The change in the classification of the disaster thus conveys a shift from potential accusations directed at the forest management agencies to a statement that the situation was unmanageable. The idea of an event beyond the control of state structures is also present in the designation of the fires as a "catastrophe," "tragedy," or "nature's surprise" (*siurpriz prirody*) like anomalous heat (*anomal'naya*

[37] GREENPEACE, 'Press–reliz: Pozharnaya Katastrofa v Lesah Rossii Neizbezhno Povtoritsya, esli Polnotsennaya Sistema Gosudarstvennogo Upravleniya Lesami ne Budet Vosstanovlena', 26 August, 2010, accessed 5 November, 2012, http://www.greenpeace.org/russia/ru/press/releases/4929433/; See also YANITSKY, 'The 2010 Wildfires in Russia: An Ecosociological Analysis', p. 60.

[38] Ibid.

[39] The official definition of a "forest fire" comes from SERGEI SHOIGU, *Atlas prikhodnykh I tekhnologennykh opasnostei i riskov chrezvychainykh situatsii, Rossiiskaia Federatsiia, Privolzhskii federalnyi okrug* (Atlas of the Natural and Technological Hazards and Risks of Emergencies in Volga Federal Okrug of the Russian Federation) (Moscow: Dizain informatsiia, 2008), p. 112.

zhara).[40] Such language shapes the idea of an irrational event that cannot be handled by rational means, such as the prosecution of those found guilty of mismanaging the situation.[41]

We should not forget, however, that Russian executives have made some attempts to organize the way in which they inform the population about emergency situations through the mass media. As early as 2006 the Ministry of Emergency Situations adopted an Administrative Regulation as an Annex to the Order of the Ministry. It was stated in the Annex that the information on emergency situations should be public and open. Parts of the Annex are questionable, however. First, officials are not allowed to provide the population with any information about disasters that could cause panic among the population. This formulation could be subject to diverse interpretations, however. Second, it is not clear from the Annex why criteria for the decision on informing (or not informing) the population are based only on the scale of the disaster – from local to federal.[42] (See Chapter 2 for more details on the categorization of the scale of a disaster.)

A "PREPARED COMMUNITY" – IS THIS THE CASE IN RUSSIA?

The final crucial framework condition relates to the preparedness of a local/regional community directly affected by a disaster. The prepared community recognizes that the initial response will be from those in the affected community. External assistance will take time to arrive and in the meantime local people will turn to local agencies and organizations for assistance. Thus, increasing the ability of the local community to respond increases the ability of the community to manage the disaster. This can be defined accordingly: "a prepared

[40] http://www.putin.ru/russiannews/105-newsline-premiergovru-russian/15215-vvputin-provl-videokonferenciyu-s-rukovodstvom-regionov-postradavshih-ot-prirodnih-pojarov.html.

[41] This "nature's surprise" approach is also clearly reflected in the discussion that the State Duma deputy Evgeniy Fedorov (United Russia Party) had with Maxim Sokolov about the flood in Krymsk where 170 people died. Fedorov: "And now – it was raining, a natural catastrophe arose, this led to tragedy...". M SOKOLOV, Radio Svoboda, 17 July 2012, accessed 03 November 2012, http://www.svobodanews.ru/content/transcript/24646817.html.

[42] Annex to the Order of the MES of RF 'Ob utverzhdenii administrativnogo reglamenta ministerstva po organizatsii informirovaniya naseleniya o chrezvychainykh situatsiyakh', 29 June 2006, no. 386.

community is one which has developed effective emergency and disaster management arrangements at the local level, resulting in: (1) an alert, informed and active community, which supports its voluntary organizations; (2) an active and involved local government".[43] Deployed teams need to integrate with local services. It is the local services that will have provided the initial care and it is the local services that will continue to provide care after the deployed team has left. The local population should ideally be involved in all phases of relief operations as it enhances capacity building, empowers local communities and helps regain control over their lives.[44] Failure to do so can lead to mistrust, resentment, and lack of cooperation[45], and undermine the capacity of local people to solve their own problems.[46]

Bottom-up interventions are essential because local conditions vary greatly across the country and jurisdictional issues often revolve around who can respond to the call to increase resilience, and when. The nation's communities are unique in their history, geography, demography, culture, economic enterprise, governance, and infrastructure. Moreover, the risks faced by every community vary according to local hazards and exposure levels, vulnerabilities, and capacities to mitigate.[47]

The huge North Vietnam floods in 1971 only resulted in a few hundred deaths, largely because of a highly efficient wartime village-level organization that allowed rapid evacuation and provision of first aid, whereas the similar 1970 Bangladesh floods killed a record 300,000 people.[48] Thus, the mobilization of a broad spectrum of community organizations and sectors is a key factor enabling effective disaster response. Achieving resilience at the state or national levels begins with resilience-enhancing efforts in local communities.[49]

Meeting this condition is, however, impossible without a certain level of autonomy for regional and local authorities. In Russia, relations between the federal centre and the regions during recent years have developed according to the notorious "power vertical" model.

[43] AITKEN and LEGGAT 2012.

[44] BRENNAN et al., 2001; LEUS et al., 2001.

[45] BRENNAN et al., 2001.

[46] JUDD, 1992.

[47] *Disaster Resilience: A National Imperative*. The National Academies Press, Washington, D.C., 2012, p. 97.

[48] B WISNER, *Natural Hazards, People's Vulnerability and Disasters*. London: Taylor & Francis, 2003.

[49] *Building Community Disaster Resilience Through Private-Public Collaboration*. The National Academies Press, Washington D.C., 2011, pp. 58–59.

The abolition of direct elections of the governors, which resulted in a decrease in political competition, put regional executives in the position of agents with regard to the federal authority (the principal). Indeed, in this system the governors obeyed and acted on behalf of the federal executive that acquired the mechanisms for their punishment and rewards. The principal's main requirements from the agent were the preservation of political loyalty and the provision of electoral results "ordered" by the centre.

Beyond these agreements, the centre connived with the regional authorities, giving them the freedom to act which was, in effect, the reward for the agent.[50] The regional authorities also had the opportunity to increase the degree of their freedom using "informational asymmetry" – often providing incomplete information to the centre or deliberately misinforming it. As Gel'man and Ryzhenkov argue, in the Russian power vertical model, the actors (regional and local) know that the central authorities are indifferent towards certain results of the political process. The federal centre firstly demands social patronage from the regional authorities, followed by the guarantee of certain electoral results and political stability in the region.[51]

This order is very similar to the imperial one. Yet under the current conditions, coercion alone cannot secure the viability of such a multiethnic state if it conflicts with the interests of the regional elites. That is why the empire tries to achieve stability through the elimination of political competition and appointment to the elite on the basis of personal loyalty to the central leadership.[52] Not having adequate resources for total control over the regions, the empire imposes elements of non-centralization, namely indifference towards the activities of the regional authorities beyond the agreements reached with the centre. It seems that the federal centre is the only beneficiary of such a system. However, this is not the case. The regional authorities have little autonomy in the system, but they could effectively play this "card" to explain their unpreparedness to the population in the event of a disaster and shift all the responsibility for unsuccessful actions onto the federal authorities.

[50] I BUSYGINA, and M FILIPPOV, 'Agents and principals: what should we wait for after "power vertical"?' *Neprikosnovennyi zapas*, no. 4, 2012, pp. 67–82.

[51] V GELMAN, and S RYZHENKOV, Lokal'nye regimy, gorodskoe upravlenie I "vertikal' vlasti v sovremennoi Rossii (http://www.politex.info/content/view/764/30/)

[52] I BUSYGINA, and M FILIPPOV, 'Problema vynuzhdennoi federalizatzii', *Pro et Contra*, Vol. 13, No. 3–4, 2009.

Disasters are increasing in their frequency. As a consequence, the issue of providing a safer environment is of paramount importance. However, it cannot be achieved by technical measures alone. It should address the root causes by challenging any ideology, political or economic system which causes or increases vulnerability. The ability of society to avoid or minimize the costs of a catastrophe is profoundly influenced by its form of political and economic organization, political culture, and information-technology capabilities. These societal characteristics must be accounted for in any assessment of a society's response to particular disasters.

Political regimes demonstrate principally different reactions and different levels of state capacity when it comes to threats to critical infrastructure, the main lines of division here being between democratic, authoritarian and hybrid regimes. I argue that hybrid regimes (Russia being one such example) find themselves in the most vulnerable situation since they lack the leverage of both government and control that "pure" types of political regimes are able to apply. Therefore, threats to critical infrastructure (natural and man-triggered catastrophes) are important not only per se but could serve as good tests for state and regime capacity.

I've examined the reactions and behaviour in the Russian state during and after the forest fires of 2010, which are considered to be the most disastrous in national recorded history. In concrete terms, my analysis focused on the mode of control, the channels of communication and coordination, the problem of open and credible information and, finally, the preparedness of local/regional communities for disasters. In general, with regard to the fires, the Russian state demonstrated the "one-man control" model (instead of the all-agencies approach), the logic of subordination in terms of command and communication (which, in practice, often led to chaotic and incoherent actions), and "played" with information of different kinds, revealing serious discrepancies between the official rhetoric and the real state of affairs.

Disasters are localized in a particular territory, affecting a particular region or regions. That is why the role of regional authorities and communities is considered to be crucial. However, regional authorities, even if they were so inclined, cannot compensate for the "bad quality" of the state at the national level. Even if we envisage a group of brilliant, modern, non-corrupted and strong-willed political leaders in the regions, it would nevertheless be beyond their ability to build an “ideal” region and to successfully manage the threats to critical infrastructure alone. This would probably be hard to achieve anywhere, but in Russia they also lack the incentive to do so, using the “power vertical” model and shifting responsibility to the federal executive instead. Under such conditions, it would be naive to expect a sufficient level of preparedness for threats in the regional and local communities.

4

4. Re-reading critical infrastructure — A view from the indigenous communities of the Russian Arctic[1]

Tero Mustonen

INTRODUCTION: THE GOVERNANCE-SECURITY-KNOWLEDGE COMPLEX

This article investigates the concept of critical infrastructure (CI) in the Russian Arctic using two case regions — Murmansk and the Republic of Sakha-Yakutia — both located on the periphery. The methodology of visual documentation of developments in the region in addition to the oral histories of the indigenous peoples are used in reviewing the CI concept and its applicability to the discussion on the developments taking place in the Russian Far North.

The article starts by outlining a three-step process that is often taken for granted when we discuss critical infrastructure. First, *governance* of the state territory that is structured as a power flow from the centre to the peripheries, from the top down. Such governance, in turn, is built on the notion of "*security*", being secure, and securing the governance of violence as a state monopoly. In this sense, the notions of resilience and CI are often referred to as the capacities of the state structures to absorb damage, sustain themselves through crises, and so on. Furthermore, the contemporary

[1] Materials for this paper were gathered during a series of field visits to the Murmansk region and the Republic of Sakha-Yakutia in August and September 2012. Additional materials were drawn from the Snowchange Cooperative community-based scientific work in these communities during 2001–2012. All indigenous oral histories have been approved by the communities in question for use here. Full referencing and original digital tapes are in the possession of the communities themselves as well as the Snowchange Cooperative Oral History Archive. The author is grateful to the MATINE Research Initiative as well as Dr Katri Pynnöniemi for allowing this work to take place.

times are seen as times of "risk"[2], with whole societies and their futures being immersed in "risks". There are few discursive elements on how and why these risks are manifested or were created. Instead, the time-space reference of this discourse is one of an empty field of emergence with few or no histories or memory. Thirdly, knowledge from the experts, often scientists and policy analysts, provides state decision-makers with the means to make decisions to implement CI and act as needed.

In this article, I refer to this process as the governance-security-knowledge complex, and argue that this model of governance is built on fear. This fear consists of a number of specific aspects (fear of the loss of existing systems, fear of uncertainty, and fear of 'chaos') but most importantly, it is a fear of nature, of what nature is and how it functions. The broader context for the manifestation of this fear rests with the close integration of CI into the larger fabric of the 'Western'/ Indo-European way of life as Pynnöniemi (see Chapters 1 and 2) demonstrates. Ultimately, the CI decisions can be seen as mechanisms to protect our comforts, established truths and projections of power across the globe through the subjugation of peoples and nature, and entire ecosystems.

It has become globally recognized that the technological societies of the 21st century have become removed from sustainable relations with both their local ecosystems as well as the global biosphere.[3] The governance-security-knowledge complex is unsustainable, lacks the capacity for the self-reflection needed to correct mistakes, yet possesses *power* in the current international system. Furthermore, the fear of nature that manifests in this complex contributes to the very problem that many critical infrastructure notions are trying to "control".

It should be added that this power complex is often a mix of both state and multinational companies, and in the case of the Russian Arctic it is hard to separate the two categories of entities, especially regarding natural resource exploitation or military processes. For example, the most significant threat of our times, (Arctic) climate change[4], which is now climbing to the top of the security agenda in many states, has been caused by the very same events and actors

[2] U BECK, *World at Risk*, Malden: Polity Press 1999.

[3] T MUSTONEN, *Karhun väen ajast aikojen avartuva avara*. Joensuu: University of Joensuu Press, 2009; Arctic Council, Arctic Biodiversity Assessment, 2013. Forthcoming.

[4] Arctic Council: Arctic Climate Impact Assessment, 2005.

(unlimited exploitation of fossil fuels, unsustainable infrastructure and transportation decisions) that are now preparing to both survive the impacts and utilize the new opportunities[5] for further resource development. On the other hand, it is the indigenous communities, located on the peripheries for centuries, for whom the encroachment of CI poses a threat.

Photo 1.
Shipping along the Lena River, the Republic of Sakha–Yakutia, Russia, summer 2012.
Photo: Tero Mustonen

TRADITIONAL KNOWLEDGE USED TO REVIEW THE CRITICAL INFRASTRUCTURE CONCEPT

Juxtaposed with this power complex of fear, which is conceptualizing and defining various aspects of its existence as "critical infrastructure", is the *traditional knowledge*[6] of those local and indigenous communities in the Russian Arctic that still try to maintain their partly-autonomous cultures, communities and subsistence practices and economies such as reindeer herding, fishing, and hunting and gathering.

From the perspective of resilience, it is important to realize that these communities *choose* to maintain the core elements of their own brand of subsistence economies, knowledge and time-spaces[7] even though since the dawn of the Soviet times the modern choice has been available, albeit often through forceful repression. Even

[5] Arctic Council: Arctic Marine Transport Assessment, 2009.

[6] MUSTONEN 2009.

[7] Ibid.

though these communities do not exist in a vacuum and often have mixed ways of life where Russian and Western technologies, such as snow ploughs and radios, intertwine with the use of traditional practices and tools, the main point here is the ongoing sense of the world — traditional knowledge embedded in subsistence and landscape-wide activities — that provides these communities with autonomous, resilient capacities for a meaningful existence outside and often in direct conflict with modern needs, and modern land use. The whole notion of resilience is turned upside down, once viewed from the indigenous subsistence community perspective.

What is more, many of these indigenous communities are in a state of *re-emergence* — they are claiming spheres of life and traditional livelihood territories across the Russian North in the context of the post-Soviet withdrawal of the state. Many of the communities have re-established themselves as *obschinas*. The Federal Law No 82-F3 1999 defines *obshchina* in the following way:

> Obshchiny and other forms of social self-governance are forms of self-organisation of individuals, belonging to the Numerically Small Peoples, united on the basis of blood kin relations (family, kin) and/or territorial-neighbourhood principles, created with the aim to protect their original territories of inhabitancy and to protect and develop their traditional ways of life, economies and culture.[8]

Photo 2.
Turvaurgin community subsistence fishing along the Bolshaya Chukotskaya River, the Republic of Sakha-Yakutia, Russia, summer 2012.
Photo: Tero Mustonen

[8] V VLADIMIROVA, *Just Labor — Labor Ethic in a Post-Soviet Reindeer Herding Community*. Uppsala: Acta Universitatis Upsaliensis, 2006. p. 320.

Fondahl et al. argue that in the period since the fall of the Soviet regime, the indigenous leadership has called for a reform of the relationship between the state and the aboriginal peoples. The target of these arrangements would be "optimum land tenure organization". The establishment and creation of the *obshchina* communities would be the engine for this indigenous territorial reform. Fondahl et al. also position the prospects for the *obshchinas* in the wider fabric of the Russian context: "Aboriginal 'land claims' affect the future geographies of resource development, and can play an important role in the tug-of-war between regional governments and Moscow, as well as sculpting the opportunities of aboriginals to determine their own futures."[9]

The relationship between the indigenous societies and the Russian state has been complex for centuries, as Slezkine argues:

> "Over the last one thousand years, East Slavic agrarian society with its increasingly elaborate social and legal institutions has expanded to include and partially absorb numerous hunting and pastoral groups. No longer 'foreigners' but still alien insofar as they remained 'unsettled', these peoples have repeatedly posed a challenge to government officials, Orthodox missionaries, and assorted intellectuals seeking to define Russianness and otherness to both Russians and others. … The foragers of the 'northern borderlands' have rarely threatened the settled/Christian/civilized world and have remained invisible in most versions of its [Russian] past. Yet of all the non-Russian subjects of the Russian state and of all the non-Russian objects of Russian concern, it is the circumpolar hunters and gatherers who have proved the most difficult to reform and conceptualize. From the birth of the irrational savage in the early eighteenth century to the repeated resurrection of the natural man at the end of the twentieth, they have been the most consistent antipodes of whatever it meant to be Russian. Seen as an extreme case of backwardness-as-beastliness or backwardness-as-innocence, they have provided a remote but crucial point of reference for speculations on human and Russian identity, while at the same time serving as a convenient testing ground for policies and images that grew out of those speculations."[10]

[9] G FONDAHL, O LAZEBNIK, G POELZER, and V ROBBEK, 'Native "land claims", Russian style'. *Canadian Geographer*, January 2001.

[10] Y SLEZKINE, *Arctic Mirrors — Russia and the Small Peoples of the North*. Cornell University Press, 1994, p. ix.

To offer a context for these times, a respected Even scholar from the Republic of Sakha-Yakutia, Vasili Robbek, conceptualized the current moment in the following:

> "During the recent decade, the Indigenous Peoples of the North, Siberia and Far East [...] discussed the single vital question of the present-day reality – to be or not to be – to preserve themselves in the 21st century as a self-reliant ethnic group or to assimilate and dissolve in the million-strong mass of Russians, to lose the centuries-old culture, languages, customs and tradition. The successful solutions of the issue depend on the [capacity] to overcome the generation gap, not just on the ethnic level but even deeper – on the internal level of a nomadic family. The united efforts during the recent decade have resulted in a solution which is the creation of a completely new education system for the Indigenous Peoples of the North with the formation of various types of nomadic schools as the core constituent."[11]

This view will be explored using the case studies from Murmansk and the Republic of Sakha-Yakutia. More specifically, the traditional knowledge of the indigenous communities, as opposed to the governance-security-knowledge complex, has some other characteristics. It is a form of experienced witness knowledge built on generations of people living with the ecosystems. We can define it as a ground-up process of knowledge as opposed to the top-down structure of state knowledge and decision-making.

This traditional knowledge provides 'real' evidence of a situation on the ground. This evidence leads the individuals and their communities to reshape (or not) their priorities on the ground. It is a constant process of occurring. Concepts of time and space are not bound or fixed as they are in technological societies.[12] This traditional knowledge and decision-making (for example on reindeer herding territories or fisheries) comes into contact and most often into conflict with the top-down produced powers and knowledge of the state (state programmes, laws, and geopolitical and critical infrastructure decisions).

[11] V ROBBEK, *Scientific Basis of Education System Formation of Nomadic Peoples of the North*, Nauka, Novosibirsk, 2007, p. 53.

[12] MUSTONEN 2009.

Traditions also contain what could be termed ancient *memory* (often extending beyond the written records of the technological societies) contained in the oral histories of the indigenous peoples, as well as hidden and esoteric knowledge. Most importantly, these societies, if still rooted in their landscapes and homelands, are operating for the most part *with* nature, as opposed to *fearing* nature or trying to control and overcome nature due to this multi-generational fear.

I argue for the need for a respectful dialogue with these communities by trying to identify and show what an observant reading of "critical infrastructure" means from this viewpoint. While criticism can be levelled at such a positioning by saying that indigenous peoples should not be romanticized, and "noble savage" stereotyping should be avoided, I am strongly convinced[13] that a proper dialogue with these communities can offer significant improvements for the technological societies amidst their current crisis of fear of nature. One of the strongest arguments for this is that indigenous societies, such as the Sámi of the Kola Peninsula or the Chukchi are *still here*, after thousands of years of living in their territory, and continue to manifest (relatively) stable societies and relationships with their ecosystems, despite the damage inflicted on them due to the colonial and Soviet processes.

For the state, in this case Russia (and with its arrangements, the EU), critical infrastructure means for the most part securing energy sources (e.g. oil and gas), transport corridors (e.g. the Northern Sea Route), and portraying an ongoing military presence in the Arctic, especially in these unstable and unpredictable modern times. For the indigenous communities, which have been located since time immemorial along these state locations and manifestations, the CI presence becomes a threat in itself — nowhere in more pronounced ways than in the little-regulated oil and gas industries in the Nenets and Khanty homelands (treatment of which is beyond the scope of this article).

The following sections will explore three cases (the Murmansk region, Northern Sakha-Yakutia, and Southern Sakha-Yakutia) and the ways in which the governance-security-knowledge complex is manifested in the regions in their relationship with the traditional knowledge of the indigenous communities. The concluding notes will then steer us towards a redefinition of what "critical infrastructure" could mean for the Russian Arctic territories.

[13] Ibid.

THE MURMANSK REGION AND THE CRITICAL INFRASTRUCTURE OF GLOBAL FLOWS

The Murmansk region is located on the Kola Peninsula, in the northwestern corner of the Russian Federation. The city of Murmansk is an ice-free port, and the administrative centre of the area. The region has a population of approximately 795,000, and the territory spans approximately 144,900 square kilometres. The region is known for its rich mineral deposits and for being a convenient departure point for the Northern Sea Route. This allowed minerals from other parts of the Soviet Union to be transported[14] to the region for processing. Many of these sites, such as Monchegorsk, Apatity and Nikel have suffered significant ecological damage due to these developments since the 1940s and have been declared global environmental hotspots.[15]

The presence of the governance-security-knowledge complex is very pronounced in Murmansk. It is an essential geopolitical asset (home of the Northern Fleet), home base of the transport corridors of the Northern Sea Route (home of the Atomic civilian fleet) and a potential source of oil and gas from the Arctic zone. As a result, the Murmansk region is aptly located at the heart of the CI debates on crucial systems of operation for the survival of the state and the modern society.

The region declined in importance in the 1990s[16] and many people moved to southern Russia. Currently, the region is re-emerging as a global energy and geopolitical hotspot due to the effects of climate change and the opening of the transport corridor in the Arctic. The Northern Sea Route (the NSR) can shave 2–3 weeks off shipping time between Europe and Asia, achieving significant savings on fuel and transportation costs. Rapidly advancing climate change[17] is opening up the route, which is predicted to be ice-free as early as the 2030s, according to some estimates.

By way of comparison, in the late Soviet period in the 1980s, approximately six million tonnes of cargo were transported along the NSR. In 2010, four ships used the route with a total cargo of 110,000 tonnes. In 2011, 30 ships used the route, with a total cargo of

[14] T MUSTONEN and K MUSTONEN, *Eastern Sámi Atlas*. Kontiolahti: Snowchange Cooperative, 2011.

[15] Ibid., pp. 148, 153.

[16] Ibid.

[17] Arctic Council 2005; Arctic Council 2013.

820,000 tonnes. In 2012, according to Rosatomflot, only nine ships had passed through the Northern Sea Route by September, including seven cargo ships, one tugboat ship and one Chinese icebreaker.[18] The cargo has primarily comprised oil and gas products. Ice conditions have not been good, and the East Siberian Sea remained frozen in late July 2012. The legal context is still evolving, and the framework for increased shipping will not be in place until 2013. State officials have said that the NSR needs a significant upgrade in terms of "monitoring and security systems"[19], with the home base for rescue vessels currently slated to be Amderman village on the Kara Sea.

The atomic icebreakers stationed in the port of Murmansk and in the vicinity assist the NSR operations. The Northern Fleet of Russia is situated a little further up the coast, with its headquarters in the closed military city of Severomorsk. The Russian state is looking to secure and strengthen its geopolitical and military assets in the region. At the centre of this process are the nuclear facilities, and both civilian and military ships. This is where the disparity between the governance-security-knowledge complex and its CI aspirations is most acutely felt: there is a lack of understanding and knowledge concerning what happened the last time such power structures were built up during Soviet times.

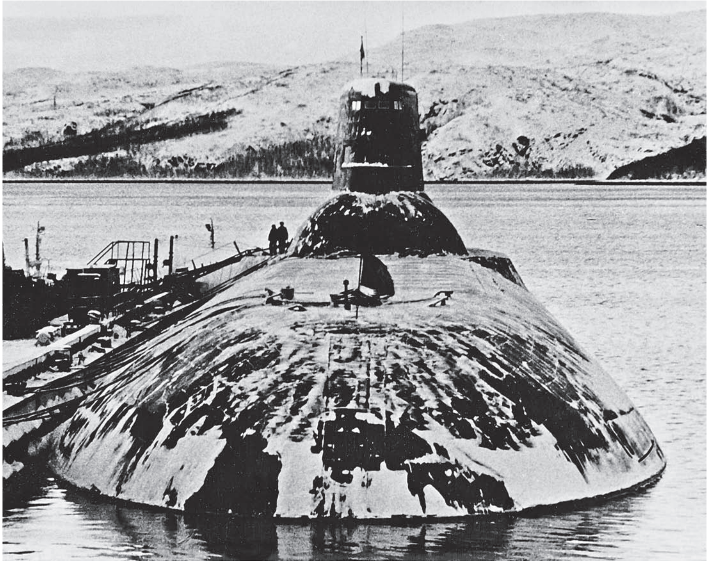


Photo 3.
Nuclear submarine of the Northern Fleet in port on the Kola Peninsula.
Photo: Museum of the Northern Fleet, used with permission.

[18] J YLÄJOKI, 'Koillisväylälle ei uskalleta mennä'. *Karjalainen*, 9 September 2012; T PETTERSEN, 'Slow Start on the Northern Sea Route'. *Barents Observer*, 27 August 2012.

[19] YLÄJOKI 2012.

Nuclear material dumped in the Arctic and Barents Sea remains an environmental threat. All in all, the Soviet Union dumped 17,000 containers of nuclear material, 19 radioactive ships, 14 radioactive reactors, and 735 pieces of heavy, radioactive machinery.[20] Of these, the submerged submarine K-27 poses the biggest single threat to the marine environment.[21] Added to this, the nuclear submarine Yekaterinburg caught fire in the Roslyakovo naval shipyard in late December 2011. According to Russian media sources such as *Kommersant Vlast*, there were nuclear bombs onboard despite local authority and media claims to the contrary.[22]

The focus on the transportation of Arctic oil and gas has prompted environmental organisations to step up their activities in the region too. In late August 2012 Greenpeace conducted an action close to the Novaya Zemlya archipelago in protest against the Prirazlomnaya oil rig development.[23] Environmental groups have been very critical of the capacity to act in the event of an oil spill in the Arctic Sea.[24]

Yet, much will depend on the fate of the Shtokman natural gas fields, which were discovered in 1988 and which have played a significant role in the region's development ever since.[25] It seems, however, that the situation has shifted somewhat. In late August 2012 Gazprom reported that plans for the Shtokman gas development had been suspended in the wake of a fall in the price of natural gas.[26] The decision will impact many local people in the cities and urban districts of the Kola Peninsula[27], who are bitterly disappointed with the renewed plans and promises for jobs, security and a better future that never come to fruition. "Shtokman is only a dream," as one local person put it in a recent media interview.[28]

[20] I KUDRIK, A NIKITIN, N BOHMER, N DIGGES, N THOMAS, M MCGOVERN, and A ZOLOTKOV, 'The Arctic Nuclear Challenge'. *Bellona Report* Volume 3 – 2001. Oslo: Bellona, 2001; I KUDRIK, A NIKITIN, N BOHMER, C DIGGES, V KUZNETSOV, V LARIN, 'The Russian Nuclear Industry'. *Bellona Report* Volume 4 – 2004. Oslo: Bellona, 2004; H KALLIO, 'Painajainen pohjassa'. *Lapin Kansa*, 23 September 2012.

[21] KALLIO 2012.

[22] A AHONEN, 'Arktinen energiavillitys alkoi tympiä', *Helsingin Sanomat*, 3 August 2012.

[23] P PELLI, 'Suomalaisaktivisti sai vesisuihkusta', *Helsingin Sanomat*, 3 September 2012.

[24] R OLIPHANT, 'Gazprom Spill Response Plan Vague'. *The Moscow Times*, 17 August 2012.

[25] It is estimated that the field contains around 3.8 billion cubic metres of natural gas.

[26] 'Suuri kaasuhanke pysähtyy Barentsinmerellä', Helsingin Sanomat, 30 August 2012.

[27] AHONEN 2012.

[28] Ibid.

In the following, I will try to conceptualize the CI in the Murmansk region with the help of a series of maps that illustrate the area accordingly.

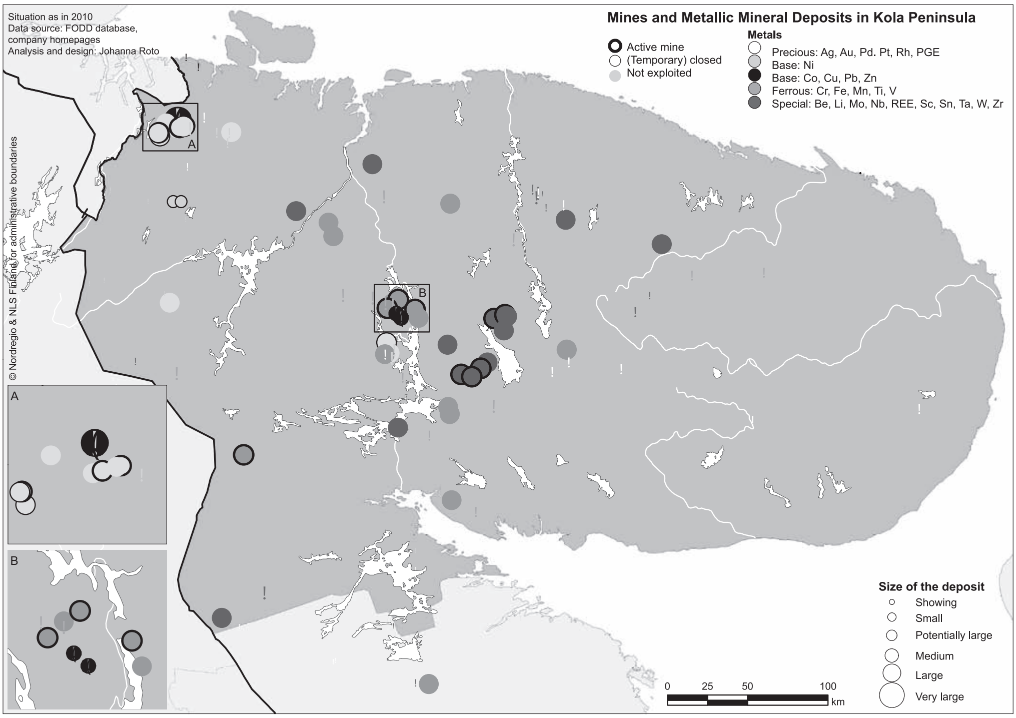
The first map has been compiled from available public sources and provides a view from the governance-security-knowledge complex position. The region is seen as a crucial resource periphery, a "*terra nullius*", or "empty land", to be used for the benefit of the mainstream society, economy and beneficiaries, such as the international and national mining companies.

The second map portrays the historical *siidas* or tribal / indigenous territories and land use and occupancy of several Eastern Sámi communities. The place names of the peoples reflect the oral histories, specific ecological knowledge, and seasonal rounds of the subsistence life in the region prior to the 1900s. As opposed to the governance-security-knowledge complex reading of the same territorial area, this is a region or homeland pulsating with life and intimate connections with the surrounding ecosystems, most of which is encoded in the Sámi *traditional knowledge*, best expressed through the various dialects and three Eastern Sámi languages, Skolt, Kildin and Ter.

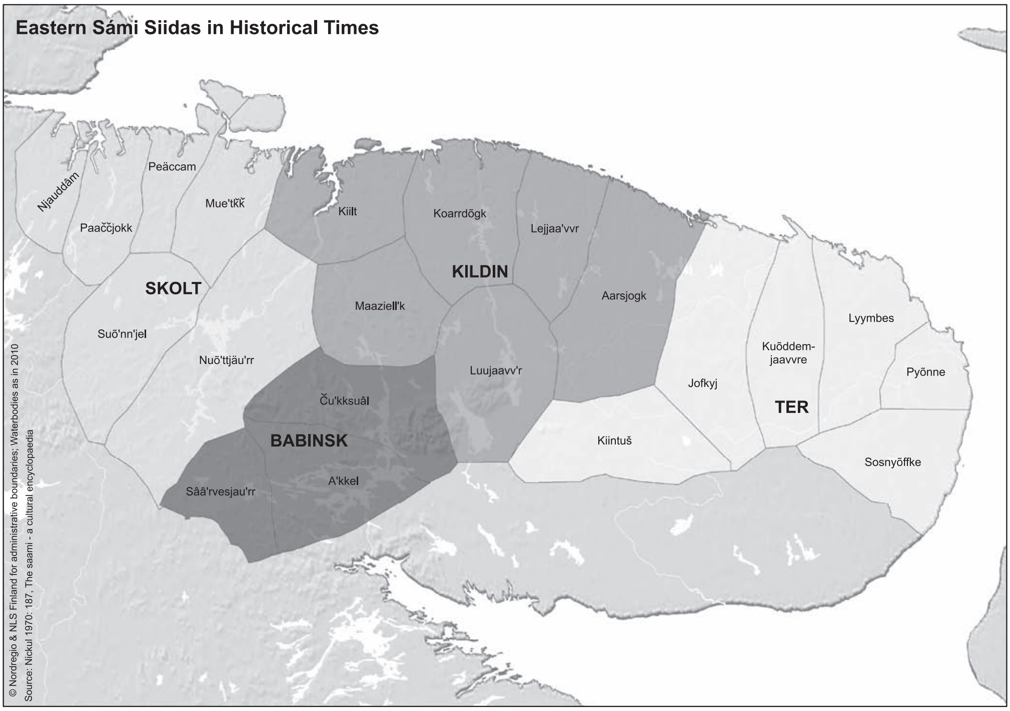
The third map illustrates the contemporary (mid-1990s to 2000s) *land use* of the subsistence economy communities of the Kola Peninsula. Various species and ecosystem features have been identified on the map. Again, this view is in stark contrast to the governance-security-knowledge complex view (Map 1). In fact, the various ecosystems that support the ongoing subsistence economies of the local Sámi and Komi are *in direct conflict* with the imposed state interests and the CI in the region. A question begins to emerge — what is critical infrastructure and how is it portrayed on the land?

Using this cartographical representation of the same region from three different viewpoints, we arrive at an understanding that resilience also means very different things depending on the viewpoint. As outlined in the Preface, the Murmansk region is spot-on in terms of how Mayakovski conceptualized the conquest of time and space in the first modernization of Russia. Imposing railroads, military installations and mining facilities have now emerged in a mere 60–70 years as critical components of "resilience" for the state.

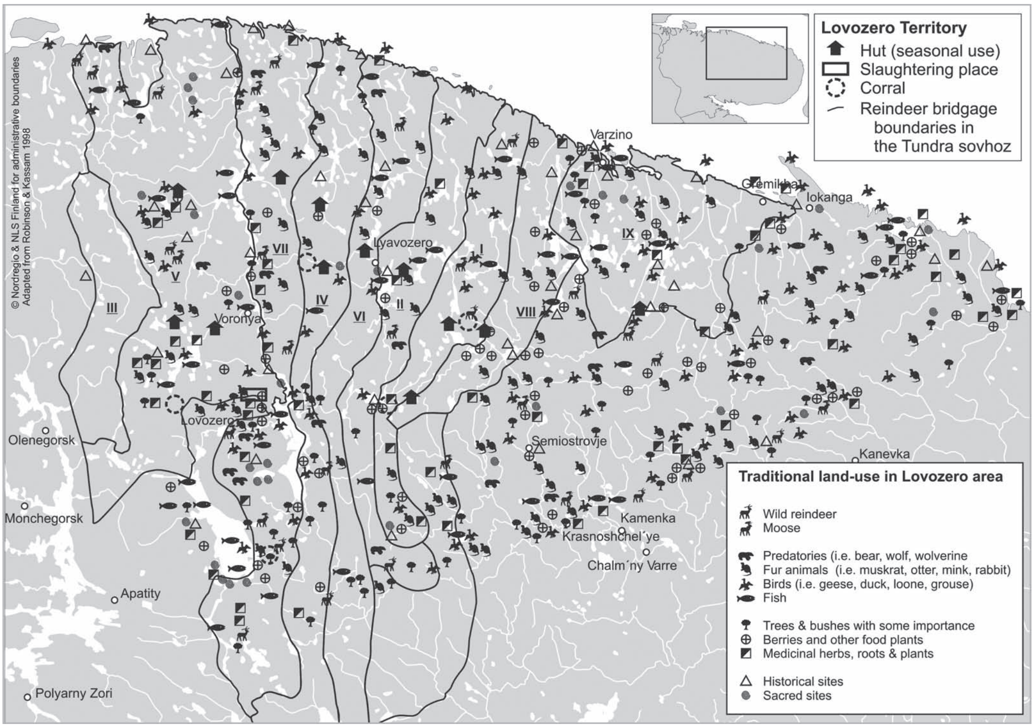
Kola Map 1. Map by Johanna Roto, Nordregio / Snowchange Cooperative, 2011.


Situation as in 2010
Data source: FODD database, company homepages
Analysis and design: Johanna Roto
Mines and Metallic Mineral Deposits in Kola Peninsula
○ Active mine
○ (Temporary) closed
● Not exploited
Metals
○ Precious: Ag, Au, Pd. Pt, Rh, PGE
● Base: Ni
● Base: Co, Cu, Pb, Zn
● Ferrous: Cr, Fe, Mn, Ti, V
● Special: Be, Li, Mo, Nb, REE, Sc, Sn, Ta, W, Zr
A
B
© Nordregio & NLS Finland for administrative boundaries
Size of the deposit
Showing
Small
Potentially large
Medium
Large
Very large
0
25
50
100
km

Kola Map 2. Map by Johanna Roto, Nordregio / Snowchange Cooperative, 2011



Kola Map 3. Map by Johanna Roto, Nordregio / Snowchange Cooperative, 2011.



© Nordregio & NLS Finland for administrative boundaries
Adapted from Robinson & Kassam 1998
Lovozero Territory
Hut (seasonal use)
Slaughtering place
Corral
Reindeer bridgage boundaries in the Tundra sovhoz
Varzino
Gremikha
Iokanga
Lyavozero
Voronya
Lovozero
Olenegorsk
Monchegorsk
Apatity
Polyarny Zori
Semiostrovje
Kamenka
Krasnoshchel´ye
Chalm´ny Varre
Kanevka
I
II
III
IV
V
VI
VII
VIII
IX
Traditional land-use in Lovozero area
Wild reindeer
Moose
Predatories (i.e. bear, wolf, wolverine
Fur animals (i.e. muskrat, otter, mink, rabbit)
Birds (i.e. geese, duck, loone, grouse)
Fish
Trees & bushes with some importance
Berries and other food plants
Medicinal herbs, roots & plants
Historical sites
Sacred sites

However, as the maps demonstrate, resilience for the local indigenous Sámi is founded on diametrically different aspects of how the land is used. How do they conceptualize this process? The documented oral histories of the Sámi themselves may provide an answer, as illustrated in the words of one of the Skolt Sámi leaders and President of the Sámi Council, Pauliina Feodoroff:

> “The first genocide and destruction against the Sámi peoples and our society began in the 1500s and 1600s. Unless there are dramatic changes in the near future, the Sámi culture will die, disappear in my lifetime […] Sámi knowledge is knowledge about how to co-exist with your environment, how to have your relationships with humans and with the world. Therefore the most effective ways to control a people are to destroy the things that reality consists of for that people. In the North this ancient knowledge has been beaten and destroyed for centuries in order that the indigenous peoples would forget this knowledge. If nothing else can be done, we can at least try to prolong things. To play for more time to survive. We can try to gather indigenous knowledge from the old people who possess it. We can try to create safe havens of ecosystems which

> contain our knowledge — the fells, forests, and lakes which remain in pristine condition."[29]

Analysing the essence of what Feodoroff says, the Sámi identify healthy, functioning ecosystems as key sources of their resilience, the last of which are being threatened by the contemporary imposition of natural resource extractions. Importantly, she makes the case that the specific ecosystems are not just locations of subsistence and food security sources — they are indeed the "sources of knowledge" of resilience — identifying the link between the landscape, traditional knowledge and indigenous cultures. This further advances the notion that CI and resource development not only have a direct impact on other types of resilience and ecosystems — they also have social, cultural and spiritual dimensions that can be damaged. Such a realisation expands the definition and understanding of resilience into a substantively wider spectrum.

THE NIZHNIKOLYMA REGION IN THE ARCTIC ZONE — CRITICAL INFRASTRUCTURE NON-EXISTENT

Nizhnikolyma (Lower Kolyma) lies in the Russian Arctic in the far North-east of the Sakha Republic.[30] Splintered by the great Kolyma River and its tributaries, it covers 87,100 square kilometres, with a population of only some 5,600 people. Most roads in the area are made of ice and thus exist only in winter. Most supplies are transported to remote communities by river and air.[31] In 2012, as a part of the initiative to deploy troops to the Arctic and enhance the infrastructure in the region, the airport in the regional capital Cherskyi was rebuilt and attached to the network of "Airports of the North".

Outside the main settlements, the region comprises tundra and woodland, and is home to an abundance of wildlife. There are several regional and national nature conservation initiatives, including

[29] In MUSTONEN and MUSTONEN 2011, p. 14.

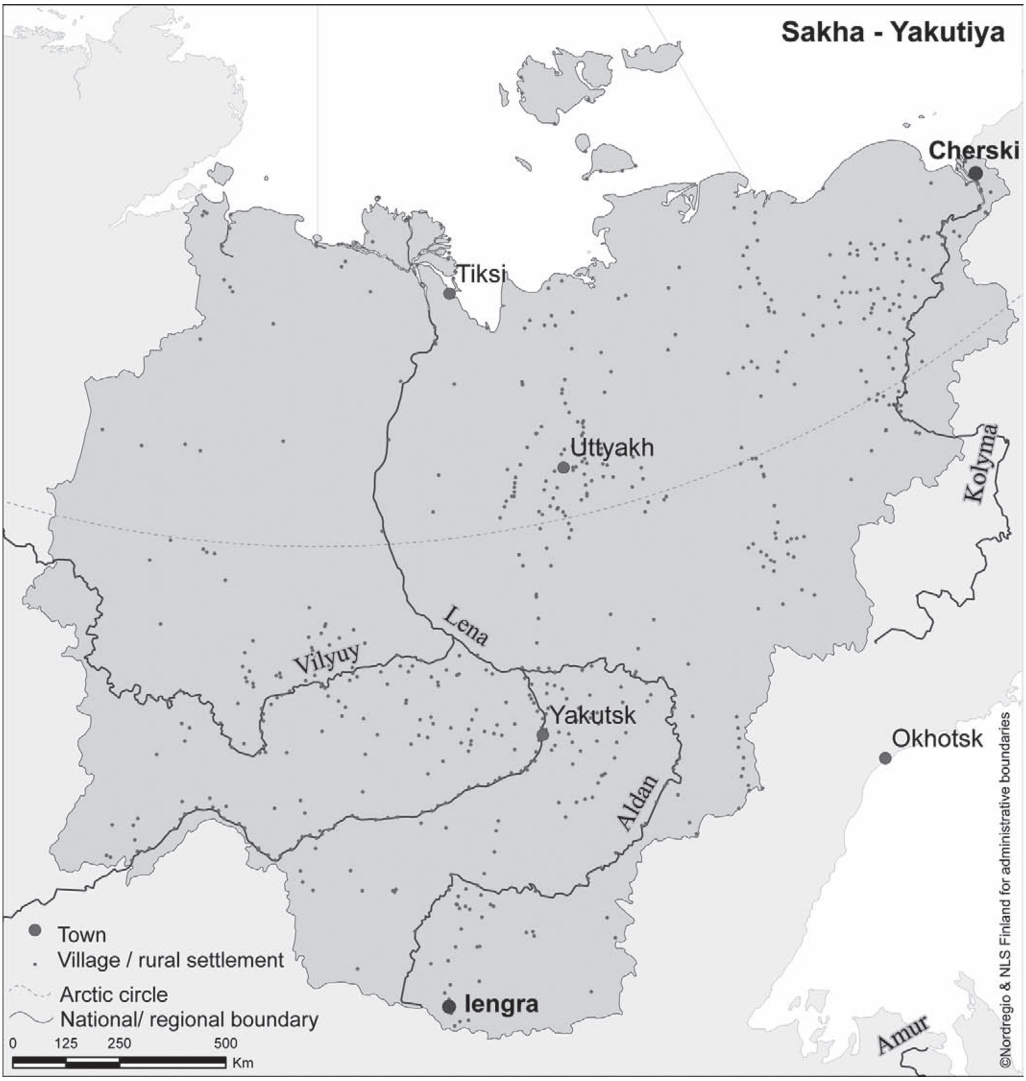
[30] The Republic of Sakha-Yakutia is the largest territory of the Russian Federation, with a total land mass of 3.1 million square kilometres. 40 per cent of this land mass is north of the Arctic Circle. Continental Sakha-Yakutia is a zone of continental permafrost, with an average depth of 300–400 metres, but which reaches depths of 1,500 metres in places. In terms of energy resources, 330 million tons of oil and 2.4 trillion cubic metres of natural gas exist in the region (Jakutija 2012: 29).

[31] MUSTONEN 2009.

protected areas and the ECORA process, a UNEP-initiated and funded project to conserve the habitats in the Russian Arctic that are still in prime condition.

The region is also home to many different indigenous peoples, including the Dolgan, Evenki, Even, Yukagir, Chukchi, and Nenets. Nomadic reindeer herding is a traditional way of life in Nizhnikolyma and, along with hunting and fishing, the main traditional occupations of the area. Weather plays a crucial role in daily life, as do landscape features and conditions. The impacts of climate change are therefore crucial.

Map 4. Fieldwork locations in Republic of Sakha-Yakutia. Map by Johanna Roto, Nordregio / Snowchange Cooperative, 2011.



The indigenous peoples are integral to the Arctic, as together with the Nenets and Even, the Kolyma communities have preserved *nomadic reindeer herding*. The relationship that the local indigenous peoples have with their territory is best expressed by one of the herders in the Turvaurgin community:

> "The tundra is our life. We live there. We are so accustomed to life in the tundra that we do not know any other kind of life. It is our homeland, place of birth. I cannot explain it, I do not have words for it. I know the tundra is our life. Especially in the summertime. Those who have lived all of their lives in the tundra cannot go to the taiga in the summer. In the summer, together with our families, we migrate (with the reindeer) to the coast of the Arctic Sea. In close proximity to the sea. That is our natural habitat."[32]

There are currently two reindeer herding *obshchinas* in the region. The Nutendli *obshchina* was established in the early 1990s in the north-eastern corner of the Lower Kolyma Delta. Nutendli has a nomadic school and one nomadic reindeer herding brigade at present.[33]

The Turvaurgin *obshchina* is organized primarily as an economic unit of indigenous nomadic reindeer herders.[34] It was founded in the early 1990s to replace the Soviet-era *kolhoz* state farm of the same name. Its base is the village of Kolymskaya. Most of the herders in the community are Chukchi and Yukagir. The lands used today by Turvaurgin start along the Kolyma River close to the village of Kolymskaya and extend to the Arctic Ocean some 350 kilometres to the north, where the brigades spend spring and summer with their herds.[35]

Permafrost changes in the Lower Kolyma area are identified by the communities as the most significant of the climate- and weather-related changes in the region. Both Turvaurgin and Nutendli herders have witnessed a rapid process of collapsing riverbanks, disappearing fishing lakes and increasing erosion along the Kolyma River. The thawing of continuous permafrost started in the mid-1990s

[32] MUSTONEN 2009, p. 221.

[33] The community consists mainly of the relatives of Grandmother Akulina Kemlil and Grandfather Yegor Nutendli, who are the Chukchi elders of Nutendli (Mustonen 2009). Akulina passed away in summer 2012.

[34] MUSTONEN 2009.

[35] Ibid.

according to the Nutendli herders, but it has accelerated during the 2000s. Riverbanks, such as those on the Philipovka River, which is along the Nutendli seasonal round, are collapsing. Herders report that the thawing is changing the annual water cycles and affects floods and accessibility to fishing lakes and water sources for the reindeer. The disastrous Andreyuskino flood in 2007, the worst in the recorded history of the community, is attributed to this phenomenon by local residents.[36]

Photo 4. Melting permafrost along the coast of the East Siberia Sea, August 2012. Photo: Tero Mustonen

The region is planned to be along the Northern Sea Route. Several ships already use the Kolyma River to transport oil and other resources to the settlements upstream. Now the plans include using Cherskii port as a supply and stopover destination along the NSR.

The Nizhnikolyma region and its inhabitants constitute a very unique region in the world where the state governance-security-knowledge complex has never overtaken their way of life, and since the collapse of the Soviet Union, the local indigenous subsistence communities have had the time, space and

[36] Ibid.

possibility to return to their own ways of living as the state withdrew in 1991. However, here too the results of climate change have started to influence life on the land in the context of melting permafrost. This process also has potentially global significance, as the permafrost contains methane that will be released into the atmosphere as the feedback loop proceeds, thereby accelerating global warming.

Secondly, due to the increased shipping and state military presence, the CI impacts may soon start to limit the capacity and autonomic status of the indigenous societies in the region. At present, however, the impact is still one of emergence.

Photo 5.
Cherskii harbour.
Photo: Tero
Mustonen

SOUTHERN SAKHA — CRITICAL INFRASTRUCTURE AS A THREAT

In Southern Sakha the situation is very different from the Arctic zone of Nizhnikolyma. The Republic of Sakha-Yakutia, together with several national enterprises, including the Transneft Company, has employed far-reaching plans to extract the region's natural resources.

Photo 6.
Coal mine in Neriungri.
Photo: Saija Lehtonen

Some of these developments include the planned Lensk Oil Refinery with a capacity of 500,000 tonnes, the East Siberia-Pacific Ocean Pipeline, several hydropower stations along the local rivers, increased mining for coal and uranium amongst other metals, and the completion of the Berkakit-Tommot-Yakutsk railway.

The Neriungri region is located in the Siberian taiga, or boreal zone. It is also home to the Evenk indigenous people in the community of Iengra. Since coal deposits were discovered in their traditional territories, they were collected, or forcefully re-located to the community. However, the Evenk have tried to preserve their culture, reindeer herding and subsistence economies in the midst of these changes. Local place names are encoded with ecological and spiritual knowledge, which guides the Evenk in their lives in the taiga. Or, as they say themselves:

> "We know where to travel (in the taiga). We are always moving. We know every path. We know every tree."[37]

[37] Ibid, p. 87.

Photo 7. Reindeer are still the traditional means of transportation in the Evenk taiga. Photo: Tero Mustonen

Of all the northern Russian locations, the impact of CI is possibly most pronounced in the Neriungri region today. In Murmansk, the harvesting and exploitation of mineral deposits started back in the early 1900s. In Kolyma, climate change can be identified as one of the few intrusions that have resulted from industrial development. But in the Neriungri region the process is unfolding *right now*, with the biophysical and social impacts becoming more pronounced every year.[38]

It is here too that the underlying severed, mangled relationship with nature that the technological society has in Russia today is most visible. What the state proclaims as security assets (natural gas, oil and mining territories) are in a continuous state of *expanding* into the territories of the Evenk in the taiga. Several fishing rivers have been devastated by gold mining, the railway has cut reindeer pastures in half, and despite the attempts by state officials to deny this information, the East Siberia–Pacific Ocean Pipeline has already leaked into the taiga, a stark reminder of the oil pipe spill in the Komi Republic in the 1990s.

[38] Ibid.

A respected spiritual leader of the local Evenk, Elder Matryona Kulbertinova, stated in the 1990s that:

> “Some people say that the Soviet power gave us everything. It taught us how to live, what to do and how to do things. The wisest and most important of the Russians told us: ‘we gave you everything: food, clothes, a good life.’ I think they forgot the most important of all, the spirit of a human being. The human being was ruined and has become evil. In taiga I am more afraid of humans than animals. Look, they have turned the whole taiga upside down. There is no room for us or the reindeer. That most important human says that life has to be organised, just like in a kindergarten. Everybody has to have the same kind of house, the same food. Thus believes the person who wishes to organise our lives. I think he is probably wrong. If life transforms into this, it becomes frightening.”[39]

The consequences of the rapid exploitation of waters, land and utilities in the Neriungri region have had a tremendous impact on the Evenk. As early as the 1970s, when the Baikal-Amur Magistrate railway (BAM) was being constructed, several reindeer herders ended their own lives because they could not adapt to the changes imposed on them. This trend is continuing and spreading.

CONCLUSIONS

This article has reviewed the notion of critical infrastructure and its manifestations in two regions of the Russian Arctic. If we view the CI concept more critically, we can establish that it is rooted in the governance-security-knowledge complex of a modern state. Its relationship with nature is built on subjugation (the unlimited harvesting of natural resources) and *fear* (of uncontrollable weather, ecosystem collapse, and unpredictable, costly natural hazards).

Juxtaposed with this reading of nature and reality are the surviving and ongoing, re-emerging communities of the indigenous people of the Russian Arctic. By reviewing their oral histories and documented land use, which is still present today, we can establish that the *traditional knowledge* of these rooted communities provides

[39] Ibid., p. 102.

a crucial alternative and sustainable frame for a dialogue with the state governance-security-knowledge complex. The indigenous communities embrace knowledge about nature in their little-known practices, traditions, memories and oral histories that the technological society has forgotten.

I have explored, using the results from field visits, land use maps and visual documentation, three cases on the Northern Russian peripheries in the context of a re-reading of critical infrastructure and how it manifests locally.

Photo 8.
Abandoned ships in the Kola Fjord.
Photo: Marko Kulmala

In the context of the Murmansk region, the existing and planned CI initiatives, if understood as a mix of private and state governance-security-knowledge complexes, threaten the very existence of the indigenous peoples and natural habitats, both on-shore and off-shore. The most pronounced of these threats include the nuclear legacy of the Soviet Union and the ongoing plans for the expansion of mining operations on the Kola Peninsula.

In the Arctic zone of Nizhnikolyma, both the indigenous societies and the ecosystems are relatively stable and healthy. However, the increased shipping along the Northern Sea Route and the impacts of the melting permafrost as an existing consequence of Arctic climate change qualify the region as potentially relevant to the global discussion on climate change.

In the southern part of the Republic of Sakha-Yakutia, both the taiga ecosystems and the indigenous Evenk are in retreat following the tremendous, renewed assault from the state and enterprises on multiple fronts, in the name of 'securing' the crucial assets of the land for the 'benefit' of the society. Mining, railways and hydropower have caused, among other things, the social and economic destruction of the Evenk reindeer herding culture.

The oral history materials collected from the case regions emphasize the need to assess past damage and the current urgent situation of traditional economies, and provide a crucial reflective mirror for mainstream society as it tries to find ways of adapting to the multiple "risks" and challenges caused by global and climate change.

The survival of the indigenous communities is crucial in these times of change. In addition to constituting a sustainable reserve and a source of food security in the regions (for example in the form of reindeer husbandry and fisheries), if allowed to function as they should, these human societies can contribute significantly to our understanding of *what* changes in nature and perhaps more importantly, *what it means*. There is inherent value in the survival of these ecosystems and diverse human societies even today. The knowledge of the indigenous peoples can provide us with crucial lessons and a re-reading of what critical infrastructure means from the ground up, based on their long memory, traditional knowledge and unique experience.

5

5. Conclusions and policy recommendations

Katri Pynnöniemi

The Russian policies on critical infrastructure protection (CIP) are evolving against a background composed of an uneasy combination of factors: the degeneration of infrastructures critical for the country's economic and social development, and the de-legitimization of political institutions responsible for protecting 'population' and 'territory'. Taking this as our general starting point, the three separate case studies presented in this report have tried to explicate the situational and conceptual factors that have influenced the evolution of the Russian policy on critical infrastructure protection, as well as the political implications of potential natural or technological catastrophes for the current political regime. We have focused in particular on three issues. Firstly, on the evolution of the Russian policy towards critical infrastructures, and how these infrastructures are defined in the first place. Secondly, on an analysis of the forest fires in 2010 from the viewpoint of Russia's state capacity, and thirdly, on assessing the multiple challenges Russia faces in the Arctic region. In this concluding section we will briefly outline the main findings of the research project and also suggest some ideas for further research.

The Russian policy on critical infrastructure protection was outlined in the early 2000s and has been consolidated in recent years as a part of the national security strategy. It is built upon the civil defence system of the Soviet era, a system that has been modernized under the auspices of the Ministry of Emergency Situations of Russia. It has been argued throughout the report that even if the policy framework in Russia is considerably different from that in the US and Europe, a comparative perspective may help to avoid certain pitfalls in understanding this difference. In the case of CIP, the Russian policies seem to fit within the general framework of CIP policies conducted in Europe or in the US. This relates in particular to the consolidation of the CIP policies as a response to multiple threats against 'our way of life' and the placing of risk at the centre of the policy.

What sets Russia's CIP policy apart is the general political framework against which it is evolving. To explain this difference, we employ a hybrid regime concept that is used here as an umbrella term for those regimes that could neither be described as democratic nor as authoritarian. The main source of legitimacy of Russia's hybrid regime has been its ability to improve the economic well-being of citizens and to present changes made to the state governance structure at the beginning of the 2000s as an advancement of 'order and stability' in Russia. Since the beginning of President Putin's third presidency in 2012, the frictions and flaws of the current political system have become more pronounced in the Russian domestic discussion, with little or no real political consequences in evidence, at least at the moment.

The key points of vulnerability/strength of the political regime and its capacity to respond to major catastrophes and threats to critical infrastructures are interlinked and can be summarized as the responsibility of the political leadership (legitimacy), the management of information (reliability of information and monitoring practices), and the political culture in general (regulation practices and systemic corruption). As the analysis of forest fires in 2010 shows, the 'power vertical' in Russia has, in fact, undermined the key variables of state capacity: 'manual control' overrides the division of power between the regional and federal authorities, which, in turn, has a negative influence on the response to (and prevention of) of major disasters, ultimately undermining the legitimacy of the regime itself. In this way, the forest fires in 2010, or the flood catastrophe in Krymsk in the Krasnodar region in July 2012, are not just natural catastrophes but have become examples of *political events* that offer a point of reference for the current regime's failure to uphold its promises of 'order and stability'.

It is, however, important to look beyond our immediate concerns and include in this discussion a variable with global implications. Global climate change and the extraction of natural resources in the Arctic region are regarded as both a challenge and an opportunity for Russia. In Russian and European discussions, the Northern Sea Route is usually viewed in terms of opportunity, as it will form one of the major corridors of the global commercial flows. The extraction of oil and gas reserves in the Arctic is a long-term project that has intensified in recent years, although the pace of development has slowed down of late. However, it is generally acknowledged that the 'opening of the new northern frontier' is anything but simple. Climate change, and the possible melting of the Russian permafrost resulting from it, pose a real challenge that adds an entirely new dimension to the notion of 'critical infrastructures'.

In this report we have explored the 'mindset' of Russia's policy on critical infrastructure and we hope that this discussion will contribute to further discussion on this important topic. An issue that should be studied in detail in future relates to changes in the conceptualization of new threats, such as vulnerabilities related to the penetration of IC technologies into new areas of life and emerging interdependencies in the sphere of critical infrastructures and between countries. On the basis of the current analysis, we observe that there is a certain difference between Russian policy and the US and EU formulations concerning the acknowledgement of vulnerabilities related to interconnectivity. The Russian policies do not seem to take this as a starting point for policy-planning but, for the moment at least, focus instead on 'traditional' physical threats and terrorism against critical infrastructures.

In terms of policy options and the future planning of critical infrastructure policies, we can therefore issue a number of recommendations as policy-relevant options based on the materials presented here.

- Cooperation in the sphere of complex human security should be intensified at all levels of state administration as well as between civil societies in Russia and the European states.
- Threats to CI as well as disasters of any kind are localized on particular territory, affecting a particular region or regions. Therefore the role of regional authorities and local communities is obviously crucial. However, under the status quo in Russia they lack the incentives to actively engage in disaster management, shifting responsibility to the federal executive. Thus, when dealing with Russia, the existing degree of centralization and the unpreparedness of regional and local communities should be taken into consideration. At the same time, decentralization should be observed as one of the key points in the (possible) modernization agenda of the country.

- The states operating in the Arctic should work in close cooperation with scientists and the indigenous peoples to identify territories of traditional nature use and protection that would be zoned away from industrial land use. Such stable ecosystems will also act as carbon sinks and other climate-mitigating systems if allowed to function properly. Indigenous representatives from the local communities should be allowed to participate as equal partners in the land use decisions of a region to prevent further damage in the future.
- Past problems and impacts of CI development in the North, such as the Soviet nuclear legacy, should be dealt with through international cooperation.

Bibliography

PRIMARY DOCUMENTS

Arctic Council 2005. Arctic Climate Impact Assessment, 2005. Available at http://www.acia.uaf.edu. Accessed 5 October 2012.

Arctic Council 2009. Arctic Marine Transport Assessment, 2009. Available at http://arcticportal.org/uploads/4v/cb/4vcbFSnnKFT8AB5lXZ9_TQ/AMSA2009Report.pdf. Accessed 9 September 2012.

Arctic Council 2013. Arctic Biodiversity Assessment, 2013. Forthcoming.

Council Directive 2008/114/EC, On the Identification and Designation of European critical Infrastructures and the Assessment of the Need to Improve their Protection, *Official Journal of the European Union*, 23 December 2008, L 345/75–L 345/82.

Concept of National Security of the RF, approved by Presidential decree no. 24, 10 January 2000.

Concept of National Security of the RF, approved by Presidential decree no. 130, 17 December 1997.

Edinaya mezhvedomstvennaya informatsionno-statisticheskaya sistema, informatsiya o chrezvychainyh situatsiyah. Accessed 23 October, 2012, http://www.fedstat.ru/indicator/data.do?id=41317&referrerType=0&referrerId=947198.

EMERCOM, R*eport on implementation of the tasks in 1992–1993*. Accessed 27 May 2012, http://www.mchs.gov.ru/eng/ministry/?SECTION_ID=591.

EMERCOM, Metodicheskie rekomendatsii po provedeniyu inventarizatsii kriticheski vazhnyh i potentchial'no opasnyh ob'ektov RF i formirovaniyu oerecheniya kriticheski vazhnyh ob'ektov na regional'nom urovne. Administrative order no. 2-4-60-10-14, 19 June 2008.

EMERCOM, 'National Crisis Management Center'. Accessed 14 November 2012, http://www.mchs.gov.ru/eng/powers/?SECTION_ID=609.

EMERCOM, Otchet ob itogah realizatsii federalnoi tselevoi programmy " Snizhenie riskov i smyagchenie posledstvii chrezvychainyh situatsii prirodnogo i tehnogennogo haraktera v RF do 2010 goda. Accessed 15 October 2012, http://www.mchs.gov.ru/upload/FCPRiski2010.doc.

EMERCOM, Prognoz chrezvychainoi obstanovki na territorii RF na 2012 god, Tsentr "Antistihiya", Moskva 2011. Accessed 15 November 2012, http://www.mchs.gov.ru/forecasts/detail.php?ID=701495.

EMERCOM, *Report on implementation of the tasks in 2005–2006*. Accessed 27 May 2012, http://www.mchs.gov.ru/ministry/index.php?SECTION_ID=298.

Federalnyi Zakon, O zashchite naseleniya i territorii ot chrezvychainyh situatsii prirodnogo i tehnogennogo haratera, no 68-FZ, 21 December 1994.

GOLDAMMER, J., 'Preliminary Assessment of the Fire Situation in Western Russia', The Global Fire Monitoring Center, 15 August 2010. Accessed 3 November 2012, http://www.fire.uni-freiburg.de/intro/about4_2010-Dateien/GFMC-RUS-State-DUMA-18-September-2010-Fire-Report.pdf.

Greenpeace, 'Press-reliz: Pozharnaya Katastrofa v Lesah Rossii Neizbezhno Povtoritsya, esli Polnotsennaya Sistema Gosudarstvennogo Upravleniya Lesami ne Budet Vosstanovlena', 26 August, 2010. Accessed 5 November, 2012, http://www.greenpeace.org/russia/ru/press/releases/4929433/;

The National Strategy for Physical Protection of Critical Infrastructures and Key Assets, The White House, February 2003. Emphasis added. http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

'Osnovy gosudarstvennoi politiki v oblasti obespecheniya yadernoi i radiatsionnoi bezopasnosti RF na period do 2010 goda i dal'neishuyu perspektivu'. *Rossiiskaya Gazeta*, 7 April 2004.

Pravitelstva RF, Kontseptsiya federal'noi sistemy monitoring kriticheski vazhnyh ob'ektov i/ili potentsial'no opasnyh ob'ektov infrastruktury RF i opasnyh gruzov. Rasporyazheniem no. 1314–p, 27 August 2005.

Pravitelstvo RF, Kontseptsiya federalnoi tselevoi programmy 'snizhenie riskov i smyagchenie posledstvii chrevytsainyh situatsii prirodnogo i tenogennogo kharaktera v RF do 2015 goda. Rasporyazhenie no. 534–p, 29 March 2011.

Pravitelstvo RF, O Federal'noi tselevoi programme snizhenie riskov i smyatsenie posledstvii tsrezvytsainyh situachii prirodnogo i tehnogennogo haraktera v Rossiiskoi Federatsii do 2010 goda. Postanovlenie no. 1, 6 January, 2006.

Pravitelstvo RF, O klassifikatsii chrezvychainyh situatsii prirodnogo i tehnogennogo haratera. Postanovlenie no. 1094, 13 September 1996.

Pravitelstvo RF, O klassifikatsii chrezvychainyh situatsii prirodnogo i tehnogennogo haratera. Postanovlenie no. 304, 21 May 2007.

Pravitelstvo RF, O federal'noi tselevoi programme "Snizhenie riskov i smyagchenie posledstvii chrezvychainyh situatsii prirodnogo i tehnogennogo haraktera v RF do 2015 goda. Postanovlenie no. 555, 7 July 2011.

Pravitelstvo RF, O federalnoi tselevoi programme "Snizhenie riskov i smyagchenie posledstvii chrezvytsainyh situatsii prirodnogo i tehnogennogo kharaktera v RF do 2005 goda. Postanovlenie no. 1098, 29 September 1999.

Prezident RF, Osnovy gosudarstvennoi politiki v oblasti obespecheniya khimicheskoi i biologicheskoi bezopasnosti RF na period do 2010 goda i dal'neishuyu perspektivu. Ukaz no. Pr–2194, 4 December 2003.

Prezident RF, Osnovy gosudarstvennoi politiki v oblasti obespecheniya bezopasnosti naseleniya RF i zashchshchennosti kriticheski vazhnyh i potenchial'no opasnyh objektov ot ugroz tehnogennogo, prirodnogo kharaktera i terroristicheskih aktov. Ust. Pr–1649, 28 September 2006.

President RF, Osnovy gosudarstvennoi politiki v oblasti obespecheniya besopasnosti naseleniya RF i zashchishchennosti kriticheski vazhnyh i potentsialno opasnyh ob'ektov ot ugroz prirodnogo, tehnogennogo kharakteri i terroristicheskih Aktov na Period do 2020 goda. Utv. no. Pr–3400, 15 November 2011.

President RF, O sozdanii kompleksnoi sistemy obespecheniya bezopasnosti naseleniya na transporte, Ukaz, 31 March 2010. Accessed 12 May 2012, http://news.kremlin.ru/news/7295/print.

'Predsedatel' pravitels'tva RF V.V. Putin provel soveshchanie po ukrepleniyu materialno-tehnicheskoi bazy MCHS', 12 November 2010. Accessed 15 November 2012, http://government.ru/docs/12895/.

PUTIN V., Annual Address to the Federal Assembly of the Russian Federation, The Kremlin, 25 April 2005. Accessed 13 October 2012, http://archive.kremlin.ru/eng/speeches/2005/04/25/2031_type70029type82912_87086.shtml

PUTIN V., 'Vstupitel'noe slovo na sovmestnom zasedanii Soveta Bezopasnosti i preziduma Gosudarsvennogo soveta po voprosu o povyshenii zashchity kriticheski vazhnyh dlya natsional'noi bezopasnosti ob'ektov infrastruktury i naseleniya strany v usloviyah obostreniya ugroz prirodnogo, tehnogennogo, i terroristicheskogo haraktera'. 13 November 2003, Moskva, Kreml. Accessed 15 May 2012, http://archive.kremlin.ru/text/appears/2003/11/55532.shtml.

Russia's National Security Strategy, approved by Presidential decree no. 537, 12 May 2009.

'Zaklyuchenie Obshchestvennoi Komissii po Rassledovaniyu Prichin i Posledstvii Prirodnyh Pozharov v Rossii v 2010 godu', 14 August, 2010, Yabloko Party. Accessed 3 November 2012, http://www.yabloko.ru/mneniya_i_publikatsii/2010/09/14.

BOOKS

AALTO, P. (ed), *Russia's Energy Policies: National, Interregional, and Global Levels*, Edward Elgar Publishing Ltd., Cheltenham, 2012.

BECK, U., *World at Risk*, Malden: Polity Press 1999.

Building Community Disaster Resilience Through Private–Public Collaboration. The National Academies Press, Washington D.C., 2011.

BESLEY, T. AND PERSSON, T., *Pillars of Prosperity: The Political Economics of Development Clusters*. Princeton University Press, Princeton, 2011.

CASTELLS, M., *The Information Age. Economy, Society and Culture. Vol I The Rise of the Network Society*, Blackwell Publisher, Oxford.

Disaster Resilience: A National Imperative. The National Academies Press, Washington, D.C., 2012.

EBERT, D., *The Age of Catastrophe: Disaster and Humanity in Modern Times*, North Carolina: McFarland and Company Inc, 2012.

GORMAN, S.P., *Networks, Security and Complexity: The Role of Public Policy in Critical Infrastructure Protection*, Edward Elgar, Cheltenham, 2005, pp. 2–4.

HARTE T., *Fast Forward: The Aesthetics and Ideology of Speed in Russian Avant-Garde Culture, 1910–1930*, University of Wisconsin Press, Wisconsin, p.3.

HEDLUND, S., *Russian Path Dependence*, Routledge, London and New York, 2005

HILL, F. AND G. CLIFFORD, *The Siberian Curse. How Communist Planners Left Russia Out in the Cold*, Brookings Institution Press, Washington, 2003.

MASSA, I., 'Yhteiskuntatieteellisen ympäristötutkimuksen paradigmat ja keskeisimmät suuntaukset', teoksessa *Vihreä Teoria: Ympäristö Yhteiskuntateorioissa*, I Massa (ed), Gaudeamus, Helsinki, 2009, s. 28.

MEDVEDEV, S., 'Post-Soviet Developments: A Regional Interpretation (A Methodological View), in *Post-Soviet Puzzles. Mapping the Political Economy of the Former Soviet Union*, vol. II, Nomos Verlagsgesellschaft, Baden-Baden, p. 5.

MUSTONEN, T., *Karhun väen ajast aikojen avartuva avara*. Joensuu: University of Joensuu Press, 2009.

MUSTONEN, T. and K. MUSTONEN, *Eastern Sámi Atlas*. Kontiolahti: Snowchange Cooperative, 2011.

OPITZV, S., 'Government Unlimited. The Security dispositif of illiberal governmentality', In *Governmentality. Current Issues and Future Challenges*, U BRÖCKLING, S KRASMANN and T LEMKE, Routledge, New York, 2011.

PYNNÖNIEMI, K., *New Road, New Life, New Russia: International transport corridors at the conjunction of geography and politics in Russia*, Acta Universitatis Tamperensis, Tampere, 2008.

ROBBEK, V., *Scientific Basis of Education System Formation of Nomadic Peoples of the North*, Nauka, Novosibirsk, 2007.

ROSE, N., *Powers of Freedom: Reframing Political Thought*, Cambridge University Press, Cambridge, 1999, p. 3.

SAKWA, R., *The Crisis of Russian Democracy. The Dual State, Factionalism and the Medvedev Succession*. Cambridge, Cambridge University Press.

SEARLE, J., *The Construction of social reality*. Penguin Books, London, 2005.

SLEZKINE, Y., *Arctic Mirrors — Russia and the Small Peoples of the North*. Cornell University Press, 1994.

SHOIGU, S., *Atlas prikhodnykh I tekhnologennykh opasnostei i riskov chrezvychainykh situatsii, Rossiiskaia Federatsiia, Privolzhskii federalnyi okrug* (Atlas of the Natural and Technological Hazards and Risks of Emergencies in Volga Federal Okrug of the Russian Federation). Moscow: Dizain informatsiia, 2008.

RISLAKKI J., *Paha sektori. Atomipommi, kylmä sota ja Suomi.* Juva, WSOY, 2010, p. 61.

PERROW, C., *Normal Accidents: Living with High-Risk Technologies.* Princeton University Press, Princeton 1999.

VLADIMIROVA, V., *Just Labor — Labor Ethic in a Post-Soviet Reindeer Herding Community*. Uppsala: Acta Universitatis Upsaliensis, 2006.

WISNER, B., *Natural Hazards, People's Vulnerability and Disasters*. London: Taylor & Francis, 2003.

YANITSKY, O., 'Sustainability and risk. The case of Russia', in *Russian Environmentalism. The Yanitsky Reader*, Taus, Moscow, 2010, p. 61.

ÅSLUND, A. and A. KUCHINS, *The Russian Balance Sheet,* Peterson Institute for International Economics and Center for Strategic and International Studies, Washington, DC, April 2009.

ARTICLES

AITKEN, P. and LEGGAT, P., Considerations in Mass Casualty and Disaster Management. In: *Emergency Medicine — An International Perspective.* Ed. by Michael Blaivas. InTech, 2012.

ALEXANYAN, K., BARASH, V., ETLING, B., FARIS, R., GASSER, U., KELLY, J., PALFREY, J.G. and ROBERTS, H., Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere (March 2, 2012). Berkman Center Research Publication No. 2012-2. Available at SSRN: http://ssrn.com/abstract=2014998

ARNOLD, J.L., LEVINE, B.N., MANMATHA, R., LEE, F., SHENOY, P., TSAI, M.C., IBRAHIM, T.K., O'BRIEN, D.J. & WALSH, D.A. (2004). Information sharing in out-of-hospital disaster response: The future role of information technology. Prehospital and Disaster Medicine, vol. 19, no. 2, pp. 201–7.

BARASH, V. and KELLY, J., 'Salience vs. Commitment: Dynamics of Political Hashtags in Russian Twitter', Berkman Center Research Publication, no. 2012–9, April 4, 2012, Available at SSRN: http://ssrn.com/abstract=2034506

BERTRAND, E., 'Constructing Russian Power by Communicating During Disasters The Forest Fires of 2010', *Problems of Post-Communism*. Volume 59, Number 3, 2012, pp. 31–40.

BRAHAM, M., AGHABABIAN, R., ANDREWS, R.A., AUSTIN, C., BROWN, R., YAO-ZHONG, C., ENGINDENIZ, Z., GIROUARD, R., LEAMAN, P., MASELLIS, M., NAKAYAMA, S., POLENTSOV, Y.O. & SUSERUD, B.O., 5th Asia-Pacific conference on disaster medicine. Theme 7. Sharing international experiences in disasters: Summary and action plan. Prehospital and Disaster Medicine, vol. 16, no. 1, 2001, pp. 42–5.

BRASSET, J., N. VAUGHAN-WILLIAMS, 'Governing Traumatic Events', *Alternatives: Global, Local, Political*, vol. 37, no. 3, p.183.

BRIGGS, C. M., 'Climate Security, Risk Assessment and Military Planning', *International Affairs*, vol. 88, no. 5, 2012, p. 1049

BRZOSKA, M, 'Climate change and the military in China, Russia, the United Kingdom, and the United States', *Bulletin of the Atomic Scientists*, vol. 68, no. 2, 2011, pp. 43–54.

BUSYGINA, I. and FILIPPOV, M., 'Problema vynuzhdennoi federalizatzii', *Pro et Contra*, Vol. 13, No. 3–4, 2009.

BUSYGINA, I. and FILIPPOV, M., 'Agents and principals: what should we wait for after "power vertical"?' *Neprikosnovennyi zapas*, no. 4, 2012, pp. 67–82.

BÄCK, H. and HADENIUS, A., 'Democracy and State Capacity: Exploring a J-Shaped Relationship'. *Governance* 21, 2008, pp. 1–24.

CAROTHERS, T., 'The End of the Transition Paradigm', *Journal of Democracy*, vol. 13, no. 1, 2002.

CAVELTY, M., 'Critical Information Infrastructure: Vulnerabilities, Threats and Responses', *UNIDIR Disarmament Forum*, no. 3, 2007, pp. 15–22.

CHAN, T.C., KILLEEN, J., GRISWOLD, W., LENERT, L., Information technology and emergency medical care during disasters. *Academic Emergency Medicine*, vol. 11, no. 11, 2004, pp. 1229–36.

COLLIER, S., 'Topologies of Power: Foucault's Analysis of Political Government beyond 'Governmentality', *Theory, Culture & Society*, vol. 26, no. 6, p. 83.

COSTA, S., Government Repression and the Death Toll from Natural Disasters (January 23, 2012). CESifo Working Paper No. 3703. Available at SSRN: http://ssrn.com/abstract=1990191

DIAMOND, L., 'Thinking About Hybrid Regimes', *Journal of Democracy*, vol. 13, no. 2, 2002, pp. 21–35.

FONDAHL, G., O. LAZEBNIK, G. POELZER, and V. ROBBEK, 'Native "land claims", Russian style'. *Canadian Geographer*, January 2001.

GELMAN, V. and RYZHENKOV S., Lokal'nye regimy, gorodskoe upravlenie I "vertikal' vlasti v sovremennoi Rossii (http://www.politex.info/content/view/764/30/)

GERACE, R. V., 'Role of medical teams in a community disaster plan'. *Canadian Medical Association Journal*, 120, 1979, pp. 923–8.

GLENNY, M., 'The Cyber Arms Race has Begun'. *The Nation*, October 31, 2011, p. 18.

GROVE, K., 'Insuring "Our Common Future?" Dangerous Climate Change and the Biopolitics of Environmental Security', *Geopolitics* vol. 15, no. 3, 2010, p. 539.

HEDLUND, S., 'Such a beautiful dream: how Russia did *not* become a market economy'. *The Russian Review* vol. 67, April 2008, pp. 187–208.

HEUSALA, A-L., 'Kokonaisturvallisuus-käsite Venäjän turvallisuuspolitiikan tutkimuksessa'. *Kosmopolis* vol. 41, no. 4, 2011, pp.23–38.

HUSKEY, E., 'Nomenklatura Lite? The cadres reserve in Russian public administration'. *Problems of Post-Communism*, vol. 51, no. 2, 2004, pp. 30–39.

KIPP, J., 'Russian Military Doctrine: Past, Present, and Future'. In S Blank, *Russian military politics and Russia's defence doctrine*, Strategic Studies Institute, SSI Monograph, 2011, p. 95.

LAZAREV, Y., A. SOBOLEV, I. SOBOLEVA, and B. SOKOLOV, 'Trial by Fire: A National Disaster's Impact on Attitude Towards the Government in Rural Russia'. HSE Working Papers WP BRP 04/PS/2012

LEMKE, T., 'Foucault, Governmentality, and Critique'. A paper presented at the *Rethinking Marxism Conference*, University of Amherst (MA), 21–24 September 2000.

LEWIS, J., 'Nightmare on Nuke Street: Twelve Terrifying Tales from the Nuclear Crypt', *Foreign Policy Journal*, October 30, 2012.

LUNDBORG, T. and N. VAUGHAN-WILLIAMS, 'Resilience, Critical Infrastructure and Molecular Security: the Excess of Life in Biopolitics', *International Journal Political Sociology*, vol. 5, no. 4, p. 375.

LYNCH, A., 'Roots of Russia's Economic Dilemmas: Liberal Economics and Illiberal Geography', *Europe-Asia Studies*, vol. 54, no. 4, 2002, p. 33.

MCENTIRE, D. A., 'Balancing international approaches to disaster: rethinking prevention instead of relief'. *Australian Journal of Emergency Management*, 13(2), 1998, pp. 50–55.

OLIKER, O., *Assessing Russia's Decline: Trends and Implications for the United States and the US Air Force*. Santa Monica, CA: Rand Corporation, 2002.

OVERLAND, I., 'The Siberian curse: a blessing in disguise for renewable energy'. Sibirica, vol. 9, no. 2, Summer 2010, pp. 1–20.

PETROVA, E., 'Critical infrastructure in Russia: geographical analysis of accidents triggered by natural hazards'. *Environmental Engineering and Management Journal*, vol. 10, no. 1, 2011.

Pursiainen, C., ‘The Challenges for European Critical Infrastructure Protection’. *Journal of European Integration*, vol. 31, no. 6, 2009.

Pursiainen, C. and M. Pei, ‘Authoritarianism or Democracy?’. In C Pursiainen (ed.), *At the Crossroads of Post-Communist Modernization. Russia and China in Comparative Perspective,* Palgrave Macmillan, London, 2012.

Pynnöniemi K., ‘Securing Russia? New security law raises more questions than it answers’. *FIIA Comment,* 14 February 2011. Accessed 15 November 2012, http://www.fiia.fi/en/publication/168/.

Pynnöniemi, K., ‘The political constrains on Russia’s economic development: the visionary zeal of technological modernization and its critics’. *FIIA Working Paper*, The Finnish Institute of International Affairs, Helsinki, 16 June 2010. Accessed 19 November 2012, http://www.fiia.fi/en/publication/127/.

Quiroz Flores, A. and Smith, A., Surviving Disasters. Unpublished manuscript, 2010 (New York: New York University, 2010). Available at http://politics.as.nyu.edu/docs/IO/14714/Surviving_Disasters.pdf.

Robbek, V., ‘Scientific Basis of Education System Formation of Nomadic Peoples of the North’. Novosibirsk: Nauka, 2007.

Roberts, A., ‘Building Resilience: Macrodynamic Constraints on Governmental Response to Crises’. In: *Designing Resilience for Extreme Events: Sociotechnical Approaches*, A. Boin, L. Comfort, C. Demchak, eds., Pittsburgh, PA, University of Pittsburgh Press, 2009. pp. 84–105.

Rothstein, H., ‘The Institutional Origins of Risk: A New Agenda for Risk Research’, *Health, Risk & Society*, vol. 8, no. 3, 2006, pp.216–217.

Savoia, A. and S. Kunal, ‘Measurement and Evolution of State Capacity: Exploring a Lesser Known Aspect of Governance’. Effective States and Inclusive Development Research Centre Working Paper 10, April 2012. Available at SSRN: http://ssrn.com/abstract=2141901.

Savelyev, A., ‘Russian Defense Doctrine’. in S Blank, (ed.) *Russian Military Politics and Russia’s 2010 Defense Doctrine*, Strategic Studies Institute (SSI), March 2011, pp.153–180.

Shenoi, S., ’Editorial’, *International Journal of Critical Infrastructure protection*, vol. 1 no. 1–2, 2008, p. 1.

Shibin, A., J. L. Shibina, and A. A. Kuklin, ‘Regional Social and Economic Risks as Conditions of Formation of Critical Infrastructures’, *ASCE Conf. Proc.* 400, 2011, http://dx.doi.org/10.1061/41170(400)20.

Shlyakhter, A. and R. Wilson, ‘Chernobyl: the inevitable results of secrecy’. *Public Undestand. Sci.* N1, 1992, pp.251–259

Szakonyi, D., ‘You’re Fired!: Identifying Electoral Accountability in a Competitive Authoritarian Regime’. New York: Columbia University, Department of Political Science. April 29, 2011.

Thomas, T., ‘Russia’s information warfare structure: understanding the roles of the security council, Fapsi, the state technical commission and the military’, *European Security*, vol. 7, no.1, 1998, pp.156–172.

Tomanov, G.N., Buldakov, L.A., and Shvedov, V.L. Irradiation of the population and medical consequences of the accident. Priroda, May 1990. 63–67.

Tsalikov, P., V.A. Akimov, K.A. Kozlov, *Otsenka prirodnoi, tehnogennoi i rkologicheskoi besopasnosti Rossii*. FGU VNII GOTcS, MChS Rossii, 2009.

Yanitsky, O., ‘The 2010 Wildfires in Russia. An Ecosociological Analysis’, *Sosiological Research*, vol. 51, no. 2, 2012, pp. 57–75.

Yusupov, P. and V. Shishin, ‘Informatsionno-kommunikatsionnye tekhnologii i natsionalnaya besopasnost — protivorechivaya realnost’. *Informatizatsiya i Svuaz*’, no. 1, 2010.

NEWSPAPER ARTICLES

AHONEN, A., 'Arktinen energiavillitys alkoi tympiä', *Helsingin Sanomat*, 3 August 2012.

ANDREEVA, N., 'Puteshestvie tuda, kuda vas ne pustyat'. *Saratovskie Vesti*, 10 January, 2001.

GLINKI, M. and N. KOSTENKO, 'Nazad v buduschee', *Vedomosti*, 18, 2536, 3 February 2010.

'Hurricane causes blackouts in Russia's northwest', *The Voice of Russia*, 16 August, 2010. Accessed 3 November 2012, http://english.ruvr.ru/2010/08/16/15875344.html.

IVANOV, M., 'Sovet federatsii zanyalsya tsifrovym suverenitetom'. *Kommersant*, 6 November 2012. Accessed 12 November 2012, http://www.kommersant.ru/doc/2060832/print.

KALLIO, H., 'Painajainen pohjassa'. *Lapin Kansa*, 23 September 2012.

KONCHALOVSKY, D., 'Chernobyl tragedy: the last "gift" from the Soviet regime'. *Moscow Times*, Apr 26, 2012.

MAKSIMOV, F. and N. SKORLYGINA, 'Tri goda sputstya vodu'. *Kommersant*, 17 August 2012.

MIHAILOV, A., 'Kriticheskaya infrastruktura okazalas' v kiberopasnosti'. Business FM, 17 November 2010. Accessed 14 November 2012, http://www.bfm.ru/articles/2010/11/17/kriticheskaja-infrastruktura-okazalas-v-kiberopasnosti.html.

OLIPHANT, R., 'Gazprom Spill Response Plan Vague'. *The Moscow Times*, 17 August 2012.

PELLI, P., 'Suomalaisaktivisti sai vesisuihkusta', *Helsingin Sanomat*, 3 September 2012.

PETTERSEN, T., 'Slow Start on the Northern Sea Route'. *Barents Observer*, 27 August 2012.

POLYAKOV, R., 'Vladimir Rushailo obsudil problemy natsional'noi bezopasnosti Rossii'. *Kommersant* (Voronezh), 7 July 2003.

ZVEREVA, E., 'Zimnyaya Skazka'. *Moskovsky Komsomolets*, 10 August 2001.

YLÄJOKI, J., 'Koillisväylälle ei uskalleta mennä'. *Karjalainen*, 9 September 2012.

'Bolee poleviny rossiiskih objektov kriticheskoi infrastrukturu ne obespetsivajut dolzhnyh mer informatsionnoi bezopasnosti', 22 March 2011. Accessed 7 February 2012, http://www.antivirus43.ru/news/222.

'Novaya sistema bezopasnosti Rossii rozhdaetsya v Tambove'. Tambovskaya Zhizn' (Tambov), 10 August 2004.

'Ohrana Pod'ezdov'. *Petrovka*, Moskva 20 June 2001.

'Pri glave Voenno-promyshlennoi komissii bidet sozdan obshchestvennyi sovet'. *Kommersant*, 2 July 2012. Accessed 17 August 2012, http://www.kommersant.ru/news/1971998.

'Sergei Shoigu poprosili zakryt Norilsk'. *Kommersant*, 14 March 2001.

'Sistemy Preduprezhdeniya Katastrof v RF Mnogim Meshayut', Interview of Prof. G Malinetskii, TV-Doshd, 24 July 2012. Accessed 10 October, 2012, http://www.newsland.ru/news/detail/id/1001911/.

'Suuri kaasuhanke pysähtyy Barentsinmerellä', *Helsingin Sanomat*, 30 August 2012.

'Te, kto pridet posle nas, vy zhe v dva raza huzhe'. *Kommersant* Vlast, 20 August 2012.

'V Putin provel selektornoe soveshchanie po voprosu podgotovki organizatsii elektroenergetiki i predpriyatii ZhkH k prohozhdeniyu osenne-zimnego perioda 2009–2010', 5 October 2009. Accessed 11 October 2012, http://www.government.ru/docs/5100/.'Vladimir Putin schitaet, sto budushchee Rossii dolzhno byt svyazano s vysokimi tehnologiyami, a ne s energosistelyami'. ITAR-TASS, 3 December 2001.

'Vse energopredpriyatiya Severo-Zapada poluchili pasporta gotovnosti k zime 2012–2012'. IA REGNUM, 10 October 2012. Accessed 13 October 2012, http://www.regnum.ru/news/polit/1579772.html.

REPORTS

AALTOLA, M., J. SIPILÄ and V. VUORISALO, *Securing Global Commons: A Small State perspective*, FIIA Working Paper, June 2011.

BERGER, H., *Venäjän informaatio-psykologinen sodankäyntitapa terrorismintorjunnassa ja viiden päivän sodassa.* Julkaisusarja 1, Tutkimuksia no. 5, 2010, Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos.

BRUNNER, E. M., and M. SUTTER, *International CIIP Handbook 2008/2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, Center for Security Studies, ETH Zurich, 2009, p. 37.

CONCHAROV, M., *Russian Underground 101.* Research Paper, Trend Micro Incorporated, 2012. Accessed 6 November 2012, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf.

'Facing Hazards and Disasters: Understanding Human Dimensions', Committee on Disaster Research in the Social Sciences: Future Challenges and Opportunities. National Research Council. The National Academies Press, Washington, D.C., 2006.

GORDON, K., and M DION, 'Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security', *OECD*, May 2008, p. 3.

HELLENBERG, T. and P. VISURI (eds), *Preventing Terrorism in Maritime Regions: Case Analysis of the Project Poseidon.* Aleksanteri Institute, Aleksanteri Papers, no. 1, 2009.

HELLENBERG, T., 'Energy security and transportation risks in the Baltic Sea Region'. *Aleksanteri Series*, 2007.

Infrastructure to 2030: Telecom, Land Transport, Water and Electricity, Secr etary-General of the OECD, Paris, May 2006. Accessed 3 November 2012, http://www.inst-informatica.pt/servicos/informacao-e-documentacao/biblioteca-digital/gestao-e-organizacao/0306011E.pdf;

KUDRIK, I., A. NIKITIN, N. BOHMER, N. DIGGES, N. THOMAS, M. MCGOVERN, and A. ZOLOTKOV, 'The Arctic Nuclear Challenge'. *Bellona Report* Volume 3 – 2001. Oslo: Bellona, 2001.

KUDRIK, I. , A. NIKITIN, N. BOHMER, C. DIGGES, V. KUZNETSOV, V. LARIN, 'The Russian Nuclear Industry'. *Bellona Report* Volume 4 – 2004. Oslo: Bellona, 2004.

PALLIN, V., (ed.), *Russian Military Capability in a Ten-Year Perspective – 2011.* Swedish Defence Research Agency (FOI), June 2012.

PLEKHANOV, A. and ISAKOVA, A., 'Region-specific Constrains to Doing Business: evidence from Russia', EBRD, *Working Paper*, no. 125, March 2011. Accessed 3 November 2012, http://www.ebrd.com/downloads/research/economics/workingpapers/WP0125.pdf.

POLISHCHUK, L., 'Misuse of Institutions: Lessons from Transition', UNWIDER, Working Paper no. 2010/75, June 2010.

ROFFEY, R., *Biotechnology in Russia: Why is it not a success story?* Swedish Defence Research Agency, User Report, 2010.

PRESENTATIONS

KAISER, R., 'Estonia and the Birth of Cyberwar'. Presentation at Aleksanteri Institute, 4 October 2012.

LENCHUK E., 'EU-Russia Programme partnership for modernization and its role in the technological upgrade of the Russian Economy', presentation at the seminar on I*ndustrial modernization: is it possible to boost innovation in Russia –seminar*, 27 October 2011, Moscow, The Moscow State University.

Previously published in the series

TANJA TAMMINEN (ed.)
Strengthening the EU's peace mediation capacities:
Leveraging for peace through new ideas and thinking
FIIA Report 34 (2012)

HARRI MIKKOLA, JUKKA ANTEROINEN,
VILLE LAUTTAMÄKI (eds.)
Uhka vai mahdollisuus?
Suomi ja Euroopan puolustus- ja
turvallisuusmarkkinoiden muutos
FIIA Report 33 (2012)

TOUKO PIIPARINEN & VILLE BRUMMER (eds.)
Global networks of mediation:
Prospects and avenues for Finland as a peacemaker
FIIA Report 32 (2012)

MIA PIHLAJAMÄKI & NINA TYNKKYNEN (eds.)
Governing the blue-green Baltic Sea:
Societal challenges of marine eutrophication
prevention
FIIA Report 31 (2011)

ARKADY MOSHES & MATTI NOJONEN (EDS.)
Russia-China relations:
Current state, alternative futures,
and implications for the West
FIIA Report 30 (2011)

TEIJA TIILIKAINEN & KAISA KORHONEN (eds.)
Norden — Making a Difference?
Possibilities for enhanced Nordic cooperation
in international affairs
FIIA Report 29 (2011)

TIMO BEHR (ed.)
Hard Choices:
The EU's options in a changing Middle East
FIIA Report 28 (2011)

JYRKI KALLIO
Tradition in Chinese politics:
The Party-state's reinvention of the past and
the critical response from public intellectuals
FIIA Report 27 (2011)

STEVEN PARHAM
Controlling borderlands?
New perspectives on state peripheries in southern
Central Asia and northern Afghanistan
FIIA Report 26 (2010)

MARI LUOMI
Managing Blue Gold:
New Perspectives on Water Security
in the Levantine Middle East
FIIA Report 25 (2010)

TAPANI PAAVONEN
A New World Economic Order:
Overhauling the Global Economic Governance
as a Result of the Financial Crisis, 2008–2009
FIIA Report 24 (2010)

TOBY ARCHER, TIMO BEHR, TUULIA NIEMINEN (eds)
Why the EU fails
– Learning from past experiences
to succeed better next time
FIIA Report 23 (2010)

LOUISE WIUFF MOE
Addressing state fragility in Africa:
A need to challenge the established 'wisdom'?
FIIA Report 22 (2010)

TARJA CRONBERG
Nuclear-Free Security:
Refocusing Nuclear Disarmament and the Review
of the Nuclear Non-Proliferation Treaty
FIIA Report 21 (2010)

KRISTIAN KURKI (ed.)
The Great Regression?
Financial Crisis in an Age of Global Interdependence
FIIA Report 20 (2009)

ANNA KORPPOO & ALEX LUTA (ed.)
Towards a new climate regime?
Views of China, India, Japan, Russia and the United States on the road to Copenhagen
FIIA Report 19 (2009)

MINNA-MARI SALMINEN & ARKADY MOSHES
Practise what you preach
– The prospects for visa freedom
in Russia-EU relations
FIIA Report 18 (2009)

CHARLY SALONIUS-PASTERNAK (ed.)
From Protecting Some to Securing many:
Nato's Journey from a Military Alliance
to a Security Manager
FIIA report 17 (2007)

TOBY ARCHER & TIHOMIR POPOVIC
The Trans-Saharan Counter-Terrorism Initiative:
The US War on Terrorism in Northwest Africa
FIIA Report 16 (2007)

SERGEI MEDVEDEV
EU-Russian Relations:
Alternative futures
FIIA Report 15 (2006)

HANNA OJANEN (ed.)
Peacekeeping — Peacebuilding:
Preparing for the future
FIIA Report 14 (2006)

HANNA OJANEN
The EU and the UN: A shared future
FIIA Report 13 (2006)

GRZEGORZ GROMADZKI, RAIMUNDAS LOPATA
& KRISTI RAIK
Friends or Family?
Finnish, Lithuanian and Polish perspectives on the EU's policy towards Ukraine, Belarus and Moldova
FIIA Report 12 (2005)

HU ANGANG, LINDA JAKOBSON & SHEN MINGMING
China's Transforming Society and Foreign Policy
FIIA Report 11 (2005)

KRISTI RAIK & TEEMU PALOSAARI
It's the Taking Part that Counts:
The new member states adapt to EU foreign and security policy
FIIA Report 10 (2004)

HISKI HAUKKALA & ARKADY MOSHES
Beyond "Big Bang":
The Challenges of the EU's Neighbourhood Policy in the East
FIIA Report 9 (2004)

LINDA JAKOBSON
Taiwan's Unresolved Status:
Visions for the Future and Implications
for EU Foreign Policy
FIIA Report 8 (2004)

LINDA JAKOBSON
Taiwanin kiistanalainen asema:
Tulevaisuudennäkymät ja niiden
vaikutukset EU-Kiina-suhteisiin
UPI-raportti 8 (2004)

TOBY ARCHER
Kansainvälinen terrorismi ja Suomi
UPI-raportti 7 (2004)

HANNA OJANEN (ed.)
Neutrality and non-alignment in Europe today
FIIA Report 6 (2003)

SOILE KAURANEN & HENRI VOGT
Piilopoliittisuudesta poliittisuuteen:
Afrikan, Karibian ja Tyynenmeren valtioiden
ja Euroopan unionin yhteistyön kehitys
UPI-raportti 5 (2003)

ARKADY MOSHES (ED.)
Rethinking the Respective Strategies
of Russia and the European Union
Special FIIA -Carnegie Moscow Center Report (2003)

ARKADY MOSHES
Ukraine in tomorrow's Europe
FIIA Report 4 (2003)

HANNA OJANEN
EU:n puolustuspolitiikka ja suhteet Natoon:
Tervetullutta kilpailua
UPI-raportti 3 (2003)

HISKI HAUKKALA

Towards a Union of Dimensions
The effects of eastern enlargement
on the Northern Dimension
FIIA Report 2 (2002)

HISKI HAUKKALA

Kohti ulottuvuuksien unionia: Itälaajentumisen
vaikutukset pohjoiselle ulottuvuudelle
UPI-raportti 2 (2002)

CHRISTER PURSIAINEN & SINIKUKKA SAARI

Et tu Brute!
Finland's NATO Option and Russia
FIIA Report 1 (2002)

CHRISTER PURSIAINEN & SINIKUKKA SAARI

Et tu Brute!
Suomen Nato-optio ja Venäjä
UPI-raportti 1 (2002)

FIIA REPORT 35

Russian critical infrastructures

Vulnerabilities and policies

Katri Pynnöniemi (ed.)

The Russian policy on critical infrastructure protection was outlined in the early 2000s and has been consolidated in recent years as a part of the national security strategy. It is built upon the civil defence system of the Soviet era, a system that has been modernized under the auspices of the Ministry of Emergency Situations of Russia.

The Russian policies on critical infrastructure protection (CIP) are evolving against a background composed of an uneasy combination of factors: the degeneration of infrastructures critical for the country's economic and social development, and the de-legitimization of political institutions responsible for protecting 'population' and 'territory'. The recent major catastrophes in Russia, the forest fires in 2010 in particular, have become examples of political events that offer a point of reference for the current regime's failure to uphold its promises of 'order and stability'.

Global climate change and the extraction of natural resources in the Arctic region are regarded as both a challenge and an opportunity for Russia. In Russian and European discussions, the Northern Sea Route is usually viewed in terms of opportunity, as it will form one of the major corridors of the global commercial flows. The extraction of oil and gas reserves in the Arctic is a long-term project that has intensified in recent years, although the pace of development has slowed down of late. However, it is generally acknowledged that the 'opening of the new northern frontier' is anything but simple. Climate change, and the possible melting of the Russian permafrost resulting from it, poses a real challenge that adds an entirely new dimension to the notion of 'critical infrastructures'.

ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

ISBN 978-951-769-365-3
ISSN 1458-994X