

CONNECTIONS

THE QUARTERLY JOURNAL

THE ARAB SPRING: CHALLENGES, OBSTACLES AND DILEMMAS

By Graeme P. Herd



PARTNERSHIP FOR
PEACE CONSORTIUM
OF DEFENSE
ACADEMIES AND
SECURITY STUDIES
INSTITUTES

FALL 2011

Distance Learning in the Bundeswehr: Skills Are More Than Knowledge

By Dr. Manuel Schulz and Andrea Neusius

The Correlation Between Non-State Actors and Weapons of Mass Destruction

By Reshmi Kazi

The Essence of Crosscultural Security Education

By Lt. Col. Andrzej Pieczywok

Partnership for Peace Consortium of Defense Academies and Security Studies Institutes

The PFP Consortium Editorial Board

Sean S. Costigan	Executive Editor
Jean Callaghan	Managing Editor
Gediminas Dubauskas	Lithuanian Military Academy
Peter Foot	Geneva Centre for Security Policy
Piotr Gawliczek	National Defence University, Warsaw
Hans-Joachim Giessmann	Berghof Conflict Research Centre, Berlin
Fred Labarre	Royal Military College of Canada (Kingston)
Todor Tagarev	Bulgarian Academy of Sciences
Michael Schmitt	George C. Marshall European Center for Security Studies
Elena Kovalova	George C. Marshall European Center for Security Studies
Leila Alieva	Center for National and International Studies, Baku
David Mussington	National Railroad Passenger Corporation (Amtrak)

The PFP Consortium Publication Manager

Enrico Müller	Partnership for Peace Consortium Operations Staff
---------------	---

The articles appearing in all *Connections* publications do not necessarily represent the views of the authors' institutions, their governments, or the PFP Consortium itself.

The Consortium's family of publications is available at no cost at <https://consortium.pims.org/publications>. If you would like to order printed copies for your library, or if you have questions regarding the Consortium's publications, please contact the PFP Operations Staff at pfpcpublications@marshallcenter.org. Should you have any problems with your subscription, please include the ID number found on the first line of the mailing label.

John J. Kane
Acting Executive Director

Sean S. Costigan
Chair, Editorial Board

CONNECTIONS

The Quarterly Journal

Volume X, Number 4

Fall 2011

The Correlation Between Non-State Actors and Weapons of Mass Destruction	1
<i>By Reshmi Kazi</i>	
Global Warming and Security: The Security Implications for NATO and the EU of a Melting Polar Ice Cap in the High North.....	11
<i>By Udo Michel</i>	
The Emergence of Organized Criminal Networks as Extralegal Authorities.....	51
<i>By Priscilla Bittencourt Ribeiro de Oliveira and Plamen P. Penev</i>	
The Essence of Crosscultural Security Education.....	61
<i>By Lt. Col. Andrzej Pieczywok</i>	
International Arms Control and Law Enforcement in the Information Revolution	73
<i>By Yury Barmin, Grace Jones, Sonya Moiseeva, and Zev Winkelman</i>	
Distance Learning in the Bundeswehr: Skills Are More Than Knowledge.....	95
<i>By Dr. Manuel Schulz and Andrea Neusius</i>	
The Arab Spring: Challenges, Obstacles and Dilemmas.....	103
<i>By Graeme P. Herd</i>	

The Correlation Between Non-State Actors and Weapons of Mass Destruction

By Reshmi Kazi*

The probability of non-state actors acquiring and using weapons of mass destruction against vulnerable non-combatants has remained a worrisome threat since the turn of the century. However, the watershed event of the terrorist attacks on the World Trade Center in New York City and the Pentagon in Washington, D.C. on 11 September 2001 has significantly raised concerns regarding the availability of chemical, biological, radiological, and nuclear (CBRN) weapons and their probable usage. The reasons for increased concerns are varied. They include:

- Widespread perceptions that the events of 9/11 marked the crossing of a threshold in terrorist constraint and lethality¹
- Open source accounts of interest in WMD technology by non-state actors²
- Increased availability of WMD technology³
- Greater media attention⁴
- Persistent Western military presence in global affairs and an upsurge of anti-Western sentiments⁵

* Dr. Reshmi Kazi is an Associate Fellow at the Institute for Defence Studies and Analysis in New Delhi, India. She received her Ph.D. in Disarmament Studies from the School of International Studies at Jawaharlal Nehru University in New Delhi.

¹ Prior to September 2001, no terrorist attack anywhere in the world had killed more than 500 people. In the twentieth century, only fourteen terrorist events killed more than 100 people. See Bruce Hoffman, "CBRN Terrorism Post 9/11," in *Weapons of Mass Destruction and Terrorism*, eds. Russell D. Howard and James Forest (New York: McGraw-Hill, 2007).

² On 11 May 2008, *RIA Novosti* reported that Russia's antiterrorism committee had said it had evidence that terrorists were trying to gain access to weapons of mass destruction and to technology needed to produce them, as stated in Nancy K. Hayden, "Terrifying Landscapes: Understanding Motivations of Non-state Actors to Acquire and/or Use Weapons of Mass Destruction," in *Unconventional Weapons and International Terrorism: Challenges and New Approaches*, eds. Magnus Ranstorp and Magnus Normark (New York: Routledge, 2009), 188.

³ See Matthew Bunn and Anthony Wier, "Terrorist Nuclear Weapon Construction: How Difficult?" *Annals of the American Academy of Political and Social Science* 607 (Sept. 2006): 133–49.

⁴ See Jonathan B. Tucker, "The Proliferation of Chemical and Biological Weapons Materials and Technologies to State and Sub-State Actors," Testimony before the Subcommittee on International Security, Proliferation and Federal Services of the U.S. Senate Committee on Governmental Affairs, Washington, D.C., 7 November 2001.

⁵ See Brigitte Nacos, *Mass-Mediated Terrorism: The Central Role of the Media in Terrorism and Counterterrorism* (Lanham, MD: Rowman and Littlefield, 2007).

- The vital role played by Internet technology for Al Qaida in propagating its ideology and integrating its loose networks of affiliates and sympathizers.

Despite these important factors, one needs to ponder the fact that it is just not enough to have heightened concerns about the threat of a probable CBRN attack by violent non-state actors. In qualitative terms, understanding the reasons behind a threat is “not the same thing as facing an actual increase in a threat.”⁶ However, a comprehensive understanding of these factors is vital for developing an effective decision-making agenda in the interest of a successful national security and foreign policy strategy. According to John Parachini, “Although hedging against terrorists exploiting the catastrophic potential of CBRN weapons is an essential task of government resources ... attention cannot simply result in obsessing over CBRN effects but also must produce improved understanding of the motivations, vulnerabilities, capabilities and context for actual attacks, not just expressions of interest.”⁷ Hence, in tackling the challenge of preventing politically violent terrorist groups and organizations from resorting to the use of chemical, biological, radiological and nuclear weapons, it is not sufficient just to secure all nuclear weapons and weapons-usable nuclear materials. A sound policy would include concerted efforts to substantially dwell on an important question: What factors drive violent terrorist groups like Al Qaeda to seek out the most fearsome weapons? Unfortunately, research indicates that there is a paucity of statistical studies in analyzing why terrorist groups—particularly those grounded in extreme religious ideologies, like Al Qaeda—want to acquire and use CBRN weapons. This difficulty is further compounded by two additional factors: the absence of any real CBRN attacks by terrorists, which makes any empirical analysis impossible; and the problems associated with comprehending the potential extent of attacks by terrorists using CBRN weapons. However, despite these problems, this article will make an attempt to analyze certain variables that may provide a deeper understanding of violent terrorist groups’ penchant for weapons of mass destruction.

⁶ Hayden, “Terrifying Landscapes,” 164.

⁷ John Parachini, “Putting WMD Terrorism into Perspective,” *Washington Quarterly* 26:4 (2003) 37–50.

The Threat of Nuclear Terrorism⁸

The existing state of knowledge within the nuclear weapons technology field makes it painfully obvious that the danger of nuclear terrorism is no longer hypothetical. U.S. President Barack Obama, in a speech in Prague on 5 April 2009, emphasized that the danger of terrorists' acquisition and use of catastrophic weapons presents "the most immediate and extreme threat to global security."⁹ There are several indicators that frame the danger of a probable CBRN attack.

Al Qaeda is in quest of nuclear weapons, and has attempted more than once to acquire the materials and expertise needed to make them. This is evident from Osama bin Laden's pronouncement that the acquisition of nuclear weapons or other weapons of mass destruction constituted a "religious duty" for Muslims.¹⁰ Shortly before the 9/11 attacks, bin Laden and Ayman al-Zawahiri met with two senior Pakistani nuclear scientists to discuss nuclear weapons.¹¹ Al Qaeda's efforts to acquire CBRN weapons continued unabated even after the disintegration of the group following the dismantling of the Taliban regime and elimination of their sanctuaries in Afghanistan. In 2002–03, U.S. intelligence received a "stream of reliable reporting" that the leadership of Al Qaeda's cell in Saudi Arabia was negotiating to purchase three objects they believed to be Russian "nuclear devices," and that Al Qaeda's central leadership had approved the purchase if a Pakistani expert was able to confirm that they were genuine. (The actual nature of these "devices," if they existed, the name of the Pakistani expert, and the type of equipment he was to use to examine the devices have never been learned.¹²) It is well documented that even before Al Qaeda emerged into global consciousness, the Japanese terror cult Aum Shinrikyo also made concerted efforts to acquire CBRN weapons (and succeeded in launching an attack on the Tokyo subway in 1995 using sarin gas, killing thirteen people). As evidence and records indicate that at least two groups have actively pursued CBRN weapons in the last fifteen years, there is no reason to believe that future terrorist groups will not pursue the nuclear path.

⁸ See Reshmi Kazi, "Pakistan's HEU-based Nuclear Weapons Programme and Nuclear Terrorism: A Reality Check," *Strategic Analyses* 33:6 (November 2009): 863–65.

⁹ "Remarks by President Barack Obama," Prague, 5 April 2009; available at http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered/.

¹⁰ Rahimullah Yusufzai, "Interview with Bin Laden: World's Most Wanted Terrorist," *ABC News Online* (2 January 1999); available at <http://cryptome.org/jya/bin-laden-abc.htm>.

¹¹ David Albright and Holly Higgins, "A Bomb for the Ummah," *Bulletin of the Atomic Scientists* 59:2 (March–April 2003): 49–55; available at <http://thebulletin.metapress.com/content/ru1k226j4ln45851/>.

¹² Rolf Mowatt-Larssen, "Al Qaeda WMD Threat: Hype or Reality?" Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University (January 2010); available at <http://belfercenter.ksg.harvard.edu/files/al-qaedawmd-threat.pdf>.

Several studies by the U.S. and other governments have concluded that it is plausible that a sophisticated terrorist group could make a crude nuclear bomb if it got enough of the needed nuclear materials. The easy availability of the nuclear science knowledge in the public domain has eased the work of terrorists seeking CBRN weapons. For example, one study by the now-defunct Congressional Office of Technology Assessment determined: “A small group of people, none of whom have ever had access to the classified literature, could possibly design and build a crude nuclear explosive device. ... Only modest machine-shop facilities that could be contracted for without arousing suspicion would be required.”¹³ In addition, several experiments like the “Nth Country Experiment” have proved that “three post-docs with no nuclear knowledge could design a working atom bomb.”¹⁴ In January 2004, then-U.S. Senator Joseph R. Biden instructed the heads of national laboratories to “build, off the shelf, a nuclear device.” The scientists were able to “actually construct this device.”¹⁵ It is also important to bear in mind that, from the caves of Afghanistan, Al Qaeda was able to mastermind and successfully execute the 9/11 attacks. Although the 9/11 terrorist attacks presented no technical challenges of the kind a nuclear weapon poses, the precision with which Al Qaeda was able to overcome the daunting challenges in carrying out their operation deserves attention. It can therefore be presumed with a fair degree of certainty that Al Qaeda would be now be further motivated to attempt a more challenging task.

According to International Atomic Energy Agency (IAEA) reports, there have been eighteen documented cases of theft or loss of plutonium or highly enriched uranium (HEU). Fissile materials are housed in numerous buildings in many countries. Security measures at these sites vary widely, from excellent to appalling. The risks to the proliferation of nuclear materials range from insider corruption to weak nuclear security regulation. In early February 2010, peace activists broke into a Belgian base where U.S. nuclear weapons are reportedly stored. They were finally intercepted by a single guard, whose weapon appeared to be unloaded—some ninety minutes after they entered the base.¹⁶ In

¹³ U.S. Congress, Office of Technology Assessment, “Nuclear Proliferation and Safeguards” (Washington, D.C.: OTA, 1977), 140; available at <http://www.princeton.edu/~ota/disk3/1977/7705/7705.PDF>.

¹⁴ Dan Stober, “No Experience Necessary,” *Bulletin of Atomic Scientists* (March–April 2003): 57–63.

¹⁵ Joseph Biden, remarks at the Paul C. Warnke Conference on the Past, Present, and Future of Arms Control, Washington, D.C., 28 January 2004, as cited in Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York: Times Books, 2004), 95.

¹⁶ See Jeffrey Lewis, “Activists Breach Security at Kleine Brogel,” *ArmsControlWonk.com* (4 February 2010); available at <http://www.armscontrolwonk.com/2614/activists-breach-security-at-kleine-brogel>. See also Hans Kristensen, “U.S. Nuclear Weapons Site in Europe Breached,” *FAS Strategic Security Blog, Federation of American Scientists* (4 February 2010); available at <http://www.fas.org/blog/ssp/2010/02/kleinebrogel.php>.

November 2007, four armed men broke into the Pelindaba nuclear facility in Pretoria, South Africa, a site where an estimated twenty-five bombs' worth of weapons-grade uranium is stored.¹⁷ In February 2006, Russian citizen Oleg Khinsagov was arrested in Georgia (along with three Georgian accomplices) with some 100 grams of HEU enriched to 89 per cent U-235.¹⁸ According to the International Atomic Energy Agency, there have been a “disturbingly high” number of reports of missing or illegally trafficked nuclear material. According to agency figures, there were 243 incidents between June 2007 and June 2009.¹⁹ Fortunately, the amounts reported missing have been small. Insider threats are also a potential source for the terrorists to tap nuclear materials for their goal; underpaid and disgruntled soldiers and guards, along with ideologically-motivated insiders, present attractive targets for terrorist networks.

Porous borders can facilitate the illicit movement of nuclear and radioactive materials by terrorists. The vast length of national borders and the myriad potential pathways across these borders makes the interdiction of smuggled sensitive weapons-grade material extremely difficult. In addition, it is also very difficult to detect radiation from plutonium and highly enriched uranium, particularly if it is shielded by protective layers. The detectors that are being widely deployed throughout the world—or even the more expensive Advanced Spectroscopic Portals (ASPs) that are being considered to replace them—would have little chance of detecting HEU metal if it had significant shielding.²⁰

Finally, the threat of nuclear and other forms of WMD terrorism is likely to increase in the absence of substantial changes in the international policies and practices as part of comprehensive non-proliferation efforts. It leaves one to ponder that the Non-Proliferation Treaty (NPT)—the primary bulwark in the edifice of the non-proliferation regime—does not contain any provision to deal with the challenge of violent terrorists seeking to acquire and use nuclear weapons. It is open to debate whether

¹⁷ The Pelindaba nuclear facility is one of South Africa's most heavily guarded “national key points,” defined by the government as “any place or area that is so important that its loss, damage, disruption or immobilization may prejudice the Republic.” See Micah Zenko, “A Nuclear Site is Breached,” *Washington Post* (20 December 2007): A29.

¹⁸ Elena Sokova, William C. Potter, and Cristina Chuen, “Recent Weapons Grade Uranium Smuggling Case: Nuclear Materials Are Still on the Loose,” Center for Non-proliferation Studies, Monterey Institute of International Studies (26 January 2007); available at <http://cns.miis.edu/pubs/week/070126.htm>. Also see Michael Bronner, “100 Grams (And Counting): Notes From the Nuclear Underworld,” Project on Managing the Atom, Harvard University (June 2008); available at http://belfercenter.ksg.harvard.edu/publication/18361/100_grams_and_counting.html.

¹⁹ “Keeping Tabs on Nuclear Material,” *International Herald Tribune* (2 November 2008).

²⁰ See Thomas B. Cochran and Matthew G. McKinzie, “Detecting Nuclear Smuggling,” *Scientific American* (April 2008).

the NPT should be substantively amended to deal with the challenge of clandestine proliferation of nuclear weapons and weapons-grade material.

Despite the reality check provided by the various indicators of nuclear terrorism, there exists no conclusive evidence to support the claim that terrorists have acquired the relevant expertise to construct a bomb. There are also no hard facts to substantiate the claim that terrorists can successfully build a crude nuclear explosive with HEU. Building even a simple nuclear device can be a challenging task involving numerous complexities, as was encountered by Al Qaeda and Aum Shinrikyo. There is also an emerging debate among radical Islamist groups about the moral legitimacy of mass killing of innocent people.²¹ Nuclear security has also been improving, although there is still much to be done. However, this positive aspect also comes with the caveat “as of now.” It is difficult to precisely quantify the chances of nuclear terrorism. Hence, in dealing with the danger of nuclear or other forms of CBRN terrorism, there cannot be any room for complacency.

Nuclear Terrorism: Analyses of Drivers and Consequent Scenarios

It can be assumed that small terrorist organizations that are relatively young, inexperienced, and with no territory of their own in which to safely operate will choose the least risky and most reliable tactical forms of attack. Hence, it can be presumed with a fair degree of certainty that only large, well-established and well-networked organizations will seek to attempt CBRN terrorism. What are the drivers that propel terrorist organizations of the likes of Al Qaeda to seek the most catastrophic weapons?

Factors Contributing to the Potential Development of Nuclear Terrorism

State Assistance. The notion of state assistance to terrorist organizations does not necessarily imply that the state will facilitate the direct provision of weapons of mass destruction into the wrong hands. Rather, it generalizes that a terrorist group with WMD proclivities and state support will have greater access to funding, sophisticated weaponry, and logistical and technical support. The organization would possess a higher level of resources and technical expertise than it would otherwise be able to muster, while at the same time its strategic calculus would be less constrained by the need to maintain the support of a wider popular constituency.²² It is arguable, for instance, whether Al Qaeda would ever have been able to set up its chemical and bio-

²¹ Lawrence Wright, “The Rebellion Within,” *The New Yorker* (2 June 2008); available at http://www.newyorker.com/reporting/2008/06/02/080602fa_fact_wright.

²² Brian M. Jenkins, “Defense Against Terrorism,” *Political Science Quarterly* 101:5 (1986): 778.

logical weapons “laboratories” in Afghanistan, or pursue its nuclear ambitions while in Sudan, were it not for the hospitable environment provided by the anti-Western governments of these states.²³

Technological Development. It can be expected that the higher the level of technological development of the host country in which violent terrorist groups with a penchant for WMD operate, the more likely that non-state actors will be able to acquire the requisite knowledge, skills, materials, and equipment to develop nuclear or other forms of CBRN weapons. In recent years, the United Nations Conference on Trade and Development (UNCTAD) has developed an index of technological development.²⁴ However, this index is not available for countries like Afghanistan, Sudan, and Iraq. Nevertheless, according to noted analysts Victor Asal and R. Karl Rethemeyer, the UNCTAD index is highly correlated (0.86) with energy consumption per capita. Thus they settled on this widely available measure as an appropriate proxy for the technological level of a terrorist organization’s home state.²⁵

Rooted in the Global Economy. Developing and producing CBRN weapons requires access to sources of knowledge that are primarily in the Western sphere of influence. Most of these science and research data are available in the public domain, via the Internet, Ph.D. theses, and declassified documents accessible in public and academic libraries. Despite this, terrorists would require access to training and research institutions to be competent and effective in actually constructing a weapon. This can be possible only with access to scientists and engineers who are based in the host countries. The probability of non-state actors gaining access to skilled adherents can be expected to increase the more a given host country is globally integrated with learning institutions worldwide.

Terrorist organizations would also enormously benefit from the integration of the host country into the global economy. Terrorist groups would require access to sophisticated devices and materials that are not available in the open markets of less developed countries. However, the integration of such countries with the global economy will allow increased flows of trade that will provide greater opportunities for terrorists to clandestinely deliver and receive materials, blueprints, weapons, and devices concealed in legitimate cargoes.

²³ Center for Nonproliferation Studies, “Chart: Al-Qaida’s WMD Activities,” *Monterey Institute of International Studies*, 13 May 2005; available at http://cns.miis.edu/other/sjm_cht.htm.

²⁴ United Nations Conference on Trade and Development, *Indicators of Technology Development* (Geneva: United Nations, 2002).

²⁵ Victor H. Asal and R. Karl Rethemeyer, “Islamist Use and Pursuit of CBRN Terrorism,” in *Jihadists and Weapons of Mass Destruction*, eds. Gary Ackerman and Jeremy Tamsett (Boca Raton, FL: CRC Press: 2009): 337–38.

Nature of the Regime. The type of regime prevailing in the host country of a non-state actor significantly contributes to their capability and motivation to become involved in WMD terrorism through the wide variation in existing security parameters. Terrorists might find it difficult generally to operate in an autocratic environment where the state can exert greater police powers than is possible in a democracy.²⁶ However, terrorists would be able to operate more freely if the general effect of autocracy is reduced in the host country.

Internal Disturbances. Internal disturbances like civil strife and insurgency create political instability that accelerates terrorist groups' pursuit of CBRN weapons. Domestic instability creates zones where central authority becomes ineffective, thereby providing bases where authority can be exerted by terrorist groups or their political wings. This facilitates the building, developing, assembling, and transshipment of materials, knowledge, and technology needed to acquire and utilize weapons of mass destruction. For example, Hamas's partial control over the Gaza Strip has made it possible for it to illicitly acquire a variety of lethal weapons. Civil wars can also deflect the time and attention of less-developed host countries, providing terrorist organizations with the opportunity to carry out their illegal activities clandestinely.

Situation in the Network of Terrorist Alliances. The more deeply a terrorist organization is embedded in the network of global terrorist alliances, the more likely it is to pursue CBRN terrorism. To carry out an act of nuclear or some other form of WMD terrorism would require enormous planning and networking. This could be possible if a non-state actor is well integrated with the global network of like-minded terrorists.

Revenge. If Al Qaeda had only informed the global media that it would kill four million Americans unless the United States withdrew its entire military presence from Saudi Arabia, the threat might have caused concern, but the impact would not have been nearly as great as was caused by the attacks that followed in September 2001. Terrorist violence is a costly form of signaling. It is difficult for terrorist groups to impose their will by the direct use of force. However, sometimes terrorists are successful in persuading their targets to do as they wish by convincing their adversaries of their ability to impose costs and their determination to do so. Given the conflict of interest between terrorists and their targets, ordinary communication or "cheap talk" is insufficient to change minds or influence behavior.²⁷ Since it is hard for weak actors

²⁶ Paul Wilkinson, *Terrorism Versus Democracy: The Liberal State Response*, Cass Series on Political Violence (London: Frank Cass, 2000).

²⁷ Andrew H. Kydd and Barbara F. Walter, "The Strategies of Terrorism," *International Security* 31:1 (Summer 2006): 50.

to make credible threats, terrorists are forced to display publicly just how far they are willing to go to obtain their desired results.²⁸

The drivers listed above can be factors that enable violent non-state actors to seek CBRN weapons. However the good news is that there has been no recorded event of terrorists having acquired the relevant expertise to construct a nuclear bomb. There are also no hard facts to substantiate the claim that terrorists can successfully build a crude nuclear explosive, or “dirty bomb,” with HEU. Nuclear security has also been improving, though there is still much to be done to secure remaining stores of fissile materials. However, as was stated above, the caveat must be given: as of now. The trends of increasing violence, the spread of technology, and the ready availability of nuclear knowledge in the public domain compel us to think about the probability of a nuclear attack by terrorists. As was established by the bipartisan 9/11 Commission in the United States, it was a “failure of imagination” that led to the 9/11 disaster. The question now is, Can we afford to overlook any such possibility again? This question becomes more relevant especially after the attempted Al Qaeda terrorist attack on Northwest Airlines Flight 253 on 25 December 2009 (the so-called “underwear bomber” attack, when Umar Farouk Abdulmutallab, a native of Nigeria, attempted to detonate plastic explosives sewn in his underwear on a flight from Amsterdam to Detroit). To prevent a failure of imagination once again, three plausible scenarios exist under which a nuclear terrorist attack might be likely.

Probability Scenarios for Terrorist Nuclear Attack

Scenario 1. The weakening of the global nuclear nonproliferation regime—particularly the breakdown of the Non-Proliferation Treaty—will erode comprehensive nonproliferation efforts. This is likely to scuttle the possibility of ushering in any substantial changes to international policies and practices related to the NPT regime. This in turn will present a setback to the intelligence and law enforcement agencies that have spearheaded many counterterrorism missions, which will severely compromise the security measures protecting global stockpiles of nuclear weapons and materials. The terrorists will take advantage of the weakened security systems to gain access to dangerous fissile material or nuclear weapons.

Scenario 2. The present domestic uncertainty surrounding the newly acquired nuclear capability in North Korea presents another worrisome scenario. Hypothetically, should the present regime of Kim Jong Il fall from power because of internal turmoil or a military coup, there is a possibility that nuclear weapons may go missing in the ensuing disorder and eventually fall into the hands of terrorists. Cash-strapped North

²⁸ Ibid., 51.

Korea could trade its missiles and nuclear know-how with other states, who in turn may provide these warheads to terrorists.

Scenario 3. The growing civil unrest within Pakistan could divert the attention of the military, which is charged with safeguarding the nuclear assets within the country. Consequently, terrorists with insider assistance could gain access to Pakistan's fissile materials.

However, the above probabilities can be prevented by the recognition of the threat of nuclear terrorism as real, and the formulation of a clear agenda to combat the threat and pursue it with timely action to reduce the risk of nuclear terrorism. To that extent, another scenario that can be drawn is the following:

Scenario 4. Vigilance is stepped up globally, including upgrades to the security systems of sites housing dangerous nuclear materials. National laboratories develop a new suite of technologies to detect and counter unconventional weapons of all types, and these sentinels are positioned in a multilayered defense system within the country.

Conclusion

The motivation for violent terrorist groups to seek and acquire weapons of mass destruction is a complex matter, and it plays out in dynamic and evolving circumstances. It is not a process that occurs in one day. However, in spite of the complexities involved, it remains an important fact that the threat of nuclear terrorism is no longer one of science fiction. It is a plausible phenomenon, and the threat is credible in terms of the will and intention of terrorist groups like Al Qaeda to pursue the nuclear option. The only safeguard against this catastrophic possibility is a concerted global effort to counter and prevent it.

Global Warming and Security: The Security Implications for NATO and the EU of a Melting Polar Ice Cap in the High North

By Udo Michel*

Introduction

Environmental changes will have an impact on global and regional security communities. This article will examine the security challenges posed by the melting of the polar ice cap in the High North. Many NATO and EU members have manifest interests in this region, and parts of the Arctic belong to the NATO treaty area. Official documents, political statements, and actions already taken show that the most of the Nordic countries address the effects of climate change on their region's security in specific policies and national security concepts. Moscow has sparked concerns in the West with displays of its will and capabilities—for example, flying strategic bomber patrols over the Arctic, or the hoisting the Russian flag on the sea bed below the North Pole. Despite a high degree of media awareness and intensive public discussions about spheres of influence and a possible return to classical geopolitics, both NATO and the EU try to avoid sending signals that would indicate that they regard regional security questions in the Arctic as a matter of deep concern or urgency. The motivation behind this article is to investigate this disconnect, to explain it, and to draw conclusions that argue for or against changes in the present posture. If their affected members states do not securitize the threats and vulnerabilities related to the melting polar ice cap in the High North within the organizations, NATO and the EU will lack the incentive and legitimacy to adapt their security policies and strategies in order to address the evolving situation.¹ Having said this, the question of the research

* Udo Michel joined the German Armed Forces in 1985. He served as Submarine Commanding Officer, Deputy Commander of a Submarine Squadron, and Commander of the German Submarine Training Center. His last post assignments were at NATO's Maritime Component Command Headquarter in the U.K. and within the German Ministry of Defense.

This paper was presented during the 25th International Training Course in Security Policy (ITC) conducted by the Geneva Centre for Security Policy. The views expressed in this paper are those of the author alone, and do not reflect any official statement or position of the German Ministry of Defense.

¹ Barry Buzan and Ole Wæver, *Regions and Powers: The Structure of International Security*, Cambridge Studies in International Relations 91 (Cambridge: Cambridge University Press, 2003), 491.

undertaken here is whether NATO and/or the EU are required to change their current security policies and concepts in order to address the challenges and risks imposed by the melting of the Arctic ice cap.

This essay is intended to foster an ongoing academic and public discussion on the security risks posed by global warming as well as to provide input to the strategic policy-shaping and decision-making process. Isolated aspects of Arctic geopolitics are frequently addressed within political circles, the media, and in scientific publications. Hundreds of documents and articles are publicly available that allow one to investigate the subject in all its details. Despite this tremendous amount of information, the research community admits that the picture remains incomplete. The gap in understanding Arctic security issues has been acknowledged by various academic institutions and individuals. For example, in 2008 the Norwegian Institute for Defense Studies (*Institutt for forsvarsstudier*, or IFS) assumed a lead role in a five-year research program that addresses security conflicts and cooperation in the High North from various perspectives.² The Stockholm International Peace Research Institute (SIPRI) launched a three-year project entitled “Managing Competition and Promoting Cooperation in the Arctic” that aims to identify and analyze the key political and security issues, political dynamics, main security challenges, and the future of existing security frameworks.³

No doubt, this essay cannot compete with the research currently being conducted by various security institutes. Nevertheless, it seeks to contribute to the overall discussion while focusing on short-term policy implications for NATO and the EU instead of advising long-term policies for the Arctic community. The facts and information presented are derived from a study of the relevant literature. The article does not constitute an attempt to chart a course for future studies. It makes the assumption that the environment in the High North will continue to alter dramatically, and that this will accompany a rise of new challenges and threats. Neither the exact extent of global warming nor the precise timeline for its environmental effects are of fundamental relevance in order to answer the research question at hand here. The fact that other actors responded to the Arctic melting process by implementing strategies for the promotion of their own interests in the High North provides enough incentive to ask, “*Quo vadis, NATO? Quo vadis, EU?*” In order to answer the research question, the article’s first section offers a closer look towards the High North, examining the expected changes in the region and their possible impact on security issues. The second chapter addresses the level of individual actor—national governments and

² “Geopolitics in the High North: Multiple Actors, Norwegian Interests,” The Fridtjof Nansen Institute (FNI); available at http://fni.no/doc&pdf/Geonor_digital.pdf.

³ “Managing Competition and Promoting Cooperation in the Arctic,” Stockholm International Peace Research Institute (SIPRI) (Stockholm, 2011); available at <http://www.sipri.org/research/security/arctic>.

consortia—and investigates their ideational presets, spheres of influence, expected gains and other interests, positions, security strategies, actions, areas and level of cooperation, as well as their degree of dependency. Current disputes over territorial claims and demands for access to natural resources have raised tensions and trigger fears that the West and Russia might fall back into rivalry and struggle for supremacy in the region. The next section brings the single actors together and investigates how cooperation, multi-lateralism, and dispute resolution work. It points out in which areas and to what extent policy coordination and collaboration among those actors take place and how the international legal system provides tools for solving territorial disputes. Having shown what the other actors do or intend to do, the essay turns toward NATO and the EU. The next section identifies the organizations' positions and roles, their current strategy, and the significance of Arctic security as proclaimed and as practically embedded. Overlaying NATO and the EU's security policies and strategies with the analysis offered in previous sections of the article, the last part of this paper culminates in the answer to the research questions. It points out the degree of pressure for NATO and the EU to alter decisions at the strategic level in order to address the challenges and risks imposed by a melting polar ice cap in the High North.

The term "security" is widely referred to in political statements, in public discussions, and in academic work. Security can be regarded as a "degree of protection" or as a "form of protection" against non-desirable influences or events.⁴ Security has two dimensions: "real" security and perceived security. Each analysis and categorization of security depends on ideas about the objects that are to be protected. To give some examples, the term "security" can be applied to individual human beings as well as to states, organizations, systems, companies, etc. With reference to the subject at hand, this essay predominantly addresses the level of states and international organizations, not that of individuals. The research concentrates on stabilities and instabilities in the world of international relations. Taking the concept of security with its two predominant views into account, this work selects a path between the narrow and the wide approach.⁵ It addresses the military, political, and economic security sectors, including energy security. For the sake of concision, and to avoid a fundamental discussion of where security starts and where it ends, the sectors of environmental and human security must remain outside the scope of this analysis. Therefore, challenges like the loss of biodiversity or food security will not be addressed. By doing so, this

⁴ "Security," en.wikipedia.org; available at <http://en.wikipedia.org/w/index.php?oldid=415830112>.

⁵ Graeme P. Herd and Pál Dunay, "International Security, Great Powers and World Order," in *Great Powers and Strategic Stability in the 21st Century: Competing Visions of the World Order*, ed. Graeme P. Herd (New York: Routledge, 2010), 10–11.

work acknowledges the argument as expressed by Stephen E. Sachs, that “there is a significant danger in defining security as including everything that’s good in life—or everything that’s considered ‘necessary’,” and that there “are many values that policymakers might pursue, but security is only one of them, and cannot encompass the whole.”⁶

A New Arctic in a Changing World

Environmental Changes in the High North

For more than a century, the Arctic and the Antarctic have attracted the attention of scientists and travelers from around the world. 2007–08 marked the third International Polar Year. Despite intensive research and a fundamental agreement between academics about the significance of the polar regions for the global climate system, scholars were not able to develop persuasive forecast models for the Arctic climate. Intensified survey activity has taken place in order to fill the gap. Under the auspices of the World Meteorological Organization (WMO), several programs aim to generate the required datasets, in order to improve our knowledge of causes and effects and to raise the quality of predictions.⁷

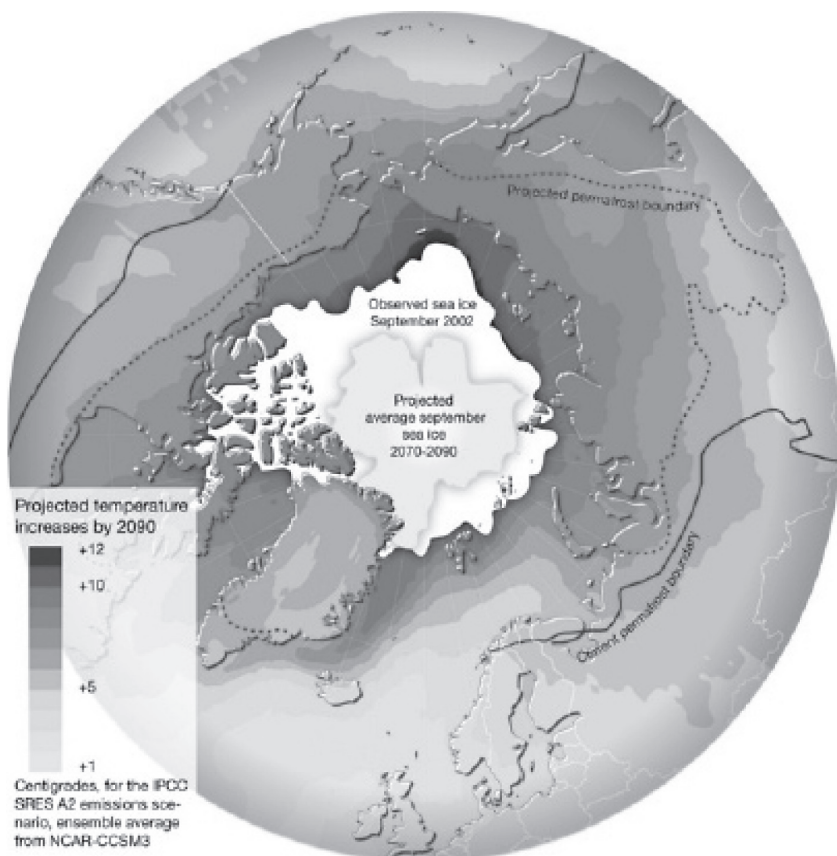
The polar regions are linked to the rest of the Earth’s climate system through atmospheric exchange and ocean circulation. The annual surface temperature across the globe is rising. Arctic temperature change is a complex phenomenon. In addition to the general increase in temperature, scientists have identified local hot spots. Areas with permafrost or seasonally frozen ground shrink, with immense outcomes for flora and fauna, land erosion, release of stored carbon dioxide and methane into the atmosphere, as well as implications for human activities, e.g. pipeline construction and maintenance. While Greenland’s ice sheet thins below an altitude of 1200 meters, it thickens above this level. In total, this leads to an increase of the country’s land ice mass. The maritime environment shows a different picture: “over the period 1978–1996, Arctic sea ice decreased by 2.8 percent per decade, or 34,300 km² per year. These reductions took place in all seasons and over the year as a whole, but the losses were greatest in the spring and smallest in the autumn. . . . Since the mid-1990s, there have been several years with record low summer-ice extents.”⁸

⁶ Stephen E. Sachs, “The Changing Definition of Security,” paper presented at Oxford University, Merton College, Department of International Relations, 2003; available at http://www.stevesachs.com/papers/paper_security.html.

⁷ World Meteorological Organization (WMO), *Polar meteorology. Understanding global impacts*, WMO-No. 1013 (Geneva: WMO, 2007).

⁸ Ibid.

Figure 1: Projected Temperature Increases in the Arctic Due to Climate Change, 2090⁹



⁹ UNEP/GRID-Arendal, Projected temperature increases in the Arctic due to climate change, 2090 (NCAR-CCM3, SRES A2 experiment), *UNEP/GRID-Arendal Maps and Graphics Library*; available at <http://maps.grida.no/go/graphic/projected-temperature-increases-in-the-arctic-due-to-climate-change-2090-ncar-ccm3-sres-a2-experiment>.

Frequently, the scientific community and the media inform the public about new forecasts of the rise of the global average temperature within the coming decades.¹⁰ The World Climate Research Program (WCRP) commented in a 2010 white paper on various models and studies. While admitting a certain degree of concern about the validity of today's predictions, the document underlines the fact that all simulations indicate a decrease of the Arctic sea ice cap, and that a number of studies even suggest that a total loss may occur in the early to mid-twenty-first century.¹¹ The Potsdam Institute for Climate Impact predicted in an article in 2010 "a predominantly ice-free Arctic Ocean in summer ... before the end of this century."¹² Many sources indicate that the Arctic sea ice melts down even faster than had been previously predicted,¹³ while few authors report contradictory results.¹⁴

"Climate change is a long-term process that will trigger a range of multi-dimensional demographic, economic, geopolitical, and national security issues with many unknowns and significant uncertainties."¹⁵ If the effects of climate change are regar-

-
- ¹⁰ Ola M. Johannessen and Martin W. Miles, "Critical Vulnerabilities of Marine and Sea Ice-based Ecosystems in the High Arctic," *Regional Environmental Change* 11, Supplement 1 (2011); available at <http://dx.doi.org/10.1007/s10113-010-0186-5>. World Meteorological Organization (WMO), WMO Statement on the Status of the Global Climate in 2009, WMO-No. 1055 (Geneva: WMO, 2010). David Shukman, "Four degrees of warming 'likely'," *BBC News* (28 September 2009); available at <http://news.bbc.co.uk/go/pr/fr/-/2/hi/science/nature/8279654.stm>.
- ¹¹ World Meteorological Organization (WMO), *Rapid Loss of Sea Ice in the Arctic*. Document JSC-31/Doc. 4.2/1 (1.2.2010), ed. Vladimir Kattsov et al., WMO/ICSU/IOC/World Climate Research Programme /Joint Scientific Committee (15–19 February 2010); available at http://www.wcrp-climate.org/jsc31/documents/jsc-31_clic_artic_4.2.pdf.
- ¹² Johannessen and Miles, "Critical Vulnerabilities," 1.
- ¹³ Jonathan Amos, "Arctic summers ice-free 'by 2013'," *BBC News* (12 December 2007); available at <http://news.bbc.co.uk/2/hi/science/nature/7139797.stm>. WMO, WMO Statement on the Status, 20. Scott G Borgerson, *The National Interest and the Law of the Sea*, Council on Foreign Relations Special Report 46 (New York: CFR, 2009), 32; available at http://www.ciaonet.org/pbei/cfr/0016458/f_0016458_14229.pdf. Richard Black, "Arctic sea ice melt 'even faster'," *BBC News* (18 June 2008); available at <http://news.bbc.co.uk/2/hi/science/nature/7461707.stm>. A. D. Romig, Jr., George A. Backus, and Arnold B. Baker, *A Deeper Look at Climate Change and National Security*, Sandia Report, SAND 2011-0039, (Albuquerque/Livermore: Sandia National Laboratories, March 2010), 8; available at https://cfwebprod.sandia.gov/cfdocs/CCIM/docs/Climate_Change_and_National_Security.pdf.
- ¹⁴ Richard Black, "Pause in Arctic's melting trend," *BBC News* (17 September 2009); available at <http://news.bbc.co.uk/go/pr/fr/-/2/hi/science/nature/8261953.stm>. "Competing Claims on the Arctic Circle," STRATFOR (24 September 2010); available at http://www.stratfor.com/graphic_of_the_day/20100924_competing_claims_arctic_circle.
- ¹⁵ Romig Jr., Backus, and Baker, *A Deeper Look at Climate Change*, 3.

ded as threats, the extent and the speed of the change determines the vulnerability of states and their populations as well, and the degree of negative impacts on them. In other words, climate change *per se* is neither purely good nor totally bad. Global warming in the High North offers certain chances for economic development, but it is also correlated with real and perceived risks.

Scientists conclude that the Copenhagen Accord is insufficient to prevent harm or loss in cases of disruption or damage to ecosystems, food production, economic development, and human cultures.¹⁶ The discussion about an acceptable level of human induced climate change goes beyond the scope of this work, as it addresses the problem of climate change on a global scale and not in the Arctic as a region in particular.

As previously stated, this article will not focus on the consequences of the predicted loss of Arctic sea-ice on ecosystems, maritime environment, food security, human rights, or human cultures. In order to address the central security concerns related to NATO and the EU, it concentrates on the issues of political and economic relations between key actors in the High North. The purpose of this essay is not to challenge the various scientific models that predict climate change in the Arctic region. In order to find an answer to the given research question, it seems to be sufficient to make the assumption that the observed melt-down tendency will continue, and that major parts of the Arctic Ocean will allow increased economic activities like enhanced fishery activities, exploration and exploitation of oil and gas deposits, as well as maritime transportation emerging along new sea lanes of communication (SLOC) that link the Atlantic and Pacific.¹⁷ The global economy depends on reliable transport routes. The oceans are the backbone for the long-range transport of mass goods. Vessels navigating along the Northwest Passage (north of Alaska and the Canadian mainland) might shorten their journey significantly in terms of distance and time compared to traditional seaways.¹⁸ Even the Northeast Passage appears to promise an advantage.

¹⁶ William L. Hare, Wolfgang Cramer, Michiel Schaeffer, Antonella Battaglini and Carlo C. Jaeger, "Climate Hotspots: Key Vulnerable Regions, Climate Change and Limits to Warming," *Regional Environmental Change* 11, Supplement 1 (2011); available at <http://dx.doi.org/10.1007/s10113-010-0195-4>.

¹⁷ Scott G. Borgerson. *The National Interest and the Law of the Sea*, 4. Romig Jr., Backus, and Baker, *A Deeper Look at Climate Change*, 15–18.

¹⁸ "For example, the distance from London to Tokyo via Panama is approximately 23,000 km. Through the Suez Canal it is approximately 21,000 km. Through northern Canada, it is approximately 16,000 km." Cleo Paskal, "How climate change is pushing the boundaries of security and foreign policy," Chatham House Briefing Paper, (London: Royal Institute of International Affairs, 2007), 6; available at http://consiglio.regione.emilia-romagna.it/biblioteca/pubblicazioni/MonitorEuropa/2007/Monitor_10/Dibattito/Clima_Politica_Estera.pdf.

This route tracks along the north of Russia, linking the North Atlantic Ocean with the Pacific Ocean. It is commonly referred to as the shortest seaway between Europe and the Pacific Ocean.¹⁹

Figure 2: Transport Routes in the High North²⁰



¹⁹ Johannesen and Miles, “Critical Vulnerabilities,” 8.

²⁰ “New Building Blocks in the North. The Next Step in the Government’s High North Strategy,” Norwegian Ministry of Foreign Affairs (Oslo/Tromsø: 12 March 2009), 52; available at http://www.regjeringen.no/upload/UD/Vedlegg/Nordområdene/new_building_blocks_in_the_north.pdf.

News headlines feed the perception that new sea routes through the Arctic are considerably cheaper, shorter, and faster than the traditional ones, and that these waters will be open for shipping soon. In consequence, many believe that a dramatic change in global trade patterns is on the horizon, with dramatic implications for other regions and other actors, such as merchant hubs like Singapore. Contemporary academic work takes the latest climate change forecasts into account and considers global economic trends. This draws a picture that deviates from widespread starry-eyed perceptions about near-future Arctic trade routes (see Figure 3 below). The major new findings are:

- Northern sea routes are not always the shortest ones between Europe and the Pacific
- Shipping in the High North will continue to struggle with sea ice, and therefore requires ice-strengthened ships
- Intra-Arctic shipping activities will expand continuously
- Northern transit routes will not become attractive for commercial shipping between the North Atlantic Ocean and the Pacific Ocean, especially not in the near future
- Most predictions indicate that the Northeast Passage will open sooner than the Northwest Passage.²¹

²¹ Svend Aage Christensen, "Are the northern sea routes really the shortest? Maybe a too rose-coloured picture of the blue Arctic Ocean," Danish Institute for International Studies (DIIS) Brief (March 2009), 2, 5; available at http://www.ciaonet.org/pbei/diis/0015955/f_0015955_13834.pdf.

Figure 3: Port Distances Along Alternative Sea Routes²²

Are the northern sea routes really the shortest?
Distance in km between harbours using various southern and northern routes

Route	Panama Canal	Northwest Passage	Northeast Passage	Suez and Malacca
London - Yokohama	23.300	15.930	13.841	21.200
Marseilles - Yokohama	24.030	16.720	17.954	17.800
Marseilles - Singapore	29.484	21.600	23.672	12.420
Marseilles - Shanghai	26.038	19.160	19.718	16.460
Rotterdam - Singapore	28.994	19.900	19.641	15.750
Rotterdam - Shanghai	25.588	17.570	15.793	19.550
Hamburg - Seattle	17.110	15.270	13.459	29.780
Rotterdam - Vancouver	16.350	14.330	13.445	28.400
Rotterdam - Los Angeles	14.490	15.790	15.252	29.750
Gioia Tauro (Italy) - Hongkong	25.934	24.071	21.556	14.093
Barcelona - Hongkong	25.044	23.179	20.686	14.693
New York - Shanghai	20.880	17.030	19.893	22.930
New York - Hongkong	21.260	18.140	20.982	21.570
New York - Singapore	23.580	20.310	23.121	18.770

Marginally longer route Shortest route

All numbers calculated by Frédéric Lasserre in SIG Mapinfo, except the numbers for the Northeast Passage through the Kara Strait south of Novaya Zemlya which have been calculated in Google Earth by Svend Aage Christensen.

Emerging Energy Demands

Following the notion that power “is the ability to attain the outcomes one wants, and the resources that produce it vary in the different contexts,”²³ it seems to be likely that further shortages and changes in allocations of scarce natural resources—e.g. fossil fuels—will spark enhanced competition between relevant actors, and that this might go along with the possibility of changes in the distribution of power on the regional and global scale.²⁴ The World Energy Outlook 2010 (WEO-2010) provides medium- to long-term energy projections. Using the latest version of the World Ener-

²² Ibid.

²³ Joseph S. Nye, Jr., “The Future of American Power: Dominance and Decline in Perspective,” *Foreign Affairs* 89:6 (November/December 2010): 2–13; available at <http://www.proquest.umi.com.ezproxy.by.edu>.

²⁴ Tomas Ries, “Global Warming,” in *Potential Global Strategic Catastrophes. Balancing Transnational Responsibilities and Burden-sharing with Sovereignty and Human Dignity*, ed. Nayef R.F. Al-Rodhan (Zürich/Berlin: LIT Verlag, 2009), 125.

gy Model (WEM), the International Energy Agency (IEA) differentiates between three scenarios in order to forecast corridors for energy-related trends²⁵ like future oil prices, the world's primary energy demand, the world oil production, coal-fired electricity generation, or renewable primary energy demand.²⁶ Keeping the probable location of unexplored hydrocarbon deposits in the Arctic in mind, the following key findings of the WEO-2010 should be noticed: "In the New Policies Scenario—the central scenario this year—world primary energy demand increases by 36% between 2008 and 2035, or 1.2% per year on average. ... Oil remains the dominant fuel in the primary energy mix to 2035. ... Natural gas is set to play a central role in meeting the world's energy needs for at least the next two and a half decades. ... Oil demand (excluding biofuels) continues to grow steadily in the New Policies Scenario, reaching about 99 million barrels per day by 2035—15 mb/d up on 2009."²⁷ With respect to the international community's attempt to limit the global average temperature rise, the WEO-2010 predicts, "The costs of getting on track to meet the climate goal for 2030 has risen by about \$1 trillion compared with the estimated costs in last year's Outlook. ... The timidity of current commitments has undoubtedly made it less likely that the 2°C goal will be achieved."²⁸ While predictions indicate a rising demand for energy due to the recovery of Western economies and the needs of emerging economic powers like China, India, or Brazil, the sustainable supply of fossil fuels might be threatened by political instability within producing regions and along transport routes. The Arctic offers an alternative to other energy regions. While the expected resources are of a significant scale, the volume of future oil and gas extraction in the High North remains a function of multiple variables and leaves us with a high level of uncertainty.

²⁵ International Energy Agency (IEA), "World Energy Model – Methodology And Assumptions," OECD/IEA (2010); available at http://www.worldenergyoutlook.org/docs/weo2010/World_Energy_Model.pdf. International Energy Agency (IEA). "World Energy Model," OECD/IEA, (2011), 3; available at <http://www.worldenergyoutlook.org/model.asp>.

²⁶ International Energy Agency (IEA), "World Energy Outlook 2010, Key Graphs," available at http://www.worldenergyoutlook.org/docs/weo2010/key_graphs.pdf. And IEA, "World Energy Outlook 2010, Presentation to the press" (9 November 2010); available at http://www.worldenergyoutlook.org/docs/weo2010/weo2010_london_nov9.pdf.

²⁷ International Energy Agency (IEA), "World Energy Outlook 2010 Factsheet, What does the global energy outlook to 2035 look like?" (2010); available at <http://www.worldenergyoutlook.org/docs/weo2010/factsheets.pdf>.

²⁸ International Energy Agency (IEA), "World Energy Outlook 2010 Factsheet," 6.

Figure 4: Probable Location of Unexplored Hydrocarbon Deposits in the Arctic²⁹



Arctic Actors

Russian Federation

Russia has faced rapid demographic and economic changes since the dissolution of the Soviet Union. Under Putin and Medvedev’s presidencies, Russia redesigned its political, military, and economic systems. In foreign relations, Moscow established a pragmatic strategy towards the West that combines confrontation in some cases and collaboration in others, while in parallel strengthening its ties with Asia. Currently the country has regained its self-assertiveness as a major power. From time to time this leads Moscow to emphasize its position by flexing its muscles in the High North.

²⁹ USGS Circum-Arctic Resource Appraisal, available at <http://energy.usgs.gov/arctic/>.

The country's economic health is less robust. Russia's unproductive and inefficient energy sector faced serious structural problems that had consistently been masked by high global demand. While large volumes of oil and gas were exported, the country has failed to reinvest in its required infrastructure and technology resources, as well as to create an efficient energy market.³⁰ Russia's economy remains highly dependent on oil and gas, while the nation's developed natural gas fields face exhaustion. Russia lacks flexibility to alter the direction of its energy exports (e.g., to the Far East). New pipeline systems and especially the application of liquefied natural gas (LNG) technology can provide an answer, but gas pipelines mean large investments, and Russian companies lack the capabilities for deepwater LNG production in extreme latitudes.³¹ This being said, there is good reason to challenge Russia's self-proclaimed status as an energy superpower. President Dmitry Medvedev analyzed the nation's deficits and concluded in his 2009 "Go Russia!" article: "In the next few decades Russia should become a country, the prosperity of which will depend not so much on raw materials but its intellectual resources...." Medvedev continued with the proclamation of strategic priorities, the first of which addresses the efficiency of production, transportation, and energy use as well as the development of new types of fuel.³² In order to streamline the energy sector and to improve its competitive position on the global markets, Russia requires access to capital and technology. So far, the Putin/Medvedev axis has rejected liberal-oriented political and economic solutions. Academics and policy makers try to forecast in which direction Russia's political system and its economy will develop over the coming years. In 2010, New York University published a "Russia 2020" scenario paper that described the following three options: Working Authoritarianism, Bottom-Up Liberalization and Modernization, and Degeneration.³³ The dividing lines between the scenarios are drawn by their predicted outcomes in terms of economic strength and political reform. Access to natural resources and commodity price levels have played a significant role in the past, and might con-

³⁰ J. Robinson West, "Talking Business Facts about Europe's Gas Problems," *European Affairs* 10:1 (2009). Adnan Vatansever, *Russia's Oil Exports. Economic Rationale Versus Strategic Gains*, Carnegie Papers, Energy and Climate Program 116, Carnegie Endowment for International Peace (December 2010); available at http://www.carnegieendowment.org/files/russia_oil_exports.pdf; Vatansever, "A Russian Solution to Europe's Energy Problem," Carnegie Endowment for International Peace (10 January 2011); available at <http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=42258>.

³¹ "Norway: A New LNG Player," STRATFOR (31 July 2008); available at http://www.stratfor.com/analysis/norway_new_lng_player.

³² Dmitry Medvedev, "Go Russia!" RT.com (11 September 2009); available at <http://rt.com/politics/official-word/dmitry-medvedev-program-document/print/>.

³³ New York University, *Russia 2020* (New York: New York University / School of Continuing and Professional Studies / Center for Global Affairs, Spring 2010); available at <http://www.scps.nyu.edu/export/sites/scps/pdf/global-affairs/russia-2020-scenarios.pdf>.

tinue to do so in the future. The present authoritarian Putin/Medvedev regime relies heavily on an omnipresent security apparatus and on the promise to care for the basic needs of the population. Both depend on revenues from oil and gas. In this context, the assumption can be made that Russia's ongoing exploration and exploitation of its natural resources in the Arctic holds high importance for the government as a means to access foreign capital and technology in order to ensure continued economic growth while avoiding internal pressure for political liberalization (see Figure 5). In other words, an early utilization of Arctic resources on a large scale would help the Kremlin to decouple economic and social challenges from liberal-oriented political reforms. And circumstances continue to maneuver the country in a favorable direction: "Russia would seem to be the likely hub of global economic expansion as the Arctic becomes economically accessible. With a border that spans over 160 degrees of the Arctic region, its side of the Arctic is opening to exploration faster than the North American/European side."³⁴

³⁴ Romig Jr., Backus, and Baker, *A Deeper Look at Climate Change*, 17.

Figure 5: Potential and Known Arctic Oil and Gas Deposits and Mines³⁵

During recent years, Moscow's main priorities for the Arctic were the accelerated exploration and exploitation of oil and gas deposits, expansion of the Exclusive Economic Zone, increased international cooperation in environmental protection, and a demonstration of military power.³⁶ As Pavel Baev writes, "By 2010, serious problems had emerged in all four of these areas, which can only partly be blamed on the global economic crisis."

What does this mean for the way the Russian Federation pursues its interests in the Arctic? Some years before, Moscow sparked concerns about a return of the Cold War pattern of relations when it emphasized its will to defend Russian citizens and business interests abroad and proclaimed its renewed sphere of influence. Following Russia's 2008 conflict with Georgia, Medvedev highlighted regions where Russia

³⁵ Finnish Prime Minister's Office, "Finland's Strategy for the Arctic Region," Prime Minister's Office Publications 8/2010 (Helsinki: Prime Minister's Office, 5 July 2010), 73; available at <http://www.geopoliticsnorth.org/images/stories/attachments/Finland.pdf>.

³⁶ Dmitri Trenin and Pavel K. Baev, *The Arctic: A View From Moscow*, (Washington, D.C.: Carnegie Endowment for International Peace, 2010), 27; available at http://carnegieendowment.org/files/arctic_cooperation.pdf.

has “privileged interests.”³⁷ Although he made no direct reference to the Arctic at that time, it should be understood that the High North—inside and outside its territorial borders—plays such a role.

Nevertheless, the Russian government was forced to acknowledge political, economic and military realities. Moscow altered its posture towards the West, as expressed by Foreign Minister Lavrov: “Finally, we all should step over ourselves and stop the unnecessary talk about ‘veto power outside the UN Security Council, about ‘spheres of influence’ and the like. We can very well do without all that, as there are more important things where we undoubtedly have common interests.”³⁸ Russia’s 2010 Military Doctrine avoids any reference to threats arising from the Arctic. Baev draws the following conclusion in his analysis of Moscow’s Arctic Policy: “Russia has reevaluated the risks of geopolitical competition in the Far North and now prefers a pattern of balanced cooperative behavior, as exemplified by the maritime border agreement with Norway.”³⁹ Despite this, it should be noted that Russia will continue to assert a visible military presence in the High North⁴⁰ and to use Arctic waters as a relative safe area to deploy its seaborne nuclear deterrence capabilities.⁴¹

This being said, the overall conclusion is that Russia’s interests in the Arctic are predominantly of an economic nature, and that the country applies an approach of pragmatic cooperation with foreign governments and non-governmental partners in order to gain its desired goals. This offers great potential for foreign companies to benefit from broader cooperation with Russia, even though Moscow’s authoritarian regime and previous setbacks leave investors with some uncertainty.⁴²

³⁷ Andrew E. Kramer, “Russia Claims its Sphere of Influence in the World,” *New York Times* (1 September 2008); available at http://www.nytimes.com/2008/09/01/world/europe/01russia.html?_r=1&pagewanted.

³⁸ Sergei Lavrov, “Russia and the World in the 21st Century,” *Russia in Global Affairs* 6:3 (2008): 17; available at http://kms1.isn.ethz.ch/serviceengine/Files/ISN/96338/ichapter-section_singledocument/C2DAF5EF-6CA0-4A57-8ABA-D1A2E73E1334/en/1.pdf.

³⁹ Pavel K. Baev, “Russia’s Arctic Policy: Geopolitics, Merchantilism and Identity-Building,” *Finnish Institute of International Affairs Briefing Paper No. 73* (2010); available at <http://www.upi-fiia.fi/fi/publication/162/>.

⁴⁰ “Russia: Aviation Brigade To Be Stationed In Alakurtti,” *STRATFOR* (1 October 2010); available at http://www.stratfor.com/sitrep/20101001_russia_aviation_brigade_be_stationed_alakurtti.

⁴¹ “Russia: Navy To Continue Arctic Nuclear Submarine Patrols,” *STRATFOR* (1 October 2010); available at http://www.stratfor.com/sitrep/20101001_russia_navy_continue_arctic_nuclear_submarine_patrols.

⁴² “Russia, U.K.: Lavrov and Miliband Play the ‘Great Game’,” *STRATFOR* (2 November 2009); available at http://www.stratfor.com/memberships/148198/analysis/20091102_russia_uk_lavrov_and_miliband_play_great_game.

Medvedev's "Go Russia!" slogan has already produced some outcomes: in January 2011, the international oil company BP and the national Russian oil company Rosneft announced the formation of a strategic global alliance. Their collaboration had started in 1998. Now, both companies had agreed to exchange share packages, to develop licensed oil field blocks in the South Kara Sea, to establish an Arctic technology center in Russia, and to continue their joint technical studies.⁴³

The United States

Until the end of the Cold War, the Arctic played an important role within U.S. politics. Since then, Washington's administrations lost much of their interest in the region. Forecasted environmental changes, the re-consolidation of the Russian Federation as a major power, and the rise of China and other emerging powers combined with a new approach to foreign and security policy followed by President Obama's administration bear high potential that the U.S. will reexamine its attitudes towards the High North. Indeed, "The U.S. National Security Council is now preparing a review of the U.S. policy in the Arctic, and that might lead to a reappraisal of U.S. interests in the region."⁴⁴

The Arctic region serves an important role for the U.S. in pursuing its national interests, namely security, wealth, economic growth, and power.⁴⁵ Therefore, it is in the country's interest to limit the maritime influence and the claims of other coastal states while at the same time enlarging its own legal and economic position.⁴⁶ Having said this, it appears perfectly logical to argue that the U.S. harms and marginalizes itself through its ongoing resistance to become a party of UNCLOS.⁴⁷ Limiting the argument to the matter of secured access to natural resources, one can also argue directly in the opposite direction. Despite its enormous demand for energy, the U.S. is far from facing any threatening shortage in fossil fuel supply. The country possesses more coal than any other state in the world, and coal presently covers more than half of the

⁴³ BP plc Press Release, "Rosneft and BP Form Global and Arctic Strategic Alliance," 14 January 2011; available at <http://www.bp.com/genericarticle.do?categoryId=2012968&contentId=7066710>. Tony Hayward, "Russia and the Energy World – Challenges of a new decade," speech at the Academy of National Economy, Moscow, 21 January 2010; available at <http://www.bp.com/genericarticle.do?categoryId=98&contentId=7059344>.

⁴⁴ "Geopolitics in the High North. Multiple Actors. Norwegian Interests," Work Package 3 Description.

⁴⁵ Scott G. Borgerson, "Arctic Meltdown: The Economic and Security Implications of Global Warming," *Foreign Affairs* 87:2 (2008): 63–77; available at <http://www.ciaonet.org/journals/fa/v87i2/0000814.pdf>.

⁴⁶ Borgerson. *The National Interest and the Law of the Sea*, 9–10.

⁴⁷ Scott G. Borgerson. "Arctic Meltdown"; Borgerson, *The National Interest and the Law of the Sea*, 22 and 33–35.

nation's electric power generation. In addition, the U.S. has considerable amounts of natural gas at its disposal. Crude oil is imported into the U.S. to a larger extent than necessary. The U.S. is blessed with the world's largest known oil shale deposits. The RAND Corporation estimates this reservoir at "between 500 billion and 1.1 trillion barrels of useful fuels. The mid-point of this range is 800 million barrels, which is more than triple the oil reserves of Saudi Arabia."⁴⁸ Until now, oil shale resources play a minor role in the U.S. energy sector, but private business shows interest and willingness to move toward utilizing this energy source.⁴⁹ On top of this, the U.S. is (according to some estimates) believed to possess methane hydrate resources on a tremendous scale, meaning that the country could run for "thousands of years" on these supplies.⁵⁰ In this respect, the Arctic Ocean and possible U.S. claims on its continental shelf attracts attention. But so far neither the exact potential of these deposits has been determined, nor has the technology to utilize them been developed, nor has their economic viability been assessed. To shorten a long story, unless the U.S. does not commit itself to a significant reduction of greenhouse gas emission levels, there is no pressure to alter its given energy mix and to increase its use of less problematic forms of fossil fuels and/or forms of renewable energy. The U.S. will secure its claims against others in the Arctic, but so far they are not being challenged, and from the perspective of energy security there is no need for Washington to rush to the High North.

Canada

As Canada's 2009 Northern Strategy emphasizes, the Arctic plays a central role for the nation: "The North is a fundamental part of our heritage and our national identity, and it is vital to our future."⁵¹ Despite this claim, Canadian security planners lost their focus on the region after the Cold War. Over the last decade, the topic of Arctic security has regained a high place on the political agenda in the media. Huebert identifies four driving factors for this: post-9/11 perceptions of terrorist threats; improved accessibility of the region caused by climate change; increased exploration and exploitation of the Arctic's natural resources; and a revived public interest in

⁴⁸ James T. Bartis. "Research Priorities for Fossil Fuels," testimony presented before the Senate Energy and Natural Resources Committee on 5 March 2009 (Santa Monica, CA: RAND Corporation, Publication CT-319, March 2003), 5; available at http://www.rand.org/content/dam/rand/pubs/testimonies/2009/RAND_CT319.pdf.

⁴⁹ *Ibid.*, 6.

⁵⁰ *Ibid.*, 4.

⁵¹ Government of Canada, *Canada's Northern Strategy Abroad*, 2010; available at http://www.international.gc.ca/polar-polaire/assets/pdfs/CAFP_booklet-PECA_livret-eng.pdf.

Arctic sovereignty and security issues.⁵² Canada's Northern Strategy determines four priority areas in order to address the region: sovereignty, social and economic development, environmental protection, and governance. In terms of military and law enforcement issues, Canada has to reinvent and reinforce its Arctic capacities: "There has been significant discussion and study of the twin issues of Arctic sovereignty and security. The emerging consensus is that there is a need to improve both surveillance and enforcement capabilities for northern operations. There is also agreement that the Canadian Forces in general and the navy specifically need to relearn how to have a greater significance in the Arctic."⁵³

Canadians have a tradition of cooperation in the High North, especially with its Allied partners in terms of security. In 2010, Denmark and Canada signed a "Memorandum of Understanding on Arctic Defense, Security, and Operational Cooperation" in order to promote enhanced collaboration.⁵⁴ Several weeks later, the government released a statement on its Arctic Foreign Policy, which is the international dimension of the northern strategy. Ottawa named the U.S. as its "premier partner in the Arctic" and committed itself to closer international cooperation, especially with Russia, Norway, Denmark, Sweden, Finland, and Iceland.⁵⁵ Progress on outstanding boundary issues has been given the highest priority.⁵⁶

Norway

In general, Norway prosecutes the following interests in the Arctic: Protection of national sovereignty, jurisdiction and exclusive rights; stability and low tension; economic growth; sustainable resource management; energy security; environmental concerns and climate change; managing the relationship with Russia; and involving Western countries.⁵⁷

⁵² Rob Huebert, "Renaissance in Canadian Arctic Security?" *Canadian Military Journal* (Winter 2005–2006): 27.

⁵³ Rob Huebert, "Canadian Arctic Maritime Security: the Return to Canada's Third Ocean," *Canadian Military Journal* (Summer 2007): 9–16.

⁵⁴ Government of Canada, "Canada And Denmark Sign Arctic Cooperation Arrangement," Press Release (14 May 2010), NR-10.042; available at <http://www.forces.gc.ca/site/news-nouvelles/news-nouvelles-eng.asp?cat=00&id=3376>.

⁵⁵ Government of Canada, Statement on Canada's Arctic Foreign Policy. Exercising Sovereignty and Promoting Canada's Northern Strategy Abroad (Ottawa, 2010), 25; available at http://www.international.gc.ca/polar-polaire/assets/pdfs/CAFP_booklet-PECA_livret-eng.pdf.

⁵⁶ Government of Canada, "Address by Minister Cannon at Launch of Statement on Canada's Arctic Foreign Policy," Press Release (20 August 2010), No. 2010/57; available at <http://www.international.gc.ca/media/aff/speeches-discours/2010/2010-057.aspx?lang=eng>.

⁵⁷ "Geopolitics in the High North: Multiple Actors, Norwegian Interests," Work Package 8 Description.

With its 2006 High North Strategy, the Norwegian Government addressed the region as “the most important strategic priority area in the years ahead” and initiated a whole-government approach for developing the region.⁵⁸ Seven priority areas were formulated, and twenty-two specific action items set in place. The 2009 strategy update reviewed the process and confirmed the increased activity and presence as well as sustainable economic and social development in the High North.⁵⁹ The underlying assumption for the Norwegian government’s policy is that the country should avoid isolation, and should instead pursue far-reaching partnerships: “Strengthened international cooperation in the north—both circumpolar cooperation and cooperation with Russia in particular—will in turn be beneficial for development in Northern Norway.”⁶⁰ In terms of foreign policy, this means that the relationship between Moscow and Oslo is the key to success. Norway has particular interests in solving the issues involving the maritime delimitation line with Russia, in overcoming both countries’ controversies concerning the Svalbard Treaty, and in achieving a positive decision in view of the outer limits of the Norwegian continental shelf.⁶¹ Besides bi- and multilateral relations, the High North Strategy highlights the areas of knowledge development, surveillance, emergency response, maritime safety, offshore and onshore business development, infrastructure, sovereignty, and safeguards for the indigenous people.

While Norway seeks close international cooperation, the country still resists joining the EU. In the wake of the Greek economic crisis, domestic support for EU membership dropped significantly, to 30.6 percent of the population in March 2010.⁶² For the foreseeable future, the EU seems to be a welcome partner for the Norwegians, but does not represent a comfortable home. Therefore, it is less likely that the EU area of responsibility will enlarge in a way that would allow it to directly border Arctic waters. In conclusion, the Norwegian absence from the EU will—at least *per forma*—restrict the Union’s ability to exercise significant influence in the region.

Good political relations and advanced technology make Norwegian companies a

⁵⁸ The Norwegian Government’s High North Strategy (Oslo/Tromsø: Norwegian Ministry of Foreign Affairs, 1 December 2006), 7; available at <http://www.regjeringen.no/upload/UD/Vedlegg/strategien.pdf>.

⁵⁹ New Building Blocks in the North. The next Step in the Government’s High North Strategy, (Oslo/Tromsø: Norwegian Ministry of Foreign Affairs, 12 March 2009), 3; available at http://www.regjeringen.no/upload/UD/Vedlegg/Nordområdene/new_building_blocks_in_the_north.pdf.

⁶⁰ *Ibid.*, 7.

⁶¹ “Geopolitics in the High North: Multiple Actors, Norwegian Interests,” Work Package 1 Description.

⁶² “Brief: Most Norwegians Against EU Membership,” STRATFOR (23 March 2010); available at http://www.stratfor.com/sitrep/20100323_brief_most_norwegians_against_eu_membership.

strong player when it comes to the exploitation of natural resources in the High North. For example, Norway's Statoil company currently operates in thirty-four countries.⁶³ Its first trade ties to Russia were established in the 1950s, and its presence in Russia proper reaches back to 1988. In the last couple of years, StatoilHydro developed a technology for LNG production in deep waters and extreme latitudes.⁶⁴ This "almost unparalleled know-how" makes the enterprise a welcomed partner, especially for Russia.⁶⁵ The LNG technology provides flexibility in energy transport and bears the potential to divert gas flows from given pipeline routes. Therefore, a boom in LNG can affect regional and global patterns of energy distribution. Consequently, Russian Gazprom awarded StatoilHydro the final stake in the Shtokman far-north deepwater natural gas field project that is located in the Russian sector of the Barents Sea. In addition to the Shtokman project, Statoil is also engaged in the Kharyaga field exploitation. Statoil states, "Russia is regarded as an important core area for Statoil's international investments," but cooperation is not restricted to Russia itself. Statoil cooperates for example with Russia's Lukoil in Iraq.⁶⁶

Denmark and Greenland

Denmark is involved in changing geopolitics in the High North via Greenland, which is a Danish territory. When the Scandinavian state joined the European Community in 1973, Greenland was included, but the territory left in 1985. Today Denmark is a member of the European Union, while the Danish territories of Greenland and the Faeroe Islands are not. In 2006 the Danish government and Greenland's representatives decided to develop a coherent strategy for the Arctic. The core idea behind this step was to support and strengthen the development of Greenland towards increased autonomy, and to maintain the Greenlandic-Danish position as a major player in the Arctic. While the major focus seemed to be placed on environmental issues and on preparation for the Danish Presidency of the Arctic Council (2009–11), the original tasking also pointed to some issues of primary concern: the Northwest

⁶³ "Statoil in brief," Statoil, published 28 October 2009, updated 18 January 2011; available at <http://www.statoil.com/en/about/inbrief/pages/default.aspx>.

⁶⁴ "Snøhvit—Unlocking resources in the frozen North," Statoil (12 October 2009, updated 23 November 2009); available at <http://www.statoil.com/en/OurOperations/ExplorationProd/ncs/Pages/SnohvitNewEnergyHistoryInTheNorth.aspx>. "Snøhvit," Statoil (2 September 2007, updated 22 November 2009); available at <http://www.statoil.com/en/ouoperations/explorationprod/ncs/snoehvit/pages/default.aspx>.

⁶⁵ "Norway: A New LNG Player," STRATFOR (31 July 2008); available at http://www.stratfor.com/analysis/norway_new_lng_player.

⁶⁶ "International exploration and production," Statoil, 2010; available at <http://www.statoil.com/en/ouoperations/explorationprod/internationalfields/pages/default.aspx>.

Passage, globalization and trade, and the continental shelf.⁶⁷ (The question about the legal status of the passage will be highlighted elsewhere in this article.) The question of whether or not the Northwest Passage constitutes an “international strait” is important for Greenland because its Western coasts form a part of it.

After the Danish state had granted home rule to Greenland in 1979, the Siumut Party ruled the territory for thirty years. The 2009 elections resulted in a power shift. For the first time, the left-wing opposition achieved a majority. In the same year Greenland achieved expanded autonomy from Denmark. Analysts conclude that the changing situation in Greenland “opens the possibility of competition for influence over the world’s largest island by other Arctic powers.”⁶⁸ Greenland depends on cooperation with external partners in order to access its natural resources. The territory’s main political parties aim for full independence from Denmark, at least in the long term. So far, the island’s foreign policy continues to be determined by Copenhagen. Nevertheless, by going into practical details, one can also argue in the opposite direction, namely that “Greenland has taken over element after element of its foreign politics.”⁶⁹ Two factors should be kept in mind when looking at the security impacts of global warming. First, enhanced economic cooperation bears potential for Greenland to increase its sustainability and therefore to promote its independence from Denmark. Second, the island continues to play a significant role in military strategic planning, especially for the North American Defense Perimeter.

Iceland, Finland, and Sweden

Iceland, Sweden, and Finland do not border the Arctic Ocean, but they are member states of the Arctic Council. All three states have significant interests in what happens in the Arctic seas because of its geographic proximity to their territory. In the wake of the global financial crisis and the collapse of its banking system, Iceland raised much attention by its search for “new friends.”⁷⁰ First, Prime Minister Geir Haarde confirmed the country’s application for a USD 5.43 billion loan from the

⁶⁷ Naalakkersuisut Allattoqarfiat, Landsstyrets Sekretariat (Greenland Cabinet Secretariat), “Fælles arktisk strategi mellem Hjemmestyret og Rigsmyndighederne,” File No. 09.16-03, 15 May 2008; available at www.nanoq.gl.

⁶⁸ “Greenland: An Opposition Victory and the Competition for the Arctic,” STRATFOR (3 June 2009); available at http://www.stratfor.com/analysis/20090603_greenland_opposition_victory_and_competition_arctic.

⁶⁹ Jans Kaalhaug Nielsen, “Greenland’s geopolitical reality and its political-economic consequences,” DUPI Working Paper No. 2001/6, 4; available at <http://www.ciaonet.org/wps/nij01/nij01.pdf>.

⁷⁰ “Iceland: Financial Crisis and a Russian Loan,” STRATFOR (7 October 2008); available at http://www.stratfor.com/analysis/20081007_iceland_financial_crisis_and_russian_loan. “Iceland: Strategic Air Base for Sale?” STRATFOR (12 November 2008); available at http://www.stratfor.com/analysis/20081112_iceland_strategic_air_base_sale.

Russian government.⁷¹ Then, Icelandic President Olafur Ragnar Grimsson shocked Iceland's allies with the idea to offer Russia the former U.S. air base at Keflavik.⁷² To complete the surprise, the President decided also to approach the Chinese government and seek help. Beijing took the occasion, and strengthened its ties with Reykjavik.⁷³ Until 2008 Iceland presented itself as a perfect EU candidate with a small population, political stability, a member of the European Free Trade Association, and party to the Schengen Agreement.⁷⁴ After being elected in 2009, the new Prime Minister Jahan-na Sigurdardottir continued the push for EU membership.⁷⁵ Nevertheless, since that time the island's population has fallen into skepticism regarding the EU, mainly over the issues of protected fishing grounds, whale hunting, and losing political influence within a larger body. In parallel, critical voices from some EU member states arose that rejected the idea of a fast track accession for Iceland. To make a long story short, currently it seems less likely that Iceland will enter the EU within the coming years. Iceland does not have any territorial claims on the Arctic Ocean, but it follows the developments there very closely.

Finland's cultural identity is fundamentally influenced by its geographic location. The territory extends far across the Arctic Circle, but it does not border the Arctic Ocean. The country acquired unique know-how and gathered great expertise in coping with extreme conditions in the High North. The constitution guarantees protection for the country's Arctic indigenous people, the Sámi. "Out of the eight Arctic countries, Finland was seventh to draft an Arctic strategy,"⁷⁶ which was released in mid-2010.⁷⁷ The core message of the document is that Helsinki strongly

⁷¹ "Iceland: Financial Crisis and a Russian Loan." "Geopolitical Diary: A Russian Financial Power Play in Iceland," STRATFOR (8 October 2008); available at http://www.stratfor.com/geopolitical_diary/20081007_geopolitical_diary_russian_financial_power_play_iceland.

⁷² "Iceland: Strategic Air Base for Sale?"

⁷³ Natalia Makarova, "China Seeks Piece of Arctic Pie," *RT.com* (8 October 2010); available at <http://rt.com/politics/arctic-region-china-vysotsky/>.

⁷⁴ "Iceland: The Road to EU Accession Gets Rocky," STRATFOR (15 October 2008); available at http://www.stratfor.com/analysis/20090801_iceland_road_eu_accession_gets_rocky.

⁷⁵ "Iceland: The Push for EU Membership" STRATFOR (27 April 2009); available at http://www.stratfor.com/analysis/20090427_iceland_push_eu_membership.

⁷⁶ Hannu Halinen, "Finland's Arctic Strategy," presentation given at the conference "Finland's Arctic Strategy and the EU" at the Finnish Institute of International Affairs, Helsinki, 25 August 2010; available at http://www.upi-fiia.fi/assets/events/Halinen_Finlands_Arctic_Strategy.pdf.

⁷⁷ Finnish Prime Minister's Office, "Finland's Strategy for the Arctic Region," Prime Minister's Office Publications 8/2010 (Helsinki: Prime Minister's Office, 5 July 2010); available at <http://www.geopoliticsnorth.org/images/stories/attachments/Finland.pdf>.

advocates the protection of the Arctic environment, and that it seeks to benefit from emerging economic opportunities in the region. The strategy emphasizes external relations, and is intended to promote Finland's interests within the EU. While Finland has no territorial claims regarding the continental shelf in the Arctic Ocean, it regards itself as being indirectly affected by the respective disputes between other states.

Sweden is another Scandinavian country that does not border the Arctic Ocean. It is an Arctic country, but only a small fraction of its population lives in the High North.⁷⁸ As demonstrated during its last EU Presidency, Sweden is an active member of the European Union, and consequently uses its bodies to pursue its ideas and interests. However, Sweden does not have an articulated policy regarding the Arctic.

Emerging Asia

China is far from being an Arctic country, but within recent years it has demonstrated significant interest in the polar regions. In 2008, representatives of Canada's aboriginal communities visited Beijing at the invitation of the Chinese Communist Party. On this occasion, the delegation expressed its ambition to establish broad business ties with China around the future exploitation of the natural resources controlled by their people.⁷⁹ Recently, a Chinese Rear Admiral as quoted as follows: "The Arctic belongs to all the people around the world, as no nation has sovereignty over it."⁸⁰ Both events underline concerns about China's future influence in the Arctic, at least in Washington and Ottawa. In practice, the Chinese outreach to the High North is characterized by the pursuit of economic interests. In preparation for this, China has undertaken academic research on the Arctic, including some studies in cooperation with Norway. China opened its first Arctic research station in 2004. In 2010, the icebreaker *Zuelong* deployed for China's longest Arctic expedition in history. The vessel had already conducted twenty-four research expeditions to the Antarctic, but only three to the Arctic. This relation is most likely to change: "China now recognizes the commercial and strategic opportunities that will arise from an ice-free Arctic."⁸¹

⁷⁸ "The Geopolitics of Sweden: A Baltic Power Reborn," STRATFOR (30 June 2009); available at http://www.stratfor.com/analysis/20090629_geopolitics_sweden_baltic_power_reborn.

⁷⁹ Cleo Paskal, "Redrawing The Map," *The Journal of International Security Affairs* 18 (2010): 93; available at http://www.ciaonet.org/journals/jisa/v0i18/f_0018657_15979.pdf.

⁸⁰ Gordon G. Chang, "China's Arctic Play," *The Diplomat* (9 March 2010); available at <http://the-diplomat.com/2010/03/09/china%e2%80%99s-arctic-play/>.

⁸¹ Trude Pettersen, "China to Boost Arctic Research," *The Barents Observer* (6 May 2010); available at <http://www.barentsobserver.com/china-to-boost-arctic-research.4781463.html>.

Consequently, the Norwegian Foreign Minister Jonas Gahr Støre proposed China as an observer to the Arctic Council.

The Russian government and Russian companies are the preferred partners for the Chinese. Beijing is strongly interested in the development of the Northern Sea Route and in joint LNG projects.⁸² Recently, Sovcomflot—a Russian firm that is the leading shipping operator along the Northern Sea Route—signed a cooperation agreement with a Chinese company in order to increase the volume of Chinese goods it would transport. In early 2011, the Chinese National Offshore Oil Company (CNOOC) won the tender for the Pechora LNG plant project, and was chosen by the Russian company Allteck to join the project with a larger stake.⁸³ While CNOOC aims for gas, another large player, the China National Petroleum Corp (CNPC), is seeking a substantial share in the exploitation of Russian oil reserves.⁸⁴

China is not the only Asian country that longs for increased economic influence in the High North, but at first glance it appears to be Russia's preferred partner. Nevertheless, Jean-Marie Holzinger has identified some arguments against the rapid development of a Russo-Chinese strategic energy partnership, namely Russia's own energy needs, Europe's attractiveness as high-price market, China's interest in independence from Russia, Sino-Russian competition in other areas, Russian concerns about China's ambitions as an emerging power, and Russian advances toward Japan and South Korea.⁸⁵ Further competition for Chinese and Western companies comes for example from India (with its state-run oil and gas company ONGC),⁸⁶ and from Vietnam (with PetroVietnam).⁸⁷

⁸² Trude Pettersen, "Chinese Interest Towards Northern Sea Route," *The Barents Observer* (6 April 2011); available at <http://barentsobserver.custompublish.com/chinese-interest-towards-northern-sea-route.4907565-16149.html>.

⁸³ Atle Staalesen, "Pechora LNG from Year 2015," *The Barents Observer* (24 August 2010); available at <http://barentsobserver.custompublish.com/index.php?id=4811601>. Trude Pettersen, "China to Invest in Pechora LNG," *The Barents Observer* (29 March 2011); available at <http://barentsobserver.custompublish.com/china-to-invest-in-pechora-lng.4903454-16149.html>.

⁸⁴ Katya Golubkova and Jessica Bachman, "India in the Tuning for Russia's Arctic Oil," *Fox Business* (21 September 2010); available at <http://www.foxbusiness.com/markets/2010/09/21/india-running-russias-arctic-oil/>. Richard Weitz, "Chinese Pipe Dreams," *The Diplomat* (3 January 2011); available at <http://the-diplomat.com/2011/01/03/chinese-pipe-dreams/>.

⁸⁵ Jean-Marie Holtzinger, "The Russo-Chinese Strategic Partnership: Oil and Gas Dimensions," *Connections—The Quarterly Journal* 9:4 (2010): 69–82; available at <https://www.pfpconsortium.org/file/3920/view>

⁸⁶ Golubkova and Bachman, "India in the Tuning for Russia's Arctic Oil."

⁸⁷ Atle Staalesen, "Pechora LNG from year 2015"; Trude Pettersen, "China to invest in Pechora LNG."

Conflicts, Competition, and Cooperation

The Law of the Sea

The 1982 United Nations Convention on the Law of the Sea (UNCLOS) is the product of a long-lasting process that culminated in three United Nations Conferences on the Law of the Sea (1958, 1960, and 1973–82). The agreement aims to establish “a legal order for the seas and oceans which will facilitate international communication, and will promote the peaceful uses of the seas and oceans, the equitable and efficient utilization of their resources, the conservation of their living resources, and the study, protection, and preservation of the marine environment.”⁸⁸ All Arctic states (except for the U.S.), all EU member states, and the EU itself are parties to the convention. As of today, 156 states and the European Union have signed and ratified the treaty.

UNCLOS represents the centerpiece of international governance of the seas. Therefore, the convention organizes the space of the sea—including its bed, its subsoil, and the airspace above—by precise distinctions between certain types of zones, universal definitions of their outer limits, comprehensive determinations of their legal status, as well as detailed specifications of the freedom, rights, and obligations of all parties. The convention serves two major purposes. First, it stipulates a legal framework for the parties (states) to define their mutual relations within the given zones in view of the use the sea and the utilization of it. Second, it provides legitimacy as well as instruments and procedures for the settlement of claims and disputes.

UNCLOS acknowledges the freedom of the seas, and transfers international customary law into international treaty law. Movement of vessels is guaranteed through a variety of mechanisms, including the right of innocent passage in the territorial sea, the right of transit passage through straits used for international navigation between one part of the high seas or an exclusive economic zone and another part of the high seas or an exclusive economic zone, and the right of archipelagic sea lanes passage. The convention guarantees the immunity of warships and ships used only in non-commercial government service. It establishes rules for various kinds of human activities related to the sea, such as research and surveys; enforcement of laws and regulations (e.g. countering piracy); interception of transport of slaves; fighting against the illicit traffic in narcotic drugs or psychotropic substances; construction of artificial islands; installations; tunneling; utilization of living resources, including execution of traditional fishing rights; offshore drilling; exploitation of non-living resources; laying of submarine cables and pipelines on the continental shelf; and

⁸⁸ United Nations Convention on the Law of the Sea (UNCLOS), 25 (Preamble); available at http://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

protection of human life and of the environment. The convention sets general provisions for the settlement of disputes by imposing the obligation to settle disputes by peaceful means. Melting ice constitutes a prerequisite for improved access to the High North, which is the key to the realization of economic opportunities in the area such as the utilization of living resources, the exploitation of non-living resources, or the establishment of new shipping lanes.

The Northwest Passage

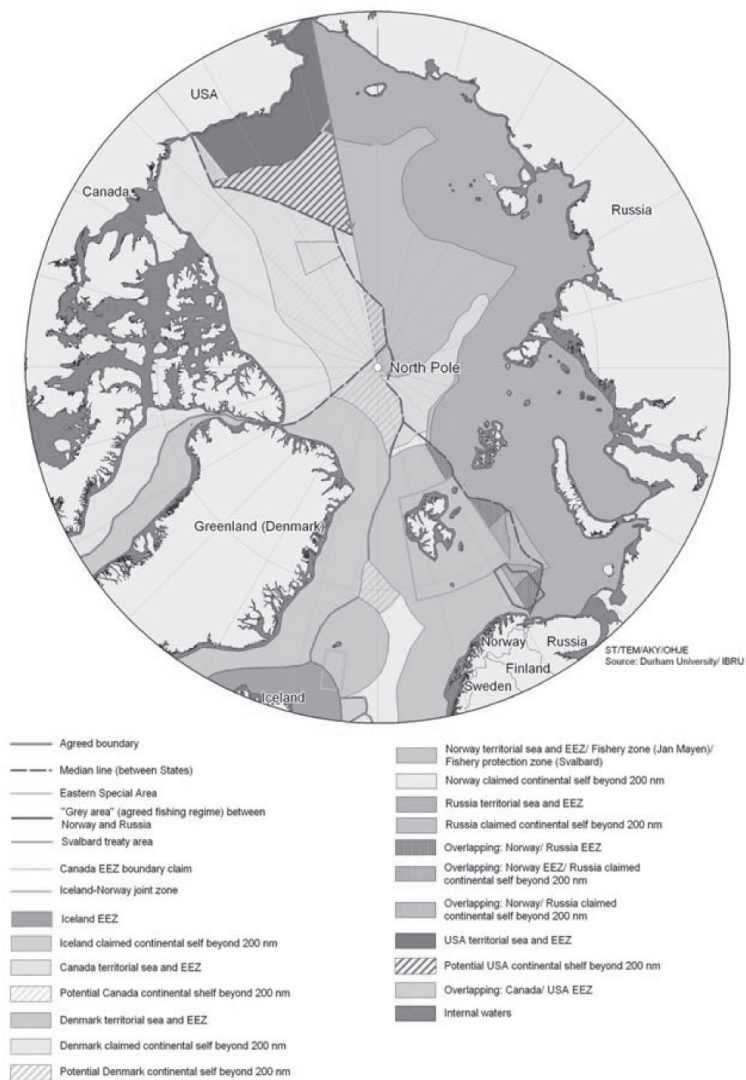
During the Cold War, the Arctic took on the highest strategic importance from its function as a safe loitering area for Soviet ballistic missile nuclear submarines and, consequently, as the hunting ground for their adversaries, the Alliance's nuclear-powered attack submarines. The U.S. and Canada established far-reaching cooperation in response to the Soviet air threat, but both partners were not able to address the surface and subsurface naval threat in the same manner. While the U.S. approached the High North with an emphasis on military security, Canada felt its sovereignty over its Arctic waters to be challenged by the American position that claimed the Northwest Passage to be an international waterway and, as such, allowing unrestricted transit. A 2010 EU report entitled "Legal aspects of Arctic shipping" comments: "Controversially, Canada has drawn straight baselines around its Arctic islands—or Arctic archipelago.... The international legal validity of enclosing the Canadian Arctic Archipelago with straight baselines remains contentious. The United States and EU member states lodged formal protests against the baselines, regarding them as inconsistent with international law. Whether Canada can justify the status of internal waters for the enclosed waters by the argument that they are historic waters is in doubt."⁸⁹ The current situation is a legal stalemate. Both sides can refer to principles of international law, and both sides are supported by cases from the International Court of Justice (ICJ). In the end, "the complexities of the legal status of the Passage" opens the door to competing interpretations and, therefore, to different solutions.⁹⁰ Once commercial and military shipping increases within the Northwest Passage, Canada will have to decide whether to focus first and foremost on sovereignty issues or on the solution

⁸⁹ European Union, *Legal aspects of Arctic shipping*. Summary report, Study commissioned by the European Commission, Directorate-General for Maritime Affairs and Fisheries MARE.C.1, Project no. ZF0924 - S03, issue ref. 2 (Brussels: European Union, 23 February 2010); available at http://ec.europa.eu/maritimeaffairs/pdf/legal_aspects_arctic_shipping_summary_en.pdf.

⁹⁰ Andrea Charron, "The Northwest Passage Shipping Channel. Sovereignty First and Roremost and Sovereignty to the Side," *Journal of Military and Strategic Studies* 7:4 (2005): 3, 7; available at http://www.ciaonet.org/olj/jmss/jmss_2005/v7n4/jms. Cleo Paskal, "How climate change is pushing the boundaries...." 7.

of pressing, practical matters in the management of these waters. While the U.S. and Canada continue to agree to disagree, the prevailing uncertainty might become an invitation for others to test Canadian sensitivity and U.S. safeguards in the High North. Further increases in Chinese activity in the High North correspond with a potential to break the stalemate, meaning to encourage U.S. acceptance of the Canadian legal position for the sake of securing the North American defense perimeter. The U.S.-Canadian border issue is not the only territorial dispute in the Arctic. A graphic illustration of the situation in the High North can be found in Figure 6.

Figure 6: Agreed Borders and Territorial Claims in the Arctic⁹¹



⁹¹ Finnish Prime Minister's Office, "Finland's Strategy for the Arctic Region," Prime Minister's Office Publications 8/2010 (Helsinki: Prime Minister's Office, 5 July 2010), 70; available at <http://www.geopoliticsnorth.org/images/stories/attachments/Finland.pdf>.

Dispute Settlement and Cooperation in the High North

In the past, various disputes in the Arctic were addressed through peaceful methods that were either treaty-based, by tacit acceptance, or through a decision by the International Court of Justice. Examples of settled territorial questions are the Svalbard Archipelago (Norway), the Franz Josef Land Archipelago (Soviet Union, now Russian Federation), the island of Jan Mayen (Norway), the Sverdrup Islands (Canada), Eastern Greenland (Denmark), and the maritime delimitation in the Vangerfjord area (Russia/Norway).⁹² Examples of economic agreements are bilateral fishery agreements like that between Norway and Russia about fishery management in the Berents Sea. Some conflicts have persisted over the years without finding a proper solution, like the Norwegian Fishery Protection Zone around Svalbard that is challenged by other states, such as Spain and Iceland.⁹³

Norway and the Soviet Union (and later the Russian Federation) successfully avoided any escalation over the issue of petroleum resources in the Barents Sea and the Arctic Ocean. Since the 1980s, both countries have followed a bilateral moratorium that suspends any exploration and exploitation of oil and gas in disputed territories. Now, following a breakthrough in their negotiations, Norway and Russia signed a treaty concerning the maritime delimitation and cooperation in the Barents Sea and the Arctic Ocean. The signing ceremony marked the end of a four-decade-long process. Once approved by the two states' parliaments, this treaty will create legal clarity and improve political predictability in the region.⁹⁴ Apart from its contribution to good relations between Russia and Norway, this treaty will grant immediate access to natural resources that are located only on one side of the agreed delimitation line. In addition to this, the 2010 Treaty contains detailed provisions for the exploitation of trans-boundary deposits.⁹⁵

⁹² Norwegian Royal Ministry of Foreign Affairs, Legal Affairs Department, "Svalbard and the Surrounding Maritime Areas. Background and legal issues - Frequently asked questions," edited by Rolf Einar Fife; available at <http://www.regjeringen.no/en/dep/ud/selected-topics/civil--rights/spesiell-folkerett/folkerettslige-sporsmal-i-tilknytning-ti.html?id=537481#>.

⁹³ Norwegian Government, *The Norwegian Government's High North Strategy*, 17.

⁹⁴ *Treaty between the Kingdom of Norway and the Russian Federation Concerning Maritime Delimitation and Cooperation in the Barents Sea and the Arctic Ocean*, Document signed in Murmansk, 15 March 2010 (English translation published by the Norwegian Government); available at http://www.regjeringen.no/upload/UD/Vedlegg/Folkerett/avtale_engelsk.pdf. Norwegian Royal Ministry of Foreign Affairs, "The Treaty on Maritime Delimitation between Norway and Russia," available at <http://www.regjeringen.no/en/dep/ud/campaign/delimitation.html?id=614002>.

⁹⁵ Treaty between the Kingdom of Norway and the Russian Federation. Norwegian Royal Ministry of Foreign Affairs, "Petroleum Resources," available at http://www.regjeringen.no/en/dep/ud/campaign/delimitation/petr_resources.html?id=614009.

In 2010, Russia and Canada announced that they will seek a UN decision over their territorial claims related to the Lomonosov Ridge, a huge Arctic underwater mountain range where rich resources are expected to be found.⁹⁶ Both Canada and Denmark claim Hans Island as their territory. In 2005, they agreed upon a joint statement. Since that time, the solution to the conflict is on the diplomatic track. The maritime boundary in the Lincoln Sea is regarded as being managed. As has been discussed above, the U.S. and Canada disagree about the legal status of the various waterways known as the Northwest Passage, while they have managed their dispute over the maritime boundary in the Beaufort Sea.⁹⁷ Climate change makes the polar ice cap in the North disappear and increases the accessibility of the region, but it has not sparked any outbreak of hostilities between states bordering the region. In fact, not a single territorial disagreement in the Arctic is perceived by the respective governments to provide sufficient reason for military confrontation.

Applied Multilateralism

Since the collapse of the Soviet Union, major efforts have been made to enhance consultation and cooperation in the High North. The Barents Euro-Atlantic Council (BEAC), and the Barents Regional Council (BRC) were established in 1993, and both of them work closely together. The BEAC provides a forum for Finland, Norway, Sweden, Denmark, Iceland, Russia, and the European Commission. The BRC is composed of representatives from regional administration units of Finland, Norway, Sweden, and Russia. The Arctic Council, established in 1996, provides a high-level intergovernmental forum “for promoting cooperation, coordination and interaction among the Arctic States, with the involvement of the Arctic indigenous communities and other Arctic inhabitants on common Arctic issues.”⁹⁸ The Arctic Council’s documents state explicitly that “the Arctic Council should not deal with matters related to military security.”⁹⁹ The active arm of the Arctic Council is represented by its six working groups that deal with contaminants, monitoring and assessment, flora and fauna conservation, emergency matters, marine environmental protection, and sustainable development. Member states of the Arctic Council are the eight Arctic states: Canada, Denmark, Finland, Iceland, Norway, Russian Federation, Sweden, and the

⁹⁶ “Russia and Canada seek UN ruling on Lomonosov Ridge,” BBC News Europe (16 September 2010); available at <http://www.bbc.co.uk/news/world-europe-11331904>.

⁹⁷ Canada’s Northern Strategy Abroad, 13.

⁹⁸ Arctic Council, *Declaration on the Establishment of the Arctic Council. Joint Communique of the Governments of the Arctic Countries on the Establishment of the Arctic Council* (Ottawa: Arctic Council, 19 September 1996), Paragraph 1; available at http://arctic-council.org/filearchive/ottawa_decl_1996-3.pdf.

⁹⁹ *Ibid.*, Footnote 1.

United States. Additionally, the council offers non-Arctic nations the opportunity to gain observer status. Multilateral organizations have proved to be important platforms for consultation, cooperation, and joint policy formulation.¹⁰⁰ In terms of security, these bodies address issues of human security in all its variations and depth.

NATO and the EU as Security Actors in the High North

NATO

Four out of the five countries that border the Arctic Ocean are NATO members. Over the past five decades, NATO and its member states have acquired enormous experience in planning and exercising Arctic security. After the dissolution of the Soviet Union, the Alliance's focus shifted towards other regions and other missions. Its collective presence in the High North—e.g., through large-scale exercises or the deployment of high-readiness forces—dropped significantly. The perceived absence of any further threat in the High North had consequences for NATO's equipment, doctrine, and training.

One outcome of the 2009 NATO Summit in Strasbourg/Kehl was the foundation of a group of experts (chaired by Madeleine Albright) that was tasked to prepare the ground for a new NATO Strategic Concept. In May 2010, the experts released their final report, where they conclude: "Conventional military aggression against the Alliance or its members is unlikely, but the possibility cannot be ignored."¹⁰¹ The document avoids the word "Arctic" entirely, and it uses the term "High North" only once: "A new level of secure maritime situational awareness is called for by changing risks around the periphery of NATO and in the High North, Gulf, Indian Ocean and other areas."¹⁰² When the issue of climate change is addressed, the expert group recommends: "NATO could, however, be called upon to help cope with security challenges stemming from such consequences of climate change as a melting polar ice cap or an increase in catastrophic storms and other natural disasters. The Alliance should keep this possibility in mind when preparing for future contingencies."¹⁰³ Neither NATO's

¹⁰⁰ "Geopolitics in the High North: Multiple Actors, Norwegian Interests," Work Package 1 Description.

¹⁰¹ North Atlantic Treaty Organization (NATO), NATO 2020: Assured Security; Dynamic Engagement - Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO, Report dated May 17, 2010 (Brussels: NATO Public Diplomacy Division, 2010), 17; available at http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf.

¹⁰² *Ibid.*, 41.

¹⁰³ *Ibid.*, 46.

New Strategic Concept¹⁰⁴ nor the Lisbon Summit Declaration of 2010¹⁰⁵ provided guidance, stated requirements, or called for action that specifically addressed the Arctic. The same picture can be taken away from the NATO-Russia Council: neither the opening statement by the Secretary-General¹⁰⁶ nor the joint resolution include any statement that would highlight security issues in the High North.¹⁰⁷ NATO's New Strategic Concept determines the Alliance's future contribution in the field of energy security as follows: "Therefore, we will ... develop the capacity to contribute to energy security, including protection of critical energy infrastructure and transit areas and lines, cooperation with partners, and consultations among Allies on the basis of strategic assessments and contingency planning."¹⁰⁸ Looking at NATO's energy security website, the Mediterranean and the Caucasus region receive mention, but the Arctic does not.¹⁰⁹

Within NATO's strategic framework, the Arctic receives no special attention, neither in terms of deterrence and defense nor in terms of actions related to energy security. NATO avoided overreacting to Moscow's proclamation of "spheres of influence" and the Russian Army's show of force in the High North. It stayed calm and did not securitize a threat that merely existed. Bringing all the environmental, political, and economic facts and trends together, this analysis concludes that NATO is not required to change its current policies and concepts in order to address the security challenges and risks in the High North. In other words, the research question is answered that there are no implications for NATO in terms of security imposed by the melting polar ice cap in the High North. Dmitri Trenin argues, "The Arctic countries have taken several practical steps over the past two years that testify to their goodwill," concluding, "the need for an increased military presence in the Arctic no longer seems

¹⁰⁴ NATO, *Active Engagement, Modern Defence—Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*, adopted by Heads of State and Government in Lisbon, 19 November 2010; available at <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>.

¹⁰⁵ NATO, *Lisbon Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon on 20 November 2010*, NATO Public Diplomacy Division, Press Release PR/CP(2010)0155 (20 November 2010); available at http://www.nato.int/nato_static/assets/pdf/pdf_2010_11/2010_11_11DE1DB9B73C4F9BBFB52B2C94722EAC_PR_CP_2010_0155_ENG-Summit_LISBON.pdf.

¹⁰⁶ NATO, *Opening Statement by the Secretary General at the NATO-Russia Council at the Level of Ministers*, 20 November 2010; available at http://www.nato.int/cps/en/natolive/opinions_68836.htm.

¹⁰⁷ NATO, *NATO-Russia Council Joint Statement*, Lisbon (22 November 2010); available at http://www.nato.int/cps/en/SID-8F957130-9D430016/natolive/news_68871.htm.

¹⁰⁸ NATO, *Active Engagement, Modern Defence*, 19.

¹⁰⁹ NATO, "NATO's Role in Energy Security," available at http://www.nato.int/cps/en/natolive/topics_49208.htm?selectedLocale=en.

relevant.”¹¹⁰ I will not go that far in this article, because contingency planning, situational awareness, and minimum presence constitute routine military safeguard measures, and should not be regarded as escalatory acts. To a certain degree NATO must (as Russia does for the same reason) respond to the environmental changes in the High North in order to maintain its credibility as a collective defense organization. These are normal adaptations, and should not create any surprise.

¹¹⁰ Trenin and Baev, *The Arctic: A View From Moscow*, 12.

Nevertheless, one issue is proposed for further attention and investigation: Article V of the Washington Treaty provides the member states with a collective security guarantee in case of an armed attack.¹¹¹ Article VI defines the area and the object (territory, forces, vessel, or aircraft) of such an attack. This being said, the legal status of the Northwest Passage appears to be an issue, one that affects not only Canada and the U.S. but also all other NATO members.

The European Union

The Lisbon Treaty entered into force in December 2009 and removed the former three-pillar structure of the European Union.¹¹² EU policies are shaped by the influence of and interaction between the Council, the Commission, and the Parliament. The power of European institutions depends on the respective policy issues in question – either the Union has exclusive competence, or it shares competence with the member states, or it supports member states. According to Article 22 (1) of the Treaty on European Union (TEU),¹¹³ decisions about strategic interests and objectives related to the Common Foreign And Security Policy (CFSP) fall under the competence of the European Council. CFSP decisions require unanimity. For external actions, the EU is rather limited in terms of its “hard power” capabilities (meaning military ones), but is well equipped with “soft power” tools in order to fulfill its role as security actor. As of today, the EU still requires that the CFSP be harmonized between its own bodies, across various policy domains, and with the governments of its member states.

In terms of military affairs, TEU Article 42 (7) establishes the EU’s collective defense mechanism. It sets the obligation to provide aid and assistance in case of an armed attack against another member state, and determines that NATO remains the foundation of collective defense for those member states that are also members of the Alliance. Article 222 of the Treaty on the Functioning of the European Union (TFEU)¹¹⁴ contains the solidarity clause for cases of terrorist attacks and natural or man-made disasters.

¹¹¹ NATO, The North Atlantic Treaty, signed in Washington D.C., 4 April 1949; available at http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

¹¹² European Union, Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 (Bussels: Office for Official Publications of the European Communities, 17 December 2007).

¹¹³ European Union, “The Treaty on European Union (Consolidated Version),” in Consolidated Treaties. Charter of Fundamental Rights (Brussels: Publications Office of the European Union. March 2010).

¹¹⁴ European Union, “Treaty on the Functioning of the European Union (Consolidated Version),” in Consolidated Treaties. Charter of Fundamental Rights, March 2010.

The “European Union is an Arctic player. Three out of eight Arctic countries are member states of the Union.”¹¹⁵ The “Northern Dimension” is a common policy shared by the EU, Russia, Norway, and Iceland, with the U.S. and Canada having observer status. It serves as an umbrella for regional cooperation in the Arctic.¹¹⁶ The EU runs cross-border cooperation programs in the Arctic in order to promote economic, social, and environmental development.

On 14 March 2008, the High Representative and the Commissioner for External Relations forwarded their policy paper “Climate Change and International Security” to the European Council that triggered the call for an EU Arctic policy. On 9 October 2008, the European Parliament (EP) welcomed the foundation of such a policy and requested the Commission to address energy and security policy in the Arctic region.¹¹⁷ The Commission replied to the parliament with a communication that contained the following assessment of the situation: “environmental changes are altering the geo-strategic dynamics of the Arctic with potential consequences for international stability and European security interests calling for the development of an EU Arctic policy.”¹¹⁸ Then the Commission defined three main policy objectives: protecting and preserving the Arctic and its population, promoting the sustainable use of resources, and contributing to enhanced Arctic multilateral governance. Several days earlier, the Commission had released its Second Strategic Energy Review, in which it identified Norway and Russia as important partners.¹¹⁹ With the Energy 2020 strategy, the European Commission underlined the link between the EU’s energy security and the CFSP.¹²⁰ It calls for the diversification of fuels, sources of supply, and

¹¹⁵ Hannu Halinen, “Finland’s Arctic Strategy.”

¹¹⁶ Finnish Prime Minister’s Office, “Finland’s Strategy for the Arctic Region,” 83.

¹¹⁷ European Union, European Parliament Resolution of 9 October 2008 on Arctic Governance, European Union/European Parliament, Document P6_TA(2008)0474 (Brussels: European Union, 9 October 2008); available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2008-0474+0+DOC+WORD+V0//EN>.

¹¹⁸ European Union, Communication from the Commission to the European Parliament and the Council - The European Union and the Arctic Region, European Union/Commission of the European Communities, Document COM(2008) 763 final (Brussels: European Union, 20 November 2008); available at http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/reports/104895.pdf.

¹¹⁹ European Union, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Second Strategic Energy Review. An EU Energy Security and Solidarity Action Plan, Commission of the European Communities. Document COM(2008) 781 final, 13 November 2008, 8.

¹²⁰ European Union, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Energy 2020. A strategy for competitive, sustainable and secure energy*, European Commission. Document COM(2010) 639 final (Brussels: European Union, 10 November 2010).

transit routes. Despite the Commission's evaluation in November 2008, the Arctic region received no special attention in the energy strategy. The EU's Arctic Policy is still in the drafting process. The Council requested the Commission to report on the progress by mid-2011, and expressed an interest in maintaining the Arctic as an area of peace and stability.¹²¹ Thus we can see that the Arctic enjoys a certain degree of de-securitization within the EU.

Summary and Final Conclusions

Melting ice constitutes a prerequisite for improved accessibility of the High North, which is the key to the realization of economic opportunities in the area. Northern sea routes are not always the shortest, and will not become attractive for commercial intercontinental shipping in the near future. While predictions indicate a rising demand for energy due to the recovery of Western economies and the needs of emerging economic powers like China, India, and Brazil, the sustainable supply of fossil fuels might be threatened by political instability within producing regions and along transport routes. The Arctic offers a potential alternative to other energy-producing regions. While the expected resources are of a significant scale, the volume of future oil and gas extraction in the High North remains a function of multiple variables and leaves us with a high degree of uncertainty.

Many authors argue that the impacts of climate change will trigger political tensions, foster legal disputes, and might even lead to an outbreak of hostilities. The research undertaken for this article suggests that this is unlikely. The players in the region have diverging interests and goals, as are described below:

- **Russia's** interests in the Arctic are predominantly of an economic nature. The country applies an approach of pragmatic cooperation with foreign governmental and non-governmental partners in order to pursue its goals. This offers great potential for foreign companies to benefit from broader cooperation with Russia.
- The **U.S.** will secure its territorial claims in Arctic waters against others, but so far they are not being challenged, and from the perspective of energy security there is no need for Washington to rush to the High North.

¹²¹ European Union, Council Conclusions on Arctic Issues. 2985th Foreign Affairs Council meeting Brussels, 8 December 2009, Council of the European Union (Brussels: European Union, 2009), http://ec.europa.eu/maritimeaffairs/pdf/arctic_council_conclusions_09_en.pdf.

- **Canada's** Northern Strategy determines four priority areas in order to address the region: sovereignty, social and economic development, environmental protection, and governance. In terms of military and law enforcement issues, Ottawa has to reinvent and reinforce its Arctic capacities. Canada regards the U.S. as its "premier partner in the Arctic," but has also committed itself to closer international cooperation, especially with Russia, Norway, Denmark, Sweden, Finland, and Iceland. Progress on outstanding boundary issues receives highest priority.
- The underlying assumption for the **Norwegian** government's policy is that the country should avoid isolation, and should pursue far-reaching partnerships in the Arctic. In terms of foreign policy, this means that the relationship between Moscow and Oslo is the key for success. Good political relations and advances in technology make Norwegian companies strong players when it comes to the exploitation of natural resources in the High North.
- The **Danish** government and Greenland's representation seek to strengthen the development of Greenland towards increased autonomy, and to maintain the Greenlandic-Danish position as a major player in the Arctic. Enhanced economic cooperation bears potential for Greenland to increase its sustainability and therefore to promote its independence from Denmark. The island continues to play a significant role in military strategic planning, especially for the "North American Defense Perimeter."
- In the wake of the financial crisis and the collapse of its banking system, **Iceland** raised significant attention by its search for new friends. Today, it seems less likely that Iceland will enter the EU within the coming years. The country does not have any territorial claims towards the Arctic Ocean, but it follows the developments there very closely.
- **Finland** strongly advocates the protection of the Arctic environment, and it seeks to benefit from emerging economic opportunities in the region.
- **China** is not an Arctic country, but in recent years it has demonstrated significant interest in the polar region. In practice, the Chinese outreach to the High North is characterized by the pursuit of economic interests. China is not the only Asian country that longs for increased economic influence in the High North, but at first glance it seems to be the preferred partner for Russia. Competition in the bid for strategic cooperation with Russian oil and gas companies also comes from Japan, Korea, India and Vietnam.

UNCLOS stipulates a legal framework to define all of these actors' mutual relations within the Arctic region, and it provides legitimacy as well as instruments and procedures for the settlement of claims and disputes. In the past, various disputes in the Arctic were addressed through a variety of peaceful channels. Climate change makes the polar ice cap in the North disappear and increases the accessibility of the region, but it has not led to any hostilities between the states that are interested in the region. In fact, no territorial disagreements in the Arctic have led or are likely to lead to military confrontation. Norway and Russia, Russia and Canada, as well as Canada and Denmark have achieved major progress in overcoming their respective territorial disputes and agreeing on permanent solutions. The complex interplay between governments, multi-lateral organizations, regional and local state authorities, NGOs, local populations, and commercial actors shapes geopolitics in the High North. The Arctic fosters new alliances. Present and future inter-state conflicts that arise directly or indirectly from a melting polar ice cap in the High North will be predominantly settled through other channels. Competition and cooperation as established in the High North can be explained by liberalist or constructivist approaches. The world is not witnessing an unconstrained struggle for hegemony in the Arctic, but, on the contrary, the achievement of mutual agreements on an equal footing, and the application of mediating principles as foreseen in UNCLOS. Commercial interests and commercial actors have already grown in importance, and it is likely that they will become even more powerful in the future.

Despite a high level of political and public recognition of the environmental, economic, and security related changes in the High North, both NATO and the EU remain restricted in their mandate, and limited in their capacities to contribute to Arctic security. In the ongoing process to reinvent NATO as a global strategic actor, the Arctic receives no special attention, either in terms of deterrence and defense or in terms of actions related to energy security.

This analysis concludes that NATO is not required to change its current policies and concepts in order to address the security challenges and risks in the High North. Adaptations must take place, but at lower levels than the strategic one, so they can be achieved within the given strategic guidelines and decisions. In the case of NATO, maintaining awareness in the region as well as the demonstration of a certain degree of military presence within its northern perimeter remain necessary. This is daily defense business, and implies no alteration of the Alliance's general cooperative posture with respect to Russia.

The EU is an Arctic actor, but Arctic security as such is not put high on the EU's agenda, because the member states are not pressing forward with this issue. The melting of the polar ice cap will require some attention in the fields of energy security and internal security. Nevertheless, following the idea of a comprehensive approach, the Arctic issue should remain an integral part of an overarching strategy and not

become relegated to a specific regional concept. Finally, the research question can be answered as follows: Neither NATO nor the EU is required to change its current security policies and concepts in order to address the challenges and risks imposed by a melting polar ice cap in the High North.

The Emergence of Organized Criminal Networks as Extralegal Authorities

By Priscilla Bittencourt Ribeiro de Oliveira and Plamen P. Penev

The Emergence of Organized Crime

Globalization and the contemporary global order have facilitated the emergence of new aspects of governance within, between, and across the state scale. The re-articulation and re-scaling of the state involves the devolution of specific aspects of governance capacities to supra- and sub-state scales, constituting a vast transglobal arena where a bewildering array of private, non-state actors, networks and polities take on roles previously performed by the state. This reconfiguration of the position of the nation-state transcends the Westphalian “territorial trap,”¹ when it comes to produce new sites of power, new forms of authority and regulation through a reshuffling of traditional sociopolitical relationships.

The distinguishing feature of these alternative authority structures is that they tend not to be embodied at what has been historically constituted as the national or local scale, but rather are represented along the multiple, overlapping scales that make up global relations.² Within those hybrid scales a broad spectrum of actors interact and struggle for power and control: from public and private alternatives to sovereign states, from institutions of global governance to the transnational third sector, from religious movements to complex criminal organizations.

Among the most significant developments that has taken within this arena and has been fostered by the attendant sociopolitical and economic changes is the emergence and empowering of criminal organizations, whose cross-border networks and ability to continue their activities depends on their capacity to delegitimize governmental efforts to control their behavior. Complicating matters further, the strengthening of regulatory regimes usually creates perverse incentives for organized crime groups to expand their activities and increase their profits.³

Throughout the 1980s and 1990s, it became increasingly clear that the rise of transnational organized crime was inextricably connected with contemporary changes in the scope and competence of states’ authority over their societies and territory,

¹ In the Westphalian order, the self-contained state is the locus of social and political organization.

² Saskia Sassen, “Globalization or Denationalization?” *Review of International Political Economy* 10:1 (2003): 5.

³ Phil Williams, “Crime, Illicit Markets, and Money Laundering,” in *Managing Global Issues: Lessons Learned*, eds. P. J. Simmons and C. Jonge Oudrat (Washington, D.C.: Carnegie Endowment, 2001), 106.

and with the inability of many states to reform their key government sectors to ensure the security of their populations.⁴ This assertion is particularly valid for states in transition and for the global south, where territorial states are more often discontinuous with social relations, where it is common for states to contend with both domestic and external frameworks of authority, and where the very notion of state sovereignty has always been contested. Yet, the vulnerability of these states is usually represented by certain institutional characteristics, such as a low level of state legitimacy, territorial vulnerability, privileged and dominant elites, little economic or social provision for the population, underdeveloped social institutions, corrupt distributive entities, functional holes (regulatory frameworks, criminal justice system, ineffectiveness of rules, electoral systems), and other deficiencies that can be exploited by criminal groups to conduct illegal enterprises with a high degree of impunity.⁵

Neither the re-scaling of states' authority nor the link between inefficient states and organized crime are new phenomena. However, since the end of the Cold War, and perhaps as a substitute for it, greater attention is being paid to the hazards posed by transnational crime to the classic concept of the state and to world societies.⁶

Within a territory ruled by a government whose authority is limited or absent, criminal organizations may regard themselves as legitimate political authorities wielding enough power and influence to counterbalance or even to replace legal authorities. However, criminal organizations generally do not wish to be bound by the obligations of sovereignty. It is essential for them to remain sovereignty-free, to use their freedom to cross borders nominally under the control of states, and their flexibility to engage in activities that are difficult for governments and international organizations to regulate.⁷

Another major problem posed by organized criminal groups is related to the complexity of their organizations' networks and their activities. Criminal organizations have become increasingly centralized at the national level, empowered by and contributing to shifting opportunities for their illegal activities at the local, regional, and global levels.⁸ These organized crime groups engage in a full range of illicit activities

⁴ Becky Mansfield, "Beyond Rescaling: Reintegrating the 'National' as a Dimension of Scalar Relations," *Progress in Human Geography* 29:4 (2005): 463.

⁵ Phil Williams, "Transnational Organized Crime and the State," in *The Emergence of Private Authority in Global Governance*, eds. R. Bruce Hall and T. Bierstecker (Cambridge: Cambridge University Press, 2002), 169.

⁶ L. Shelley, "Transnational Organized Crime: An Imminent Threat to the Nation-State?" *Journal of International Affairs* 48:2 (Winter 1995): 463.

⁷ Eric W. Hickey, *Encyclopedia of Murder and Violent Crime* (Thousand Oaks, CA: Sage Publications, 2003), 341.

⁸ H. Richard Friman, "Caught up in the Madness? State Power and Transnational Organized Crime in the Work of Susan Strange," *Alternatives* 28 (2003): 478.

including narcotics trafficking, smuggling and trafficking of people, and illegal sales of weapons. They also undertake insidious activities such as murder, extortion and corruption, financial market manipulation, and industrial and technological espionage. Money laundering has also become a central and transnational feature of these groups, who make use of offshore financial institutions and bank secrecy jurisdiction to hide their ever-increasing revenues.⁹

The financial resources generated by these criminal activities have been augmenting not just the power of criminal organizations but also the increasingly international scope of their illegal enterprises. The escalating power this wealth has generated for criminal organizations has altered the relationship between transnational criminal groups and the state. As highlighted by Susan Strange, “technology and a world market in drugs and in money together have caused states to fail to protect society against crime and criminals.”¹⁰

Long-term neglect of the problem has led to highly developed criminal organizations that are in a position to undermine political structures, the world economy, and the social order of countries in which these criminal groups are based and operate. The resulting instability invites more crime and violence, and may preclude the institutionalization of democratic institutions, the rule of law, and legitimate markets.

The Dynamics of Organized Crime

The term “organized crime” usually refers to large-scale and complex criminal activities carried out by tightly or loosely organized associations and aimed at the establishment, supply, and exploitation of illegal markets at the expense of society. Such operations are generally carried out with a ruthless disregard of the law, and often involve offenses against individuals, including threats, intimidation, and physical violence.¹¹

Although the main purpose of organized crime groups is to make a profit, an inevitable by-product of their illicit activities is an implicit challenge to the sovereignty of the state and the authority of its legitimate institutions. The major evidence of the power of criminal organizations is the challenge or threat they pose to the state as a sovereign entity, which claims a monopoly over coercive power and exclusive autho-

⁹ Shelley, “Transnational Organized Crime: An Imminent Threat to the Nation-State?”, 464.

¹⁰ Susan Strange, “The Limits of Politics,” *Government and Opposition* 30 (1995): 207.

¹¹ United Nations, Proceedings of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 27 August–7 September 1990, Havana, Cuba; documents available at http://www.asc41.com/UN_Congress/8th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/8th_congress.htm.

rity over its territory and population.¹²

To this extent, it is irrefutable that criminal groups have turned their capacity of coercion into a highly lucrative activity by threatening the power of the state in some structural areas, undermining governmental institutions and social order through corruption and the use of violence. As Janet Roitman has pointed out, “violence can be part of the very legibility of power,” in the same way that violent practices can be exerted as a legitimate mode of the exercise of power.¹³

The violence perpetrated by criminals is a frontal attack on states’ authority and is usually directed at particular state institutions that societies rely on for protection and order. Violence and the threat of violence by criminal organizations are also used to eliminate competitors or obstacles to their business, and to extort large and small businessmen. Through intimidation and assassination, organized crime limits individual expression and freedom of the press, undermines the creation of an active civil society by dominating independent organizations and by intimidating citizens in their struggle against criminal activities. To the extent that this succeeds, the state has failed in one of its major functions: securing the safety and prosperity of its citizens.¹⁴ If violence is the most dramatic manifestation of the authority of organized crime, the economic power of those criminals is another form of control used for corruption, intimidation, and destabilization of institutions, in ways that undermine the foundations of good governance (e.g., participation, transparency and accountability).¹⁵

The activities of criminal organizations undermine the rule of law and the legitimacy of democratic governments through the corruption of state institutions and the individuals designated to combat crime. Corruption is widely practiced as a tool to obstruct the functioning of criminal justice systems, to hinder border control efforts, and to ensure that organized crime operations can be conducted outside the system of rules that regulate other business practices and limit the rights of law-abiding citizens.¹⁶

¹² Aradhana Sharma and Akhil Gupta, *The Anthropology of the State: A Reader* (Oxford: Blackwell, 2007), 11.

¹³ Janet Roitman, “Productivity in the Margins: The Reconstitution of State Power in the Chad Basin,” in *Anthropology in the Margins of the State*, eds. Veena Das and Deborah Poole, D.. (Santa Fe: School of American Research, 2004), 193.

¹⁴ Shelley, “Transnational Organized Crime: An Imminent Threat to the Nation-State?,” 468.

¹⁵ Williams, “Transnational Organized Crime and the State,” 167.

¹⁶ Shelley, “Transnational Organized Crime: An Imminent Threat to the Nation-State?,” 468.

Nonetheless, the wealth that organized crime groups accrue is instrumental to creating home turfs from which they may develop a degree of legitimacy that can build up into authority structures. Likewise, criminal organizations seek to exploit functional holes in state capacity gaps by taking control and providing some rudimentary form of governance to areas disregarded by the state¹⁷

Occasionally, criminal groups engage in paternalistic behavior to build domestic support, while transforming power based on fear and the threat of violence into more legitimate notions of authority and approval. As one would expect given these practices, organized criminal organizations thrive in societies where family, kinship, clan relations, and patron-client relationships are fundamental institutions and sources of deference and loyalty to individuals.¹⁸

As criminal organizations develop from their domestic bases, their networks establish connections with other associates in every corner of the world. Specially, criminals can rely on links established with other fellow-nationals living in diaspora communities overseas. Ethnic ties among migrant groups in different countries usually work to facilitate international illicit activity. That assumption holds true across borders in African countries, in the Golden Triangle (Myanmar-Vietnam-Laos-Thailand), and along the southern frontier of the former Soviet Union (the Azerbaijan-Iran and Tadjik-Afghan borders).¹⁹

The evolution of organized crime from local to global non-state actor requires that these groups start being considered part of the global social and political agenda. Isolated local or national responses have become clearly inadequate to confront the intricate dynamics of organized criminal organizations, which have been easily eluding authorities and profiting from the existing patchwork of divergent legislative and enforcement policies among states. Only global, multilateral reactions can be proportional to the overall threat posed.

In any case, it is important to look more closely at the different forms and variations in which organized crime is manifested. For this reason, the next section explores organized crime in and emanating from Colombia, one of the most powerful and widespread drug trafficking organizations in the world.

¹⁷ Williams, "Transnational Organized Crime and the State," 179.

¹⁸ *Ibid.*

¹⁹ Shelley, "Transnational Organized Crime: An Imminent Threat to the Nation-State?", 466.

Organized Crime in Colombia

Colombian sovereign authority reflects a deep legacy of distrust of its ability to exert control over its territory and society. The difficulties in legitimizing centralized authority and the persistence of alternative political orders are a reflex of inefficient and corrupt state-making, social instability, and widespread violence.

The most significant constraint on the consolidation of the Colombian nation-state is the limited presence, and even absence, of the state apparatus in much of what legally constitutes its national territory. The marginal place to which citizens in remote geographic regions are relegated points to a politics of exclusion, and consequently a delegitimation of the state's authority. Within a "collapsing state," the development of local loyalties and identities, as well as the formation of parallel authorities become unavoidable.²⁰

During the 1970s and 1980s, Colombia offered structural conditions that were ripe with potential for organized criminal activities: the geography of the country, the structure of the political system and parties, a delegitimized regime, fragmented civil society, widespread propensity to resolve disputes through violence, numerous obstacles to upward social mobility, large scale of illegal economic activities, and the social acceptance of contraband and money laundering.²¹

To make things worse, the political-criminal linkage formed within Colombia is a complex phenomenon which encompasses a multitude of actors ranging from illegal drug traffickers and other criminal organizations, guerillas, and paramilitary groups; to the army and the police, the government and its bureaucracy, political parties, the United States government, civil society organizations, and others. Connections among those actors are usually intertwined and difficult to ascertain with accuracy, as the relationships are typically covert and vary according to context and over time.²²

One of the most compelling examples of alternative authority in Colombia has been the armed actors that have flourished alongside the state's inability to consolidate territorial control and to exert its monopoly on the legitimate use of force. Those actors are mainly represented by guerilla groups and paramilitaries whose intimidation and pervasive violence are leaving the cities of Colombia under siege and inducing a state of paranoid claustrophobia among the population.

Guerrilla groups first developed as self-defense militias made up of Ecuadorian and Colombian peasants who became politicized under Marxist political ideologies in a struggle for equality. Paradoxically, while aiming to take over rule of the state, those left-wing insurgencies resorted to criminal activities as a source of funding. The Revolu-

²⁰ Mason, _____, 15. [Authors: please provide short citation.]

²¹ Rensselaer W. Lee, III and Francisco Thoumi, "The Political-Criminal Nexus in Colombia," *Trends in Organized Crime* 5 (Winter 1999): 60.

²² *Ibid.*, 59.

tionary Armed Forces of Colombia, or FARC—one of Colombia’s largest left-wing insurgencies—has increased its profits through forced recruitment of insurgents (including teenagers from indigenous families) and an increasing number of civilian kidnappings. Moreover, it has specialized in controlling the cocaine trade, levying a tax on growers and processors.²³

In Colombia, guerillas are opposed not so much by the Colombian military as by paramilitary groups, organized and financed by landowners. Many of these are in fact coca barons, who bought their land from ranchers who were intimidated by guerillas into selling their property. They quickly moved beyond their stronghold in the north of Colombia and started branching out nationwide, engaging into a bloody struggle with guerillas to secure key access routes for the coca trade.²⁴

Paramilitaries are no strangers to the organization of violence; they operate on the principle that the only effective response to revolutionary terror is even greater counter-terror. For its part, the Colombian government does not have a clear policy against paramilitaries, and often sends clear signals of impunity to them. The armed forces watches over paramilitaries’ activity with “benevolent neutrality,” once they are doing its work for it.²⁵ Moreover, it would be impossible for the Colombian government to this war fight on two fronts—a war that has been flattening civil society in so many fields.

When guerillas and paramilitaries groups started investing in the narcotics trade, Colombia had already been transformed into the corporate headquarters of the South American cocaine industry, operating as a cartel. Drug cartels take advantage of their monopoly position in the market to artificially control the availability, quality, and prices of the product. Their activities are not restricted to the control and distribution of narcotics, since once they are established the same structural networks can be used to smuggle many other illegal products and services.

To carry out their diverse illegal activities, Colombian drug cartels recruit a diversity of workers like peasants, chemists, various types of suppliers, purchasers and intermediaries, pilots, lawyers, financial and tax advisers, enforcers, bodyguards, front men (*testaferros*), and smugglers who work to launder the organizations’ profits. This workforce is tied to the central cartels in various ways; some are directly part of the organization, but many are independent subcontractors loosely tied to them. The cartels’ networks also include politicians, police, guerillas, paramilitaries, individual army members, public employees, bankers, loyal relatives, friends, and many others.²⁶

²³ Marc Cooper, “Plan Colombia: Wrong Issue, Wrong Enemy, Wrong Country,” *The Nation* (19 March 2001): 17.

²⁴ Anthony Daniels, “Colombia’s Hell: Fear Grips a Nation,” *National Review* (6 December 1999): 50.

²⁵ *Ibid.*

²⁶ Francisco Thoumi, “Illegal Drugs in Colombia: From Illegal Economic Boom to Social Crisis,” *Annals of the American Academy of Political and Social Sciences* 582 (2002):108.

The complex social network that forms drug cartels supports and provides protection to the illegal industry, once it comes to constitute the main channel through which cartels penetrate and corrupt states' social institutions around the globe. Through this network, the illegal industry forges strong loyalties, undermines systems of justice, and becomes entrenched within the state through the distribution of its illegal income to the rest of the society.²⁷ With a large sum of money at their disposal, drug barons started discarding their traditional violent practices to achieve their goals through extortion and corruption. According to their new "business ethics," violence is bad for business.

If violence and warfare have become tools of last resort for drug cartels, they still considered by the U.S. government to be the most effective means to help Colombia to defend its democracy, eradicate drug crops, and defeat the criminal groups that have been spreading violence across the nation. In a move that has represented the legitimate delegation of authority over its territory and security matters to another state, Colombia has granted the U.S. military the use of military bases in its country.²⁸

Nevertheless, it is claimed by most critics that another military-based program is the last thing that Colombia needs. The idea of President Andrés Pastrana's plan was based on a peace initiative leading to a cease-fire, and the U.S. government has been shaping it according to their interests. "Plan Colombia" has been considered by the United States as another opportunity to project their power abroad, to achieve its own objectives at a punishing social cost to a society embedded in an endless cycle of violence. According to one U.S. Embassy official, "the U.S. and Colombia have different priorities," while "Colombia has peace as priority, we have narcotics."²⁹

All available evidence shows that drug use is not reduced by attacking the source, but only by reducing the demand. Plan Colombia, at best, will disperse drug production from Colombia to some neighboring location, and it will do nothing to reduce drug consumption in the U.S.³⁰

With regard to the situation in Colombia, it may make matters even worse. Cutting into the drug trade—a business from which all armed actors profit—might force some groups to increase kidnappings in order make up the difference in revenue.³¹ The agreement has already exacerbated tensions between Colombia and the rest of the region. The violence within Colombia has spilled over its borders into neighboring states for years. The conflict regularly causes border clashes between the Venezuelan and Ecuadorian armed forces and Colombian armed groups. Yet, Venezuela

²⁷ Ibid.

²⁸ Gregory Wilpert, "U.S. Troops in Colombia: a Threat to Peace," *NACLA Report on the Americas* (2009) 3; available at <https://nacla.org/node/6088>.

²⁹ Cooper, "Plan Colombia: Wrong Issue, Wrong Enemy, Wrong Country," 17.

³⁰ Ibid.

³¹ Ibid., 12.

is already home to one of the world's largest refugee populations—an estimated four million Colombians.³²

The illicit drug industry has become the immediate cause of Colombia's social crisis, and has also been contributing to the country's economic recession due to the destruction of its productive activities and capital flight. In a cyclical battle for profits among armed groups, drug cartels, the Colombian government and its institutions, and the United States, the civil society in Colombia is the only group that has been consistently misrepresented and whose interests have been disregarded. The Colombian state is not at war; its criminals have been waging a war within its territory and against its own civil society. It is important to evaluate those social and spatial scales to notice how many different "Colombias" have been formed around the world, and to realize that the main problem in these "Colombias" is not the illegal activities carried out by criminal groups, but rather the construction of institutional and cultural identities built on illegality and force.

³² Wilpert, "U.S. Troops in Colombia: a Threat to Peace," 3.

The Essence of Crosscultural Security Education

*By Lt. Col. Andrzej Pieczywok**

This article presents the main factors that affect the preservation of peace and security among human beings. It treats these categories as the most important goal of the education of modern man, as the basis of its performance in the world today. The core values that most significantly affect human existence are structured around three basic concepts: security, peace, and education.

Peace is a value based on a range of other values associated with each other. It is based on certain laws and rules, including international rules. According to the negative definition, peace is simply the absence of war, a lack of organized violence between states, and a lack of military resources. It can also refer to the system that interrupts the state of war between states, or a process that sets out the conditions for ending the war. The positive definition of peace is a type of harmony in international relations, a positive relationship between countries. It is not a static concept—even when a lack of war prevails, actions that support peace are still required. Peace is a state of agreement between states and peoples, not simply a lack of war.

War, on the other hand, can be defined as a structured way of using violence to resolve a dispute, the use of military means of killing as a way to achieve certain goals. War can be understood as a collision of entities, a highly organized struggle among social groups. War is a kind of armed conflict, but not all armed conflict is war.

War (according to the Stockholm International Peace Research Institute) is a form of major armed conflict in which troops that are subordinates of two or more governments and at least one military organization are engaged for a long period of time. War is said to exist when at least 1000 people are killed in a conflict in a twelve-month period, and when it is being formally waged in accordance with international law. During times of war, international agreements may be broken and diplomatic relations may be severed. Most of the conflicts that qualify as war according to these criteria nevertheless take place without an official declaration of war.

In the common understanding, war is the opposite of peace. Peace is the normal state of relations between states, while war is its unnatural counter, a state that fundamentally changes the relationship between the countries involved. Reflections on the history, essence, and nature of war, as well as speculation on the best ways to

* Andrzej Pieczywok holds a doctorate in didactics and pedagogy, and is Head of the Pedagogy Department at the Polish National Defense University in Warsaw. His research focuses on shaping the command skills of officers and on security education systems in the European Union and NATO.

achieve and preserve peace, have appeared in human thought since antiquity. Within the broad discipline of international relations, the problem of war and peace, along with a wide range of security issues, occupies a prominent place.

In the field of international relations the concept of “armed conflict” is broader than the concept of war. Conflict refers to all forms of armed struggle whose participants are not subjects of international law. Armed conflict is preceded by antagonism between the parties, increasing conflicts of interest, various forms of verbal conflict (protest, opposition, threat) and confrontational action (e.g., severing of diplomatic relations, demonstrations of force).

In today’s world it is difficult to feel completely safe. Terrorism, natural disasters, environmental degradation constitute a great threat to contemporary populations, as do good that have been created to ostensibly advance civilization. Humans themselves have created things that do not allow them to live safely. Raising public awareness about the dangers of this world, through proper upbringing and education, can help us avoid large disasters, and thus increase the feeling of security. In addition to educating our children about the dangers posed by the world, however, we must also continuously speak about peace. We must educate the world to love peace if it is to be cultivated and defended.

Security as the primary value of human existence is one of the primary subjects of discussion within both academic disciplines and the broader society. It is the object of the concerns, aspirations, and desires of people around the world. In this environment, it is important to promote actions that preserve peace. These operations are conditioned by the characteristics of human nature, and, on the other hand, by axiology, or the study of values. Human nature is analyzed by both philosophy (anthropological philosophy) and psychology (which examines in detail man’s personality, disposition, development, and opportunity). Systems of values, on the other hand, are the area of study of axiology, a basic component of philosophy. Ethics, above all, sets cardinal values that are appropriate to the adult human personality. Such a personality is attributed to man, as an entity essentially free to realize its dignity, because he is concerned with great matters. Since ancient times such a philosophical man is in every aspect a model in ethics, and has served as an important ideal in a responsible and fair education.¹

Security is the fundamental and necessary condition of healthy and well-understood human development, as well as of full self-realization in a social community. We assume that the state we define as social security is achieved when the following conditions are met:

¹ J. Świniarski, “Przywódtwo jako osnowa edukacji dla bezpieczeństwa,” *Zeszyty Naukowe AON* 1 (2001): 134.

- There is a state of harmony between stability and instability in matters of life importance
- There is a favorable ratio of predictable to unpredictable events
- There are no unfavorable changes in an individual's achieved career standing and stability regarding vital factors and plans (both long- and short-term)
- There is no external control or interference in individuals' values and private actions.²

However, one can not talk about issues of security or war while excluding an education for peace. Therefore, if we want to lead a discourse about an effective education for security, we can formulate several basic questions. Attempting to answer these questions sets the course for our thinking here. The key questions for this issue are:

1. What is the essence of education for security, and how it may affect the maintenance of peace?
2. What values determine human security?

Any reflection on peace and the values that determine its conditions requires the determination of how are they understood, especially since in every unique instance it is conditioned by one's axiological position. Let us say briefly that we recognize a value as something that is particularly valuable. Determining the value of peace lies in estimating those relations. The value may be the aim (in which case it will have a higher value) or it may be a means to an achieve aim (in which case it will have a lower value). Some values are absolute, while others are relative. The evaluation process is an essential element of human life, a key dimension of its security.

The Nature and Determinants of Education for Security

Education as the great hope of the present is itself at risk, as it is subject to many contradictions, tensions, and failures. Today, we observe the lowering of the prestige of many of the humanistic, social, and cultural disciplines as a result of views based in mechanical or psychological reductionism. Education in humanistic disciplines should assist in preparing citizens to perform their most suitable social and professional roles, in which a person finds him/herself in harmony with oneself and others.

² M. Rybakowski, "Kultura bezpieczeństwa na tle stanu bezpieczeństwa dzieci i młodzieży w ruchu drogowym," in *Edukacyjne zagrożenia początku XXI wieku*, ed. K. Pająk & A. Zduniak (Warszawa-Poznań: Wyd. Dom Wydawniczy Elipsa, 2003), 100.

Modern society is described in terms of a “risk society,”³ in which a range of phenomena—illness, unemployment, armed conflicts, security risks—serve as sources of fear and anxiety that unsettle both individual and social senses of well-being. Piotr Sztompka indicates that modern culture possesses features that are difficult for the individual to accept and overcome. These characteristics can be described as falling into three sub-categories: cynicism (distrust), manipulation (misuse of trust), and indifference (selfishness). While living in a society we cannot with certainty feel safe, but at the same time human beings must possess qualities that somehow help them deal with it this inherent lack of security.⁴

Zbigniew Kwieciński states that in the modern world we have reevaluated and changed the nature of work. His thesis on socialization shift holds that we have shifted our sources of education from family upbringing and school to mass media, peers, or “bad heroes.”⁵ A characteristic quality of the cultural development of many countries is the distance between the generations (generation gap), which is the consequence of the fact that young people are focused on change, the search for new patterns of behavior that are relevant to their changing reality, while the older generations are seen as living in the past and dedicated to preserving the status quo.

It its broadest possible terms, as a practice education refers to the notion of upbringing, especially intellectual upbringing; considered as a noun rather than a verb, it can be taken to refer to a level of knowledge, particularly in science.⁶ When understood as a way of learning to be human, however, our view of education should focus on humanistic education, and thus be oriented towards the values of humanity. Education is a social process, organized in order to induce changes in humans. Its primary focus is thus the relationship between human beings.

Education, on one hand, must prepare people to use the achievements of civilization, and on the other hand lead them to creative participation in furthering civilization. It is particularly important in the pursuit of scientific truth, and in shaping pro-social and pro-peace attitudes. It has influence on human autonomy, on building the right to choose. The educational process transmits patterns of behavior, beliefs, and traditions, and therefore it is of fundamental importance for the cohesion of society. Education shapes the personality of the social unit, and thus plays a tremendous

³ Ulrich Beck, *Risk Society: Towards a New Modernity* (London: Sage, 1992); Ulrich Beck, *World Risk Society* (Cambridge: Polity Press, 1994); Ulrich Beck, *Spółeczeństwo ryzyka: w drodze do innej nowoczesności* (Warsaw: Wyd. Scholar, 2004).

⁴ P. Sztompka, ed., *Imponderabilia wielkiej zmiany: mentalność, wartości i więzi społeczne czasów transformacji* (Warszawa-Kraków: Wyd. Naukowe PWN, 1999), 265–82.

⁵ Z. Kwieciński, “Edukacja wobec nadziei i zagrożeń współczesności,” in *Humanistyka przełomu wieków*, ed. J. Koziński (Warsaw: Wyd. Akademickie “Żak”, 1999), 56–57.

⁶ *Słownik języka polskiego* (Warsaw: Wyd. Naukowe PWN, 1994), 515.

role in shaping the functioning of democracy and civil society. In addition, it helps drive increases in the productivity of human capital, which directly affects economic growth. Better education leads to an increase in the qualifications of the workforce, so it is an important instrument in fighting unemployment.

While education is a good, threats or insecurity are valued negatively, and seen as things to avoid and combat. The lack of security or the diminishment of a sense of security are treated as threats, phenomena that are dangerous both to the current existence of life and its future prospects. A threat is—for some—a subjective emotional state, associated with an inability to realize their needs, desires, and goals. It is the lack of feeling good (security). For others, a threat is an objective state connected to instability, to changes in the status quo. In the objective case, instability and change are threats that one will have to deal with. It is unambiguous, neither good nor bad. The threat may be constructive or deconstructive for security; it may contribute to safety or weaken it.⁷

Due to these different understandings of security (subjective or objective), much has been written about it, because it is a multivalent term and because there is in fact currently no area of activity, either intangible or material, where security does not play an important role.⁸ It represents an area of interest in disciplines as diverse as philosophy, military science, political science, psychology and pedagogy, sociology, cybernetics and systems theory, and many other disciplines and sub-disciplines of modern science. Moving into the area of educational science, security has supplanted education in the areas of defense, military and military preparation. The result is that, since the early 1990s, “education for security,” has been increasingly gaining recognition.⁹

Security education is sometimes defined narrowly and instrumentally as the entire education process that is designed to shape the values, dissemination of knowledge, and procurement of skills that are important for ensuring national sovereignty (national security). From the perspective of the philosophy of education, security identified with preparing people to fight (war) and to work (peace) to improve or stabilize their lives.¹⁰

⁷ J. Świniarski, op. cit., p. 134.

⁸ J. Kaczmarek, *Bezpieczeństwo*, Myśl Wojskowa 1998, nr 6, p. 5.

⁹ R. Stępień, “Załamania i odnowa edukacji obronnej - sens nowych perspektyw myślenia,” in *Edukacja obronna w systemie bezpieczeństwa Polski*, eds. Edward Jezierski & Walerian Magoń (Bydgoszcz: Arcanus, 1997), 123–26; T. Jemioło & R. Stępień, eds, *Dylematy wychowania wojskowego* (Warsaw, 1997); and R. Stępień, ed., *Edukacja dla bezpieczeństwa*, Materiały z konferencji naukowej, 23-24 May 1994 (Warsaw 1994).

¹⁰ J. Świniarski, *Filozoficzne podstawy edukacji dla bezpieczeństwa* (Warsaw: Egros, 1999), 125.

Undoubtedly, the purpose of that education is above all to prepare people to live with a sense of assurance, stability, and development (and it is obvious that the conditions that are conducive to this are national sovereignty and national security). This education also helps people to achieve as objective states forms of existence, values, and actions, and to create stability and increase opportunities for development and improvement. This kind of condition does not require national sovereignty, but rather subjective and personal sovereignty, respect for human dignity and freedom, for individual rights and welfare.

Of course, the state's claims to sovereignty and national security are not in conflict with the personal-subjective sovereignty of its citizens. However, in the state does come into conflict with individuals' security when it deprives citizens of liberty, fails to obey the law, and does not provide the conditions for economic prosperity. Security cannot be exchanged for such personal values as freedom, respect for the law, welfare, and responsibility. It is true that exchanges of this kind falsely suggest totalitarian regimes such as North Korea, Cuba, but since (at least) the Spartan regime and the experiment inspired by Plato in Syracuse, citizens deprived of their personal values and individualism have lost the possibility to develop and fulfill their highest potential. It is no surprise that, sooner or later, regimes of this kind were neglected and eventually fell.¹¹

Education for security—in an intentional sense, that aims to effect change at the level of culture—should underscore the overriding importance of a concern for the preservation and improvement of life as its primary goal. Safety is perhaps the most important value of human nature, and is taking an increasingly prominent role as a social value as well.

The importance of education for security has increased with the development of Western civilization, as it has moved into eras characterized by industrialization and urbanization. This shift was brought about by a necessary adjustment in prevailing modes of thought about man's vocation, scope of action, technological progress, and the sustainability of the growth of human communities. The importance of education increases with the broadening understanding of freedom and human dignity, respect for the rule of law (particularly the United Nations' Declaration of Human Rights), the provision of universal prosperity, and the increasing global social tilt toward individualism.¹²

Connected to the issue of education for peace is the relationship between education for security and continuing education. The starting point is to solve a dilemma: whether to educate for war, and for behavior (and life) during times of military action or, on the contrary, to educate for peace, including behavior and life during times of

¹¹ J. Świniarski, *Przywództwo jako osnowa*, 135.

¹² *Ibid.*, 135.

no military activity. Extreme examples of these views are often treated as mutually contradictory, as leading toward militarism or pacifism. The specific emphases of these two approaches are, respectively, on educating people to exert command and apply constraint, and on collaboration and leadership. But between these two there can be a middle ground. This area holds a solution that leads to the concept of education for security. The implementation of this solution poses many difficulties, both theoretical and practical, which in turn requires a critical reevaluation of tradition and the theory of education.

The Values that Determine Human Security

Usually the term “value” is considered a basic category of axiology (the philosophical study of value). Systems and hierarchies of values define every culture. They depend on history, national traditions that are legacies of past generations, socio-economic conditions, relations among people and property, and the form of government.

We live in a world of different values. Human life consists of being confronted with endless choices. Nowadays we pay a great deal of attention to “axiological education”--that is, education that leads to conscious choices regarding values, as well as using a hierarchy of values as a basis used for forming one’s own philosophy, career goals, and lifestyle choices.

Axiological concepts influence educational goals for three reasons:

- Axiology provides a general perspective on the world of values
- Axiology helps determine educational goals in both large and small social groups
- Increasing attention is being given to individual hierarchies and value systems.

The fundamental value in modern axiology is the human being: his/her life, mental and physical development, self-realization, freedom, identity, and independence.¹³

A person’s hierarchy of values is one of the basic conditions that affects human behavior. Values direct attitudes, motives, behaviors, and lifestyle. They affect one’s evaluation of other people and events and determine one’s attitudes towards different objects. Values trigger motivations and shape human actions, but they are also the subjects of desires; they are the factor that regulate proceedings and give life more meaning. Every ideal or educational model has to be based on the understanding of the axiological specifics of human nature. Knowledge of education therefore has to be based on both knowledge of values and knowledge of human nature.

¹³ T. Lewowicki, *Przemiany oświaty. Szkice o ideach i praktyce edukacyjnej* (Rzeszów: Wyd. Foto “Art.,” 1994), 19.

Every human must make tough choices every day. Having knowledge about the nature of values and their meaning at home, at work, and in life is very helpful in navigating these choices. Values are an object of interest of the humanistic and social sciences. They help determine the mode of human existence, how people perceive their life and its quality, their interpersonal relations, their attitudes towards self, others, and the rest of the world. The question of values is the question of what we do, what we want, how we proceed, and how should we proceed. It is therefore the question what compass would provide us with the best guidance when we look to chart our own path in life.¹⁴

Education for peace-shaping values should lead gradually—by creating conditions for the experience of a stable system of values—to an understanding that stability is both possible and necessary, leading one to examine that the meaning of stability for oneself in one's own life. A man devoid of values does not progress past the stage of hedonistic and conformist standards. He evaluates options and makes decisions only on the basis of pleasure and benefit. Not only he is unable to make his own choices; he also does not realize that he has the power to make such choices, and that he is personally responsible for them.

Education for values is not precisely defined in the literature. Different authors emphasize in their interpretations a more instrumental or formation-oriented dimension of teaching.¹⁵ For the purposes of this article, I have relied primarily on an approach oriented toward axiological education.¹⁶ Axiological education consists of axiological training and education for values.

The purpose of this field of education is to prepare people for autonomous operation in the world of values. This concept allows us to distinguish between education for values and axiological education, which is the transfer of knowledge about values, including skills in evaluating hierarchies of values as well as oneself (including the clarification of values, as well as education in comparing and analyzing values due to different criteria). The axiological foundations for education are provided mainly by the humanistic social sciences. They allow us to comprehend the various psychological and social mechanisms of the assimila-

¹⁴ W. Heisenberg, *Część i całość* (Warsaw: Wyd. Państwowy Instytut Wydawniczy, 1987).

¹⁵ *Edukacja aksjologiczna*, red. K. Olbrycht; T.1. *Wymiary - kierunki - uwarunkowania*, Katowice 1994; T.2. *Odpowiedzialność pedagoga*, Katowice 1995; T.3. *O tolerancji*, Katowice 1995; T.4. *Wybrane problemy przekazu wartości*, Katowice 1999; K. Ostrowska, *W poszukiwaniu wartości*, Gdańsk 1994; T. Kukołowicz, M. Nowak (red.), *Pedagogika ogólna. Problemy aksjologiczne*, Lublin 1997; K. Denek, U. Morszczyńska, W. Morszczyński, S.Cz. Michałowski, *Dziecko w świecie wartości*, Kraków 2003; A. Szerląg (red.), *Edukacja ku wartościom*, Kraków 2004. [Author: please clarify these citations, and format them thus: Author, *Title* (Place of Publication: Publisher, Date of publication).]

¹⁶ Katarzyna Olbrycht, *Prawda, dobro i piękno w wychowaniu człowieka jako osoby* (Katowice: Wyd. Uniwersytetu Śląskiego, 2000).

tion of values, different ways of understanding values, and finally, the different types of values and ways of organizing them.

The best axiological education is no substitute for an education in values, however. As the student develops intellectually, it becomes an increasingly important factor in determining the effects of education. Education for values is essentially a mode of shaping an axiological orientation, which directed at more than merely providing a competence. It is a function of axiological maturity, one that expresses itself as a willingness to consciously and responsibly choose a value, respond to it, and embrace ability to choose. The result of an axiological education—axiological competence—is axiologically neutral. One can possess knowledge and ability while failing to orient their lives consciously toward a specific value. Orientation implies a general direction resulting from the choice of fundamental, basic abilities to organize specific values due to a chosen direction of life in accordance with decisions one has made.

Education for values is intended to prepare and encourage students to discover, live, organize, realize, and create values that result from the adoption of a specific philosophy of existence and exploration of the world. Any education, if it is not to be mere manipulation, must be essentially an education for values. These values are first inculcated in children with the help of adults, and then, as students grow older are more independently discovered and voluntarily chosen, as recognized in the sense of duties arising from a free choice.

The subject area of education for values is essentially the entire educational environment (understood broadly), which in varying degrees declares preferred axiological orientations, and rewards or forces certain choices. Education is heavily conditioned by the values that are recognized and implemented in a particular culture and society. Its effectiveness, however, depends primarily on the authority of educators. Education for values must therefore be considered as imparting the skills to identify a desirable and acceptable set of values and determine their priority. They must result from a particular vision of humankind and the world that provides arguments in favor of their adoption, and at the same time allows for a fair discussion of consequences. The educators who are to carry out this vision must accept it fully, and the fact of its adoption as the basis of education in educational institutions should be accepted by the relevant social actors.

A key consideration in this regard is an awareness of the hierarchy of values, a clear indication of which values are most important. This must also involve teaching the process of learning which specific values are subordinate to the primary values and require implementation, because if they are not fulfilled they will delay the achievement of those values that are most important for a given orientation. This awareness allows educators to treat students' decisions reflexively and evaluate them every day, because of the clearly defined hierarchy of values. One should not enforce

excessively formal, rigid value systems, but should correct students as they grow in line with the fundamental direction and purpose.

Another important element of such an education is shaping sensitivity to values, which is here understood as the ability to perceive the world and respond adequately to its actions. Simulations are therefore needed that may sharpen the desired values, associate them with a particular experience (e.g. willingness to conduct peace talks, negotiations, etc.).

One irreplaceable experience in this area is the opportunity to develop one's own specific action for a given value. The most important action is the one that requires effort, time, and work—an action that, by rejecting pleasure or conformism leads gradually to independence in formulating judgments and decision making. Well-formed character is the condition to conduct effective actions for recognized values. A secure character allows one to stand firmly by the values one has identified, even when confronted with challenges, vacillating motivation, and peer pressure.

But the most important way of assimilating values is contact with people who represent and embody the values. The lives of real people who consistently strive to act in accordance with certain values provides legitimacy for those values. It is therefore necessary for the education for values to refer to figures of personal, real authority. They may be heroes from literature or film, but the most important role is played by real people, whether living or dead. The precondition is that teachers provide a true presentation of these people, without retouching, since students are always very sensitive to perceived falsity.

In the context of determining the value of human security, we speak mostly of the three triads of values that are intertwined throughout history into one, the axiological center of European identity. In ancient Greece they took the form of the highest values: truth, goodness, and beauty. In Christianity, they constitute the basic virtues: faith, hope, and love. On the banners of the French Revolution, they were rendered as liberty, equality, and fraternity.

Modern civilization often seems to plunge into the chaos and crisis of education. It calls into question its meaning, casts doubt on the likelihood of agreeing on objectives for education, and is uncomfortable in expressing a preference for certain values. The truth about man and his values is not the truth of man, his development and goals. It is rather a picture of being doomed to struggle for success, or at least survival, alone in a dangerous world. In such a setting, the intense experience of pleasure, which constantly requires the acquisition of new resources, is the only fulfillment.

The path of such a re-evaluation is set by the concept of education for security. It is a redefinition that covers the role of the teacher, of the expectations placed on the teacher and the rights granted to him. It also requires an internally coherent system of behavior that is necessary for effective management and teaching.

Given the issues outlined above, it is worthwhile to stress that the fundamental

concept of the system of education for security cannot be achieved merely by changing the structure of the existing system. The future of this system depends primarily on the content and values within a structure that will be developed and disseminated from scratch. The value system of national symbols, a common culture and habits also has a positive effect on the creation of national identity, which is an inherent factor in security education.

The process of education for peace and security is also significantly influenced by regional challenges. In Europe these challenges are mainly associated with the systemic changes in the countries of Central and Eastern Europe brought about by the disintegration of the communist system and the end of the Cold War, and the ongoing process of integration, which has had an impact on every area of society.

These challenges pose important tasks for both philosophy and science, including pedagogy and education for security. In education, one should promote the fact that cognition and addressing challenges is a condition for avoiding threats, or for viewing circumstances as opportunities rather than dangers. Education in general, and education for peace and security in particular, can serve to impart to students the proper knowledge and shape their skills, attitudes, and value systems in ways that are conducive to building and protecting a safe and peaceful world.

Education for peace and security that is commensurate to the challenges of the twenty-first century should consider:

- The prudent application of pedagogical achievements of different countries throughout the European Community
- How best to enable the reconciliation of national interests for the common good of Europe
- Ways to overcome stereotypes and prejudices against European integration, while also highlighting the benefits and difficulties associated with it
- The promotion of sustainable values of European culture, which are “points of support” for the process of building democracy in Europe and around the world
- How to defend and protect the human dignity and human rights, which are important components of peace and security.

Conclusion

Education for peace and security is an area of pedagogy that is constantly acquiring new dimensions, many of them related to the issue of multiculturalism. Social mobility, migration, and unprecedented development of all types of tourism have revealed the ineluctably multicultural face of the world, and has raised awareness among many people to issues of diversity. Dialogue between cultures is increasingly important in educational contexts, in both the global and local dimensions, but it needs to be put in practical, concrete terms, so that students’ experiences can be enriched through

learning about and experiencing human different. Through such experiences, the new problems of unity and diversity within the world suddenly take on new vividness. They are expressed primarily through a new understanding of culture. And this understanding of culture justifies the need to seek out the basic elements of universal ethics, based on the rights and responsibilities of human beings in their humanistic integrity, which in turn make it possible to identify values that must be common to all members of the new global community, including

- The rights and responsibilities of human beings
- The values of democracy and civil society
- The obligation to provide protection for minorities
- The importance of resolving conflicts peacefully and through negotiations
- The equality of the sexes.

Peace and security seem to be particularly timely subjects for education in this historical moment, and their implementation is urgent because of the situation in the contemporary world. Peace cannot be defined as the absence of war, but rather should imply that there is harmony in all areas of human life and conduct. All the arrangements adopted in the field of human rights are related to the recognition of peace as a basic condition of human existence. Education for peace must rely on the transmission of universal values and training in permanent attitudes, as well as on developing the skills to allow individuals to be active citizens in the modern world.

International Arms Control and Law Enforcement in the Information Revolution:

An Examination of Cyber Warfare and Information Security

*By Yury Barmin, Grace Jones, Sonya Moiseeva, and Zev Winkelman **

Introduction

Cyberspace influences nearly every human being in the world, as well as virtually every area of government, industry, commerce, and education. The developments of the revolution in information technology have been a source of tremendous innovation, but as the world has increased its dependency on technology for its most basic functions, it has also become more exposed to the underlying vulnerabilities in cyberspace. These vulnerabilities continue to be probed and exploited at an increasing rate, and as a result, cyberspace has become not only a major area of concern for international security, but also a new *de facto* military arena. The United States and Russia both possess significant capabilities in this realm, and their cooperation is essential to international safety and security in the era of the information revolution.

One of the biggest obstacles to greater cooperation between the U.S. and Russia in the area of cyber and information security is the U.S. emphasis on law enforcement, and Russia's concern with arms control. Both have identified criminal and terrorist use of the tools of the information revolution as potential threats to international security. However, they have not agreed as to whether military activities in cyberspace also require international regulation and control. In the early stages of international cooperation on cyber and information security, the greatest emphasis was placed on combating cybercrime. The most substantive achievement of this cooperation was the Council of Europe's (CoE) Convention on Cybercrime, which was opened for signature in Budapest on 23 November 2001.¹ The U.S. has signed and ratified the Convention, and was actively involved in its development.

Although Russia is a CoE member, it has neither signed nor ratified the Convention, primarily out of its objection to one of the Convention's provisions that allows for

* This article is drawn from the final report of Group 6 at the 2010–11 Stanford U.S.–Russia Forum. The members of Group 6 include: Yury Barmin, a fourth-year student at the Linguistic University of Nizhniy Novgorod; Grace Jones, a junior at Stanford University; Sonya Moiseeva, a first-year student at the Academy of the National Economy in Moscow; and Zev Winkelman, a Ph.D. candidate at the Goldman School of Public Policy at the University of California, Berkeley.

¹ Council of Europe, *Convention on Cybercrime* (2001); available at <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>.

unilateral trans-border access of data by law enforcement agencies of one country without notifying the authorities in another country, thus, Russia claims, violating state sovereignty. Russia's approach has been to call for international cooperation that also places some limitations on military uses of information communication technologies. The U.S. response to the Russian proposals has been a reluctance to engage in any formal discussion of limiting military operations in cyberspace, and an emphasis on the importance of the law enforcement approach. This reaction is in part due to skepticism that such limitations could be enforced in any fashion whatsoever, let alone symmetrically. Despite some recent positive signs of engagement,² this stalemate has held for more than a decade. The predicted cyber arms race has begun, resulting in the further expansion of cyber capabilities in the U.S. and Russia, as well as many other countries.³

The current stalemate between the two nations is only one piece of the puzzle in a long history of tensions over the cyber world, and more specifically cyber crime. There have been numerous significant attacks launched in cyberspace, including attacks by both Russia and the U.S. In 1982, Russia's infrastructure took its first hit from a cyberweapon, when a virus was inserted into the USSR's SCADA (Supervisory Control and Data Acquisition) software, resulting in a powerful explosion on the Soviet Urengoy–Surgut–Chelyabinsk natural gas pipeline. There have also been a number of cyber breaches in the U.S., including 2002 incident where a hacker illegally accessed computers at NASA's Jet Propulsion Laboratory; a teenager breaking into the systems of NYNEX in March 1997, the then-dominant telecom utility in the northeastern U.S., and cutting off Worcester Airport in Massachusetts for six hours, affecting both air and ground communications; and numerous other cases, involving both security threats and thefts of personal information.⁴ A relatively new kind of cybercrime appeared in 1999, when an organized group of hackers allegedly based in Yugoslavia carried out a politically motivated, coordinated attack aimed at blocking NATO's computer networks.⁵ Other attacks of this kind have been carried out

² John Markoff, "At Internet Conference, Signs of Agreement Appear Between U.S. and Russia," *The New York Times* (15 April 2010); available at http://www.nytimes.com/2010/04/16/science/16cyber.html?_r=1.

³ David Talbot, "Russia's Cybersecurity Plans," *Technology Review* (16 April 2010); available at <http://www.technologyreview.com/blog/editors/25050/>.

⁴ U.S. Department of Justice, "Juvenile Computer Hacker Cuts off FAA Tower at Regional Airport," 18 March 1999; available at <http://www.justice.gov/criminal/cybercrime/juvenilepld.htm>.

⁵ Jose Nazario, "Politically Motivated Denial of Service Attacks," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009); available at http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf

every year since then, including cyber attacks on U.S. military networks following the collision of a U.S. surveillance aircraft and a Chinese fighter plane in 2001, and a cyber attack organized by Russian hackers on a website called “Kavkaz Center” that promotes Chechen independence.⁶ Cyber attacks have grown more frequent and destructive in recent years, including new forms of hacking called denial of service attacks (DoS) that have become a tactic of war since 2000. Today the Pentagon reports some 369 million attempts to break into its networks annually, compared to 6 million attacks in 2006.⁷

The immense threat that cyber attacks pose to critical infrastructures and state operations is clear, and recent developments in both the U.S. and Russia have emphasized the importance of addressing these issues now. In 2008, the U.S. experienced the most serious penetration of its classified military networks to date. Subsequently, on June 23 2009, U.S. Secretary of Defense Robert Gates directed U.S. Strategic Command to establish the new U.S. Cyber Command.⁸ Though its cyber force structure is less clear, Russia has recently been contributing to the creation of an information security policy for the Shanghai Cooperation Organization (SCO), an alliance that includes another cyber “titan,” China.

Though it is unlikely in the near term that Russia will sign the CoE Convention on Cybercrime, or that the U.S. will accept international regulations that limit its military cyber capabilities, we believe that there are several important steps that should be taken now to foster a continuous level of cooperation on cyber and information security issues that may allow for such agreements to be reached in the future. In order to provide adequate background and substantiation for our recommendations, we will first provide background on current U.S. cyber policy, Russia’s information security policy, and the impact of international law in cyberspace. Finally, we will propose a set of recommendations for cooperation between the U.S. and Russia that we believe will solve some of the problems identified by both nations.

⁶ Ibid.

⁷ Randy James, “A Brief History of Cybercrime,” *Time* (1 June 2009); available at <http://www.time.com/time/nation/article/0,8599,1902073,00.html>.

⁸ William J. Lynn, III, “Defending A New Domain: The Pentagon’s Cyberstrategy,” *Foreign Affairs* (September–October 2010); available at <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.

Background

U.S. Cybersecurity

In the United States, responsibilities for cybersecurity are scattered across many government agencies. One of the greatest areas of concern, especially for the Department of Homeland Security, is the protection of the nation's critical infrastructure. The Department of Justice focuses on the problem of cybercrime, as well as finding the balance between security and the protection of civil liberties and privacy rights. In order to understand the relationship between matters of cybersecurity and foreign policy, however, two other stakeholders are key: the executive branch and the military. President Barack Obama recently ordered a detailed review of cyberspace policy, which included an analysis of current threats and possible solutions.⁹

Released in May 2009, the "Cyberspace Policy Review" is the most current document detailing the executive branch's position on cyberspace. Numerous stakeholders are identified, including private sector enterprises, academia, international organizations, including the UN, NATO, and the CoE, as well as various domestic government agencies such as the National Infrastructure Advisory Council and the Joint Interagency Cyber Task Force.¹⁰ Using these key stakeholders, the review identifies several major problems facing the United States in its approach to cyber and information security, including the lack of organization in the federal government to address the growing threat, the difficulties presented by maintaining security on a network owned by the private sector, and risks to security from non-state actors who could one day cause critical damage to the U.S. infrastructure and government by compromising or stealing information.¹¹ Among the evidence of these problems cited by the review is the lack of a coordinated response by government agencies to the Conficker worm, which was activated on 1 April 2009,¹² along with a continuing game of catch-up against exploitations leading to data theft resulting in USD 1 trillion lost as well as reports by the CIA of malicious activity.

The core proposals for the near term include increased coordination through a new central policy official who would be responsible for the nation's cybersecurity, the preparation of a response plan, improving collaboration between agencies and with other governments, and a continued campaign to inform the public about the

⁹ The White House, "Cyberspace Policy Review," May 2009. See also Melissa Hathaway, "Securing Our Digital Future," *The White House Blog* (29 May 2009); available at <http://www.whitehouse.gov/CyberReview/>.

¹⁰ The White House, "Cyberspace Policy Review."

¹¹ *Ibid.*

¹² *Ibid.*

issue.¹³ Recently, this last recommendation was bolstered by the release of President Obama's new budget, which entailed a large increase in cybersecurity research and development.¹⁴ In the medium term, the review proposes creating mechanisms to generate strategic warnings, further analyzing threat scenarios, and creating a network that will act during a crisis. Medium-term goals also focus on increased communication to solve interagency disputes, and using the Office of Management and Budget's framework to ensure that budgets are used for cybersecurity goals.¹⁵ The report also emphasized some other key factors: improving the partnership between the private sector and the government through information sharing; partnering effectively with the international community through new agreements to enhance identification, tracking, and prioritization; building more resilient systems that will enhance the survivability of communications during a national crisis; and maintaining national security through a coordinated plan. The Cyberspace Policy Review clearly establishes cybersecurity as a top priority for the agencies of the U.S. government.

In 2011, the Center for Strategic and International Studies reviewed the progress on the Cyberspace Policy Review in a report on called "Cybersecurity Two Years Later."¹⁶ The report claimed that, although progress has been made in most areas, in no area has the progress been sufficient. Furthermore, the report described the debate on cybersecurity solutions as being stuck on old ideas of public-private partnerships, information sharing, and self-regulation that have fallen short for decades, and stressed the need for new concepts and strategies. The fear that only a cyber "9/11" would lead to any progress was made even greater by the prospect that waiting for such an event to take place would likely lead to suboptimal and possibly draconian policy solutions.

Among the report's revised observations are two that are particularly relevant to our analysis of opportunities for bilateral steps that can be taken by the U.S. and Russia. The first is a call for the development of a U.S. vision for the future of the global Internet that engages other nations, and acknowledges a shift away from the original U.S.-centric idea of governance by a private global community, as nations seek to extend their sovereign rights to cyberspace. This engagement could lead to an increase in the number of indictments, convictions, and extraditions related to cybercrime. The second is recognition that the cybersecurity community can now

¹³ Ibid., 37.

¹⁴ Patrick Thibodeau, "Obama Seeks Big Boost in Cybersecurity Spending," *Computerworld* (15 February 2011); available at http://www.computerworld.com/s/article/9209461/Obama_seeks_big_boost_in_cybersecurity_spending?taxonomyId=70.

¹⁵ The White House, "Cyberspace Policy Review," 38.

¹⁶ CSIS Commission on Cybersecurity for the 44th President, "Cybersecurity Two Years Later," January 2011; available at http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

identify practices that reduce risk, teach these practices to personnel, and measure their results. These observations provide support for the recommendations offered later in this article.

The U.S. military has also identified key issues in the cyber debate and has offered its own set of recommendations. Three important sources relevant to the military's stance on cybersecurity are: definitions of information operations concepts; recent comments from the commander of U.S. Cyber Command, General Keith Alexander; and Deputy Secretary of Defense William Lynn's recent article "Defending a New Domain."

First, the U.S. armed forces are expected to release the new U.S. Information Operations Concepts, in which they will offer a clear definition of "information war." It appears that the document will define "information war" as strictly information operations limited to offensive and defensive activities.¹⁷ In addition, information superiority is the main goal of information operations, as it will allow commanders to seize, retain, and exploit the initiative.

William Lynn discusses additional background issues, concerns, and recommendations. Lynn begins by emphasizing the importance of cybersecurity in light of the most significant breach of U.S. military computers to date, in 2008, when classified military networks were compromised.¹⁸ Lynn notes that the size and depth of the United States' digital infrastructure still gives it a critical advantage over any adversary. Although the U.S. offense is dominant, Lynn argues that this means that its defense needs to be dynamic, including ordinary inspections all the way to a third level of security using highly specialized active defensive tactics.¹⁹ Lynn additionally recommends that the government increase the number of personnel dedicated to U.S. cybersecurity issues, and improve tactics to acquire the latest information technology. Lynn also focuses on the critical role of allies, and the necessity of shared warning systems and stronger agreements to facilitate the sharing of information and technology. Throughout Lynn's article he emphasizes the widespread impact that a cyber attack would cause, and ways to make the U.S. more secure, but his ultimate goal is to make cyberspace safe.²⁰

General Alexander has defined some of the current problems with cybersecurity as the difficulty of centralizing command, the complexity of cyberspace systems, the growing threats that could seriously damage our ability to operate as a country, and the ability to work with other agencies to combat cyber terrorism.²¹ As solutions to

¹⁷ T. Thomas, *Comparing U.S., Russian and Chinese Information Operations Concepts* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004).

¹⁸ Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy."

¹⁹ *Ibid.*

²⁰ *Ibid.*

²¹ General Keith Alexander, Interview with Center for Strategic and International Studies, 3 June 2010.

these and other problems, General Alexander highlights the consolidation of command over cybersecurity in the creation of the U.S. Cyber Command. Cyber Command leads day-to-day protection efforts, distributes its cyber resources across the military, and works with many partners inside and outside of the U.S.²² In addition, General Alexander suggests that we need to understand our own networks from the perspective of real-time operations, and to ensure freedom of movement in cyberspace. General Alexander goes on to say that part of the solution may require establishing clear rules of engagement.²³ Similar to Lynn's goal of making cyberspace safe, General Alexander defines the goal of cybersecurity as minimizing the effect of cyber attacks on U.S. persons and not infringing on civil liberties while protecting national security—similar to the balancing act described by the executive branch review.

When questioned about Russian proposals for a cyber treaty, General Alexander responded that such issues should be handled by policy leaders, not generals, and that the Russian proposal may serve as a starting point, but that the U.S. should develop a counter-proposal. Taken together, Lynn and Alexander offer a complete view of the U.S. military's perspective, emphasizing the security threat of cyber attacks and their potential widespread impact on the population. Both also offer tangible policy recommendations to increase cybersecurity and enhance cooperation at the domestic and international level. The U.S. executive branch and the military both have substantive ideas about how to make cyberspace safer. Initiatives like strategic warning, and better definitions for concepts in cyberspace and information operations, could be enhanced through international cooperation.

Russian Information Security²⁴

Just like the United States, Russia is a “titan” of information security. Currently there are many perspectives on cybersecurity at play around the world, but Russia is primarily focused on the military aspects of the issue. Russian cybersecurity expert

²² Ibid. See also William Lynn, “Defending a New Domain: The Pentagon’s Cyberstrategy.”

²³ Ibid.

²⁴ For further background on the Russian approach to information security, see Vladimir P. Sherstyuk, ed., *Scientific and Methodological Problems of Information Security* (Moscow: Information Security Institute of Moscow State University, 2004); Machulskaya I. A. Penjkov, “Information Security of the Russian Federation,” The Council of the Federation of the Federal Assembly of the Russian Federation, Moscow, 2005; Doctrine on the Information Security of the Russian Federation,” signed by President Vladimir Putin on 9 September 2000 (No. Pr-1985); Marko Gercke, *Understanding Cybercrime: A Guide for Developing Countries* (Geneva: International Telecommunication Union (ITU), 2009); and Dylevski S. Korotkov and S. Komov, *Military Aspects of Ensuring International Information Security in the Context of Elaborating Universally Acknowledged Principles of International Law* (Geneva: United Nations Institute for Disarmament Research, 2007).

S. P. Rastorguyev defined “information war” as a battle between states involving the use exclusively of information weapons in the sphere of information models. The final objective of an information weapon’s effect is the knowledge of a specific information system and the purposeful use of that knowledge to distort the model of the adversary’s world. Rastorguyev emphasizes that there are two key aspects to any information war—information-technical and information-psychological—which makes it more dangerous than any conventional war.

Information war poses a new type of threat, and one that Russia is trying with difficulty to confront. In 2005, the Federal Council of the Russian Federation released a political analysis of cybersecurity in Russia, in which it acknowledged that Russia was not ready for the transition to an information society. Russia’s critical infrastructure was threatened due to key vulnerabilities in cybersecurity, stemming from Russia’s inability to keep up with the fast pace of information technology development at the time. The Russian Federation recognized several kinds of threats to the cyber sphere. The first threat is information weapons, which can influence the technical infrastructure of the society, and can also influence people psychologically. The second threat is that of financial crime, which involves the use of modern computer technologies. The third threat is that of electronic control, whereby one tracks the daily activities of individual citizens. And the final threat of information weapons is the potential political applications they possess to introduce informational totalitarianism, expansionism, and colonialism. Thanks to the latest technology, information technology’s influence on the enemy has evolved from individual information sabotage and acts of disinformation to a way of exercising international policy that is both massive in its implications and pervasive in its application. Among its recommendations, the Federal Council stressed the need for even more global cooperation, and made specific recommendations for Russia, including improving legislation on cyber and information security, developing a state system of protecting information as well as classified information, and applying new Russian scientific technologies in the cyber sphere.

The fundamental document that defines the Russian government’s position on the issues of information security and the threats posed by it is the Doctrine on the Information Security of the Russian Federation, signed by then-President Vladimir Putin in 2000. It explains the government’s official views on the goals, tasks, principles, and main directions of ensuring the information security of the Russian Federation. This document provides the basis for shaping state policy regarding ensuring the information security of the Russian Federation; preparation of propositions on improving the legal, methodological, scientific-technical, and organizational support for Russia’s information security efforts; and the development of target-specific programs for enhancing the Russian Federation’s information security.

As defined by the Doctrine, Russia's main concerns deal with the military application of cyber technologies. The contemporary level of information technology may enable the commission of new kinds of terrorist acts. Cyberterrorism has been identified by the Russian government as another grave threat to international peace. Terrorist acts in cyberspace have several goals today, including destroying infrastructures at the national and transnational level, as well as accessing unauthorized information. To prevent all types of threats at the operational level, it is crucial to maintain the physical security (including physical access control) of key elements of network infrastructure and software, and on a technical level to have logging and active audit systems to detect abnormal situations that can destructively impact functionality. Early detection, as well as prompt and adequate responses to these situations, is also essential to providing a higher level of security.

In order to provide better security and counter the threats discussed above, Russian officials have always favored the idea of international cooperation. The Shanghai Cooperation Organization—founded by Russia, China, Kazakhstan, Kyrgyzstan, and Uzbekistan—aims at maintaining peace, stability, and greater security in the organization's member states in general, and in Central Asia more particularly. This stability includes strengthening trust between the members, opposing threats to international information security (IIS) by improving existing and building new counter measures, improving mechanisms for joint actions between the SCO member states, and opposing information terrorism. It is important to note that SCO states should align their military policies so as not to proliferate information weapons and technologies. This is a statement promoted by Russia. Russia believes that the most effective way to achieve this goal internationally would be a collective statement of the member states of the United Nations of their adherence to the principle of non-proliferation of information weapons.

Russia's commitment to international cooperation also includes joint work with law enforcement groups within the so-called 24/7 Network, consisting of forty-eight participating countries.²⁵ The idea of the 24/7 Network is based on the existing network for twenty-four-hour contacts for international high-tech crime from the G8 Nations. With the creation of the 24/7 network, law enforcement authorities of the participating states cooperate with law enforcement authorities of other countries in order to detect, prevent, combat, and disclose cross-border crime in the information sphere; exchange operational and other relevant information of interest; execute requests for assistance in preventing, combating, and solving crimes; and organize and conduct search operations on the Internet to identify, prevent, and document cross-border crime.

²⁵ Albert Rees, "24/7 High Tech Crime Network," Department of Justice Computer Crime and Intellectual Property Section (April 2007): available at http://www.oas.org/juridico/english/cyb20_network_en.pdf.

Russia's definition of "information security" is much broader than the United States' rubric of "cybersecurity," but this allows Russia to incorporate much broader security goals, extending from individual psychology to critical infrastructure. Russia is highly concerned with the threats posed by information security. Thus, its primary goals are focused on international efforts that limit military capabilities while protecting critical infrastructure and other key components of the nation threatened by cyber attacks.

International Cyber and Information Security Activity

Computer crime and warfare do not simply affect the cyber sphere, but can extend to elements of critical infrastructure, including power grids, hospitals, financial institutions, telecommunication systems, oil and gas pipelines and refineries, and numerous other areas not usually identified with cyberspace. It is critical to demonstrate the wide scope that cyber attacks can have when examining the threat of cyberwar. The most well-known cyber weapon of recent times is Stuxnet. This computer worm, which was uncovered in 2010, is reportedly the first malware to include a program logic controller rootkit.²⁶ Stuxnet was allegedly used to target the Iranian nuclear program, as it infected personal computers of the staff at Iran's first nuclear power station. It was then capable of seizing control of the plant and ultimately destroying it. Some Western experts say its complexity suggests it could only have been created by a "nation state," being beyond the capacity of an individual hacker.²⁷ A computer worm can easily spread and infect even highly secured objects, and its damage and lasting effects can be irrevocable.

The example of Stuxnet demonstrates how widespread the effects cyberwar can be, and thus cyber warfare, just like any other arena of war, does not take place solely bilaterally, but rather predominantly in an international sphere. Although both the United States and Russia each have their own prerogatives and goals when it comes to cyber and information security, the rest of the international community is also involved in the effort, and has grappled with the same problems that the two individual states have been confronting. However, international law has struggled to keep pace with the impact of the emerging technologies of the information revolution on international security. In what might be called the first phase of the international debate on these issues, a significant discussion took place on how existing international law regarding the use of force and armed conflict should be applied to new cyber-enabled scenarios.

²⁶ Liam O'Murchu, "Last Minute Paper: An In-depth Look into Stuxnet," *Virus Bulletin* (2010); available at <http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml>.

²⁷ "Stuxnet Worm Hits Iran Nuclear Plant Staff Computers," *BBC Online* (26 September 2010); available at <http://www.bbc.co.uk/news/world-middle-east-11414483>.

In the second phase of the debate, those carrying out mischievous cyber actions were often criminals, and the international community began grappling with the problem of cybercrime. In the third and current phase, the unsolved cybercrime problem has been compounded by a greater military focus on attack and defense in what has been recently labeled as a new domain of warfare comparable to land, sea, air, or space. In each phase, problems that went unaddressed have become almost inextricably tangled with each other, further complicating the international community's response.

Phase I: International Law²⁸

In the first phase of applying current international law to the area of cybersecurity, three critical problems emerge: ambiguity, anonymity, and espionage. Defining what constitutes a threat or use of force in cyberspace depends on the facts, cases, context, relevant law, and circumstances. One must understand the law of conflict management and the contemporary norms of the UN Charter that regulate the use of force during peacetime, including necessity, proportionality, unnecessary collateral damage, and anticipatory self-defense. Short of a declaration of war or an occupation, there is no international armed conflict until a given use of force of a specific scope, duration, and intensity reaches the level of armed attack as defined under Article 51 of the UN Charter.

International law clearly permits self-defense in response to cyberspace attack under certain circumstances. Anticipatory self-defense is permissible when the necessity of self-defense is instant, overwhelming, leaves no choice of means, and no moment for deliberation. States have an obligation to refrain from a threat or the use of force against the territorial integrity or political independence of another state. But states never lose the right to necessary and proportional self-defense. Nevertheless, the right to self-defense may not justify an armed response. Any response must be necessary and proportional, and it requires a determination of the potential threat posed by the penetration of specific computer systems to the national interests of the state. Any computer network attack that intentionally causes any destructive effect within a sovereign state is an unlawful use of force under Article 2(4) to the extent that it may produce the effects of an armed attack, and thus prompt the right of self-defense.

If the identity of the attacker is known, a victim may respond in a manner that is both necessary and proportional, in kind in cyberspace or with more traditional use of force. The difficulty remains to determine identity. Anonymity undermines both deterrence and the ability for self-defense. The real challenge may not be whether international law will permit the use of force in self-defense, but whether technology will enable a state to respond by identifying an intruder or attacker.

²⁸ Walter Gary Sharp, Sr., *Cyberspace and the Use of Force* (Falls Church, VA: Aegis Research Corporation, 1999).

Espionage, including non-consensual penetration of computer systems, is recognized as an essential part of self-defense, whose lawfulness during armed conflict is recognized by the 1907 Hague Convention IV regarding the laws and customs of war, and in peacetime by the 1961 Vienna Convention on Diplomatic Relations. It may demonstrate hostile intent on the part of an intruding state, and it may invoke the victim state's right to anticipatory self-defense, but state practice has recognized a right to clandestine intelligence collection as part of foreign relations policy. It is only unlawful under the domestic law of most states. Elements of cyberspace infrastructure, such as telecommunications systems, computers, and satellites, have been used in intelligence collection since their invention under the tactical concept of information operations. However, the same tools that are used for espionage can also enable pre-attack exploration, or an actual attack. Hostile and potentially destructive acts are only one keystroke away, and may materialize into unlawful use of force at the speed of light. But, short of an actual destructive attack, it is difficult to be sure of intent. A legal regime that fails to recognize the ability of a state to defend itself before it has been attacked is unacceptable, and the difficult problem of attribution of responsibility for an attack remains.

Phase II: Convention on Cybercrime²⁹

The Council of Europe's Convention on Cybercrime is the most substantive, and broadly subscribed, multilateral agreement in existence today that focuses on issues related to cybercrime. Its most relevant properties with regard to the U.S. and Russia are its heavy Western influence, and a controversial provision for unilateral trans-border access by law enforcement agencies to computers or data with the consent of the computer or data owner.

The U.S. actively participated in the negotiations in both the drafting and plenary sessions, and both the U.S. Department of Justice and the U.S. Senate took the position that the Convention required no implementing legislation in the United States. Though the CoE includes forty-seven member states, including all twenty-seven members of the European Union as well as Russia, China is not a part of the CoE, and Russia has frequently repudiated the Convention. Given that these two countries have been widely identified as the source of some of the most serious cyberattacks in recent years, and that some of these attacks are suspected to be state sponsored (or, at least, state tolerated), their absence from the treaty is all the more troubling. Com-

²⁹ Michael Vatis, *The Council of Europe Convention on Cybercrime*, Proceedings of the Workshop on Detering Cyberattacks: Informing Strategies and Developing Options (Washington, D.C.: National Academies Press, 2010); available at http://sites.nationalacademies.org/CSTB/CSTB_059441.

pounding the lack of participation from these two key players is the fact that there is not a single nation from Asia, Africa, or South America that has ratified the treaty.

Russia has not signed the Convention, let alone ratified it, largely due to the controversial remote search provision, which is seen by Russia as an unacceptable violation of national sovereignty. The UN has also expressed concern about the reluctance of non-CoE states to accede to a treaty that they had no hand in developing. The International Telecommunication Union (ITU), the UN agency responsible for information and communication technology issues, has advocated for its ITU Toolkit, created with global participation, as a model for legislation for countries to adopt, allowing them to harmonize national legislation without a requirement to join an international treaty. Despite these criticisms, the CoE has pushed back, arguing that what is needed is to get more countries to accede to the Convention, not to reinvent the wheel. The convention has received strong support from the Asia-Pacific Economic Cooperation, the European Union, Interpol, the Organization of American States, and the private sector.

The goal of the Convention is to protect society from cybercrime by providing for the criminalization of such conduct, the adoption of powers sufficient for effectively combating such criminal offenses, the facilitation of their detection, and ultimately their investigation and prosecution. These objectives are accomplished primarily through arrangements for fast and reliable international cooperation.

The Convention requires signatories to establish certain offenses as criminal under their domestic law, when they are committed intentionally. These offenses include but are not limited to: obtaining access to or seriously hindering the functioning of a computer system without right; interception of communications without right; input, damaging, deletion, deterioration, alteration or suppression of computer data without right; and the willful infringement of copyright and related rights.

Two of the most important provisions designed to facilitate investigation address the preservation of data and the establishment of jurisdiction. The Convention seeks to enable a signatory's competent authorities to order or similarly obtain the expeditious preservation of specified computer data from another signatory. Signatories must also establish jurisdiction over any of the substantive offenses set forth in the Convention that are committed in their territory. However, the term "committed in the state's territory" is not defined. The examples neither explicitly include nor exclude the most critical case for international cooperation, that where the computer system attacked is outside the state's territory but the attacker is within it. Other forms of mutual assistance addressed by the convention include extradition, real-time collection of traffic data and recording of content data, wiretapping, the ability to spontaneously forward information to another party, and the designation of a point of contact available on a twenty-four-hour, seven-day-a-week basis to facilitate the necessary assistance.

The most controversial aspect of the Convention is the ability granted to states to access or receive through a computer system in its territory stored computer data located

in another state if the lawful and voluntary consent of the person who has the lawful authority to disclose the data is obtained, without the authorization of any other concerned state. During the negotiations of the Convention the controversy was settled by limiting unilateral actions to two types all could agree on, the other being open source data.

The Convention does not address the particular concerns that may be raised by cyberattacks that are not just criminal acts, but may also constitute espionage or the use of force under the laws of war. This gap is created by the caveat that offenses are committed “without right,” where the protection of national security is included. The negotiators of the Convention were primarily representatives of ministries of justice and foreign affairs ministries and law enforcement agencies; there was relatively little representation from any branches of the military. Therefore, the Convention does not deal with the issues that might arise when a nation is under cyber attack and cannot afford to wait for another state’s cooperation.

Phase III: Russian Proposals for a Cyber Treaty at the UN³⁰

As an alternative to the Convention on Cybercrime, Russia has focused on promoting a proposal in the UN to restrict what nation-states can do with cyber weapons. On 23 September 1998, the Russian Minister of Foreign Affairs Igor Ivanov wrote a letter to the UN Secretary-General calling for measures to be taken immediately to prevent a new area of international confrontation from emerging as a result of the information revolution. The letter identified the threat as emanating from information weapons, and described the resulting conflict as information warfare, which was defined as actions taken by one country to damage the information resources and systems of another while protecting its own. Furthermore, the letter suggested that the destructive effects of such information weapons were comparable to weapons of mass destruction.

The letter also included a draft resolution identifying the following three concerns:

³⁰ For more on Russia’s proposals to the UN for a treaty dealing with cyber and information security, see UN General Assembly A/C.1/53/3 (30 September 1998), available at <http://documents-dds-ny.un.org/doc/UNDOC/GEN/N98/284/58/pdf/N9828458.pdf?OpenElement>; UN General Assembly 53/70 (4 January 1999), available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement>; UN A/54/213 (10 August 1999), available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/235/97/PDF/N9923597.pdf?OpenElement>; UN General Assembly 54/49 (23 December 1999), available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/777/13/PDF/N9977713.pdf?OpenElement>; and UN General Assembly A/55/140 (10 July 2000), available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N00/535/02/PDF/N0053502.pdf?OpenElement>.

- The technology of the information revolution may potentially be used for purposes incompatible with the objectives of ensuring international security and stability and the observance of the principles of non-use of force, non-interference in internal affairs, and respect for human rights and freedoms
- In addition to military applications comparable to WMD levels of destruction, these technologies might be used to improve existing weapons or create new ones
- Beyond military use, such technologies might also be exploited by criminals and terrorists.

The draft also proposes to begin work on defining concepts such as “information weapons” and “information war”; to investigate international legal regimes to prohibit the development, production, or use of information weapons; and the establishment of an international center for monitoring threats to global information security.

On 10 August 1999, responses from Australia, Belarus, Brunei Darussalam, Cuba, Oman, Qatar, the Russian Federation, Saudi Arabia, the U.K., and the U.S. were reported in UN document A/54/213. The Russian response expanded on the initial proposal, adding emphasis to concerns over the military use of information weapons. The response stated that, as a result of the information revolution, the global and regional balance of power could be altered, giving rise to tension between traditional and emerging centers of power and influence. The cyber arms race that could ensue would threaten both individual states and collective security. Furthermore, the universality, efficiency, economy, secrecy, and impersonality of information weapons make them an extremely dangerous means of exerting influence. The Russian response explicitly stated that contemporary international law has virtually no means of regulating the development and applications of such threats. For these reasons, international legal regulation of civilian and military information technology is required to meet the needs of international security and to reduce the threat of the use of information technology for terrorist, criminal, or military purposes. This could be achieved by developing a code of conduct for states that could evolve from a multilateral declaration to an international legal instrument.

The U.S. response in A/54/213 was structured in five parts: general appreciation of the issues; international security aspects; economic, trade, and technical factors; law enforcement and anti-terrorist cooperation; and the advisability of developing international principles. With regards to international security and information security, the U.S. response cited the long history of national use of radio frequency jamming and electromagnetic counter-measures, and the likely future military use of technology to protect its own data links, as well as several other legitimate uses. In reference to economic, trade, and technical factors, the U.S. highlighted the importance of the need to protect scientific research and intellectual property, and of regulations that promote compatibility and safety in electronic systems.

The bulk of the U.S. response was a discussion of law enforcement and anti-terrorist cooperation. The U.S. pointed out the increased global vulnerability to criminals or terrorists as a result of the information revolution, and the fact that all states were both vulnerable and would remain increasingly so. It therefore focused on the criminal misuse of information technology. The United States' response called attention to domestic efforts to protect its own critical infrastructure, recognizing that these efforts depend in some part on the security of systems beyond its borders. Because of this dependence, the U.S. expressed the hope to place the focus on getting other states to take the necessary steps to secure their domestic information systems and to prosecute those who attempt to disrupt such systems to the fullest extent of the law. The U.S. cited its own long history of amending computer-related statutes to improve them in order to meet new problems.

Given these complexities, the U.S. response expressed the belief that it would be premature to formulate overarching principles pertaining to all aspects of information security. However, the U.S. recognized the importance of international cooperation to combat information terrorism and criminality, and cited the work being done by the CoE, the Group of Eight High-Tech Crime Group, the Organization of American States, and the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders. The U.S. response advised that it would be unwise for the General Assembly to formulate strategies that would interfere with work already under way.

Recommendations

Several goals for the U.S., Russia, and the international community have been defined above, as have preexisting conditions within each arena that would prohibit or accelerate existing policy recommendations related to cyber and information security. The pressure to develop offensive and defensive capabilities in the cyber realm is spreading, and 120 countries around the world are working on or have already developed information weapons.³¹ In addition, the issue of attribution of responsibility for cyber attacks is exceedingly difficult. One of the biggest obstacles to greater cooperation between the U.S. and Russia in addressing these problems is the United States' emphasis on law enforcement, and Russia's concern with arms control. Despite important differences in their perspectives on many core issues related to cyber and information security, both nations have emphasized the importance of working with the international community. Immediate bilateral cooperation between Russia and the U.S. could provide a foundation for further international cooperation including involvement with other key stakeholders in the cyber arena, most importantly China. Action can and should be taken in the fol-

³¹ Vladimir Sherstyuk, *Scientific and Methodological Problems of Information Security*, 87.

lowing three general areas: reducing vulnerabilities that lead to cyber attacks; expanding domestic initiatives for cyber and information security, where possible, to bilateral participation; and creating paths for increased levels of cooperation through ongoing engagement on cyber and information security which could someday lead to the level of engagement and trust necessary for a comprehensive bilateral or multilateral treaty.

Reducing Vulnerabilities

Though the attack vectors in cyberspace seem to be limitless, the vulnerabilities on which they depend are much more finite.³² This key asymmetry makes computer network exploitation (CNE) depend on the existence of such vulnerabilities, regardless of who originates the attack, for what purpose, or where they are located. An effort to eliminate as many of these vulnerabilities as possible might make the development of military weapons that exploit them more difficult, but it may not be as controversial as a limitation on the military's option to do so. Raising the bar of CNE to the point where it would only be an option for military organizations might simultaneously reduce the total number of incidents of CNE, and make the problem of attribution slightly less daunting.

Furthermore, CNE-enabling vulnerabilities in particular pieces of software or hardware are not the only vulnerabilities that can be targeted. Resilient system design, especially of critical infrastructure, and systems of systems, can help to mitigate the damage caused by individual component failures, or corruption at various stages in complex processes. By reducing the impact of such failures, the original incentive to attack these targets can be reduced, thereby increasing safety and security.³³ Again, contributing to such design improvements may make it more difficult for a military cyber weapon to take out a power grid, but doing so may be more feasible and acceptable than outright prohibitions on such actions.

Recommendation 1. The United States and Russia should jointly sponsor a bilateral research center for resilient system design and vulnerability mitigation by nominating one lead academic institution in each country and funding several yearly activities to be conducted by these organizations. Such yearly activities would include conferences to discuss joint research on resilient design, "bounty hunter" contests that reward researchers who discover existing vulnerabilities in widely used commercial and open source software and hardware, and possible joint research exercises in network security and forensics. All scholarship produced by this research center would be shared, contributing to the safety and security of both countries, as well as increasing engagement and trust in cyber and information security.

³² Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).

³³ Devabhaktuni Srikrishna, "Cyberwarfare: Surviving an Attack," *Public Interest Report* 63:3 (Fall 2010); available at http://www.fas.org/pubs/_docs/PIR_Fall_2010.pdf.

Expanding Domestic Initiatives to Bilateral Participation

The United States' Cyberspace Policy Review identified many domestic initiatives to secure cyberspace and harness the full power of the information revolution. Not all of these initiatives would be suitable for extension to bilateral participation. Nevertheless, any alternatives that could be identified as such would represent actions that have been deemed important to effectively coordinating a U.S. response across a complex and, in some ways, competing set of stakeholders. If such mechanisms enable a more effective national response to incidents of cyber attack, it would be reasonable to expect that some of them might also enable a more effective international response, provided that the issues of sovereignty, control, and unified purpose could be adequately balanced.

Several promising examples of alternatives that might fit include: developing mechanisms to obtain strategic warnings, maintain situational awareness, and inform incident response capabilities; developing a set of threat scenarios and metrics; developing mechanisms for cybersecurity-related information sharing; and expanding sharing of information about network incidents and vulnerabilities with key allies.

Recommendation 2. The U.S. and Russia should search for domestic cyber and information security initiatives currently underway that are potentially suitable for extension to bilateral participation. Any collaboration on such substantive matters—even if narrowed in scope, or spun off from a domestic initiative—would require a great deal of trust, but could also be tremendously important. It could be critically important, for example, to create a common vocabulary and efficient mechanisms that enable the U.S. and Russia to exchange incident-related information in circumstances where both states wish to do so, and to clear (or at least identify) any bureaucratic hurdles that might exist in times of crisis that might hinder the use of such mechanisms. Existing channels of communication for such communication may not be sufficient to mitigate the risks associated with crises that occur at Internet speed.

Recommendation 3. We recommend a shared warning system stemming from a domestic initiative turned bilateral. The U.S. has already promoted the idea of shared warning in Australia and the U.K.³⁴ However, it is critical that this shared warning system be extended to Russia, if not started bilaterally between Russia and the U.S. A shared warning system would consist of an agreement that if either side experienced a cyber attack or discovered information about an upcoming attack on itself or the other nation it would warn the other nation so that they may learn and adapt. It

³⁴ Transcript of speech by U.S. Deputy Secretary of Defense William Lynn, III, "Defense Department Outlines New Infosec Approach," *Gov Info Security* (26 May 2010); available at http://www.govinfosecurity.com/articles.php?art_id=2580&opg=1.

would require direct communication between the organizations in the U.S. and Russia responsible for cybersecurity, such as the U.S. Cyber Command, and the relevant stakeholders in Russia. As Lynn stated, “Collective cyber defenses are similar to air and missile defense in that the more attack signatures that you see, the better your defenses will be.”³⁵ The warning system would not only serve to warn the other nation about possible attacks from nation-states, but also attacks from non-state actors, which represent one of the biggest cyber threats today. It is crucial that Russia and the U.S. work together to warn one another of upcoming threats and current attacks in order to build better defense systems and a more secure world, both in cyberspace and on the ground.

Creating a Path for Increased Cooperation

Returning to the core problem of the United States’ orientation towards a law enforcement approach, as opposed to the arms control approach advocated by Russia, it has been noted that these goals are by no means mutually exclusive. Therefore, despite any current differences in opinion, the two approaches could in theory coexist to the benefit of all parties. Nevertheless, the road between where we are today and this ideal outcome still seems quite long.

Several incremental steps on this path could go a long way towards creating an environment where both parties could work together towards addressing each other’s concerns and building a sufficient level of trust to proceed further. One such step would be to evaluate all the ideas put forward unilaterally by each side as actions for international cooperation, and from these actions to identify and advance actions that would be most attractive to the other party.

Recommendation 4. In order to go forward with bilateral negotiations, both sides need to come together to define what cybersecurity and information security are. We recommend establishing a collaborative definition database. One of the primary issues with cybersecurity today, as discussed above, is the lack of agreement about definitions, which inhibits both law makers and military actors. In order to overcome the divide on definitions, we recommend that a research center be established where academics and policy makers from both the United States and Russia would collaborate and define the critical issues of cybersecurity. The definitions will cover a wide range of issues, but will focus on what is cybersecurity or information security, what is cyber warfare, what is a cyber weapon, and what constitutes a cyber attack. Once the center establishes what it believes is a set of definitions that both countries could accept, it would submit these definitions to the respective nations’ executive bodies.

³⁵ Ibid.

If the presidents approve of the negotiated definitions, the definitions would then be submitted to the United Nations General Assembly for global approval because—although we believe bilateral negotiation is a strong starting point—cybersecurity must be tackled at the international level. It is essential to define what cybersecurity and other related issues mean and what constitutes an attack so that law makers and policy makers can work more effectively in the complex realm of cyberspace. Since cyberspace is constantly changing, we imagine that this definition process will be ongoing, with a new set of definitions submitted to the UN once every year. In the long term, this process of defining the world of information technology and security would be a springboard to eventually defining the rules of engagement, so that militaries can know how to strategize and act.

Recommendation 5. The United States should find a way to engage Russia in as many of the law enforcement mechanisms from the CoE Convention on Cybercrime as Russia is willing to try without requiring formal ratification of the Convention. Similarly, Russia should find a way to engage the U.S. in as many of the activities of the Shanghai Cooperation Organization on information security without requiring any formal participation. These arrangements, if found, might be optimal places to explore the other party's reactions to any unilateral suggestions for international cooperation. Though these arrangements will face many challenges—such as Iran being an observer of the SCO, and Russia already being a member of the CoE—similarly challenging situations have been successfully circumvented in other arenas with some degree of success. The NATO-Russia council, for example, has kept valuable lines of communication open to the benefit of both parties, and has allowed for progress that otherwise might not have been possible. The chances for the successful resolution of the stalemate over cyber and information security will be greatly increased if the parties are given substantive opportunities to work through their issues together in the most meaningful forums.

Conclusion

As progress within the cybersphere increases in speed, more and more issues are being drawn into this new realm. The information technology revolution represents one of the greatest technological advances in human history, with the dual power to push humanity forward, but also with a grave power to harm essential components of life. Both Russia and the United States are recognized world leaders within the cyber sphere, and both countries are using this technology in its dual purposes as an innovator and a weapon. As cyberspace becomes a declared domain of warfare, comparable to land, sea, air, and space, the U.S. and Russia face a crucial test of their ability to work together on important issues of international security. The two nations' diffe-

rent approaches to cyber are information security are not incompatible. Arms control and law enforcement are both critical components of international security in the era of the information revolution. Taking action on the recommendations presented here will help to create an environment where both countries can find an appropriate balance, and set an example for the international community. Though we understand that the sphere of cyber and information security is predominantly the sphere of international collaboration, it is also true that the variety of views and positions on this issue are so varied from country to country that the states are not likely to be able to come to any agreement. Cooperation between the United States and Russia is a good start, and the implementation of these recommendations could be ultimately extended to other nations that express their willingness to participate.

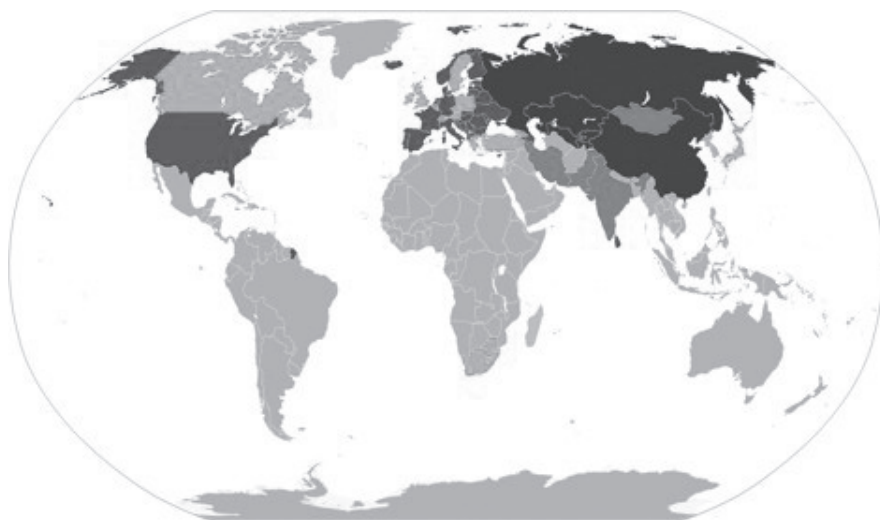







Figure 1: Arms Control and Law Enforcement in the Information Revolution

	Shanghai Cooperation Organization Member States
	Shanghai Cooperation Organization Dialogue Partners
	Shanghai Cooperation Organization Observer States
	States that have ratified the Council of Europe Convention on Cybercrime
	States that have signed but not ratified the Council of Europe Convention on Cybercrime

Distance Learning in the Bundeswehr: Skills Are More Than Knowledge

By Dr. Manuel Schulz¹ and Andrea Neusius²

As it is a military force that often conducts operations, the German Bundeswehr must always be prepared to cope with new tasks and challenges. This holds true not only for the organization as a whole, but also for each soldier and civilian employee. The diverse nature of these challenges imposes new and complex requirements on the Bundeswehr, requirements that must be met primarily through the competent action of Bundeswehr soldiers and staff. Therefore, the field of training holds a central position in the organization's diverse processes. The success of the overall organization in all fields depends heavily on the competence of its staff. As a result, it becomes clear that training that is appropriate in terms of tasks and their complexity has a considerable influence on the force's success at all levels and across the entire spectrum of tasks.

The Bundeswehr has long recognized the overriding importance of training, advanced training, and continuing education. Among other things, this is represented by the fact that the field of joint military training alone—that is, all training fields which are not specifically designed for the air force, navy, land forces, or the medical service—has been given the third-highest budget allocation in the field of education in Germany. Only the budgets of the Federal States of Bavaria and Baden-Württemberg (the two largest federal states in terms of area and population) are higher.

However, it is not only the financial aspect that displays the great importance placed on training, advanced training, and continuing education in the German military. Training and education also play a major role with regard to the attractiveness of the Bundeswehr as an employer. Particularly with their manifold possibilities of training and continuing education, which cover a great bandwidth from vocational training to fully recognized academic studies, the German Armed Forces, in the competition with other employers and in the view of an aging society, make a strong bid to win the “smart brains and skilled hands” of tomorrow for a career in their own ranks.

¹ Dr. Manuel Schulz, Colonel (GS) and Private Lecturer, is Senior Academic Director and Head of the Center for Technology based Training and Education (CTTE) – a central scientific institute of the Helmut-Schmidt-University / University of the Bundeswehr Hamburg.

² Andrea Neusius has a Graduate Degree in Education and is Chief Executive Officer of CTTE.

Why There Is No E-learning in the Bundeswehr

The Bundeswehr has only recently begun incorporating new media in its training and education efforts. This is an advantage rather than a hindrance, given that the great hopes that were placed on the new possibilities of e-learning in many fields in the 1990s have largely been dashed, leading to disappointment and frustration. For instance, many companies and organizations realized that the provision of new technologies did not automatically result in better-trained workers who were more qualified for their tasks. Quite the contrary, the level of frustration and demotivation has often clearly increased in response to education programs that allow for hardly any real interaction among real-life people.

The primary aim of introducing e-learning was often to save money in training and education efforts, by centralizing curriculum development and instruction. Hopes that the reduction of training personnel would lead to a clear reduction of costs without incurring any losses in the quality of the training were not fulfilled. What is the reason for this?

From an educational point of view, direct contact with other people in the learning process plays a central role. Communication between people helps to motivate and inspire them in their search for solutions to technical problems. Given that teamwork is an essential prerequisite for successfully accomplishing one's tasks in nearly all work environments, it also becomes clear that within the framework of training, advanced training, and continuing education, cooperation is of crucial importance in the process of acquiring new knowledge and skills.

This is where the educational concept of distance training has its roots. Distance training in practice is the Bundeswehr's further development of an alternative to the traditional forms of e-learning, in which the interaction between people and computers takes a central role, and where students are left alone with the technology (a PC, a learning software package, and possibly an anonymous network) and have to get along by themselves.

Instead, distance training adheres to the principle of *active learning* during phases of physical presence, and to the principle of *collective learning* during phases of remote cooperation. This means that the process of learning is primarily based on the active involvement of the students. This is done through so-called action simulations, during which tasks from real-life situations are simulated. In a given situation, the students then have to work out the solution to a problem themselves, not only by means of theoretical discussions, but also in practice. In this context, realistic action situations are generally characterized by the fact that the solution to a problem can only be found by cooperating with others. At that point it becomes clear that any preparation for a task that requires teamwork can only be done adequately if the learning process is based on teamwork as well.

It is equally important to appoint an instructor as a contact person in order to have him or her set the framework for the training so that it does not lead to a state of chaotic arbitrariness. On the other hand, active learning always requires intensive follow-up study and reflection when students return to their positions. This is always a part of distance training. The results of an action simulation are subsequently discussed and analyzed together with the other students and with the instructor. In this context, the students become aware of both the positive and negative aspects of their solution to the problem presented. In this way, all the students can understand the reasons for the success or failure of the approach to the problem, so that they can consider these aspects in future tasks.

The Teletutor: Presenting and Accompanying the Learning Process

Unlike many e-learning concepts, the instructor plays a central role in the field of distance training as practiced in the Bundeswehr. However, the instructor's function actually is not to have comprehensive knowledge and competence of everything in related to the subject area of the course, and there is no need to be able to "explain the world" to the students. Rather, the instructor's primary function is to ensure that the activities in the distance training program are actually a realistic representation of applications in the real world, that the framework of the distance training program is being adhered to, and that the students can always contact him or her in case of questions and problems.

In distance training, the instructor is the "teletutor." The teletutor provides live support to the students, either personally during the phases of training when the students are physically present, or virtually when they have returned home. His/her task is to ensure that, particularly during the virtual training phases, the students do not "get lost." Thus, the teletutor actively attends to the students by having fixed appointments with them either as a group or individually in a virtual environment, and also by working with them via network-supported communication means on an individual basis.

Therefore, the role of the instructor as a teletutor has been changing from the omniscient teacher towards a facilitator of the learning process who accompanies the students, is partially responsible for their learning success, and ensures that the framework conditions for a successful distance training program are in place.

During a three-month distance training program, instructors in the Bundeswehr undergo further training to become teletutors. In this teletutor training, the instructor learns to plan a course that he/she has previously taught as an attendance-based course as a future distance training program. In this context, the relation of the virtual elements of the program to the real tasks becomes visible. The results and findings gained during distance training represent direct additional benefits for the actual occupational field of application.

Skills Are More Than Knowledge: The Realization of Action Orientation

Distance training always connects virtual training periods with training phases of physical presence. Maintaining regular meetings when students are physically present helps to enable direct interaction and communication. It is much easier for a student to contact the teletutor or another student via chat or by means of a virtual video conference if one has met them in person before. Moreover, in many training fields, certain practice-oriented exercises that are important for the action simulation in distance training can only be realized in in-person meetings because they require special equipment and sometimes even higher security standards.

In this context, actions by the students themselves and, as a result, the acquisition of skills and knowledge always take center stage in distance training. We act on the assumption that competent action (= skills) requires more than having as much theoretical knowledge as possible about a topic. Finally, there is a great difference between having done something oneself already or having personal experience and simply knowing how something works.

Each distance training program begins with a kick-off meeting. During this meeting, the students and the teletutor get to know each other and the students are briefed on how to use the technical equipment available for the course. By doing so, the students overcome their reluctance to use the technology and do not feel inhibited in using the network for communication. Moreover, the students are given information about the sequence of events during the course, as well as what expectations the instructor has of them. The main focal points of the program are discussed, and the students are informed that they have to deal with the first action simulation right at the beginning of the first physical presence phase.

The following phase is the tutor-guided self-learning phase, in which the students prepare for their first action simulation while being supported by the teletutor. For this purpose, they are provided learning materials and tasks regarding the action simulation, which they can access via the network. Based on the work the students do on the learning tasks during the self-study phase, the teletutor obtains information regarding the students' initial baseline level of knowledge and possible areas of expertise, which enables him/her to tailor individual responses to each student's learning needs.

However, particularly during the action simulation, which marks the beginning of the first physical presence phase, the students' different states of knowledge will become readily apparent. Thus, active commitment is required right at the beginning. Subsequently, the results are discussed. For many students, this part of the training measure is an eye-opening experience, since they see a clear picture of their strengths and weaknesses in their approach to the given issue. Based on this experience, wor-

king groups are formed for the continuation of the distance training program. In this context, the heterogeneous composition of the group of students, which is often said to be a problematic phenomenon, turns into an advantage. If successful action can be better realized in a team (because it is impossible for one single person to know everything necessary to solve a complex problem), then it is even more probable that a comprehensive and successful solution to a problem can be found if there is a great variety of expertise available in a team when compared with a team made up of members with similar backgrounds and areas of knowledge. In the area of distance training, we call this “expert mix.” The fact that everyone is responsible for the group’s learning success by contributing his/her expertise is a motivation for all students. At the same time, the students can support each other, which lightens the teletutor’s workload and gives him/her the ability to individually deal with the students’ specific learning needs instead of applying the “sprinkler” method, and explaining the same content to all students in the same way.

The working groups then work jointly on the solution to more complex tasks in order to prepare the second action simulation. This is done in the tele-cooperation phase. For this phase, materials and information are provided online, and the teletutor supports and accompanies the students in their joint efforts to develop strategies for a solution. The main focus is on the joint acquisition of knowledge in the working groups. In the tele-cooperation phase, the teletutor’s main task is to ensure that teamwork also works via networked cooperation and communication, because the students are usually at their actual workplaces during the day and cannot meet in person to coordinate their efforts. As a side effect, the students also improve their media literacy, which should be considered an additional benefit of distance training.

In the second physical presence phase, the students assemble again in order to start with the second action simulation. At this point, the students can directly experience their increased competence when comparing it to the first action simulation. This contributes considerably to another boost of motivation, and at the same time it demonstrates that learning and working together in a team holds clear advantages over the traditional, solitary model of study. The evaluation of the results of the second action simulation is also done on a common basis. This marks the end of the “official” part of the distance training measure.

Facilitated Knowledge Management, or the Abolition of Course Completion

However, the networks—personal as well as technological—will remain active after the end of the individual distance training program, so that they can also be used afterwards. This marks the beginning of the application phase. The participants return

to their workplaces and must apply their newly acquired or deepened knowledge and skills in their daily work. At some point, almost everyone encounters the problem of not being able to solve a task or problem all by himself and with the means available on site. In this context, the network established with the teletutor and the other participants—the experts from different fields—during the distance training measure can be helpful. Thus, distance training does not only imply the end of the idea of ever completing a specific course of learning, but also marks the beginning of facilitated knowledge management. We call it “facilitated” because the teletutor helps enable the continued functioning of the network, providing access to relevant information and making connections to experts who may help to solve a given problem.

Thus, in distance training, technological networks, network-based tools for cooperation and communication, learning programs, and databanks can only be a means to an end. Training relies and will always rely on human beings as actors, which concerns the instructor as well as the participants. Therefore, human beings with all their needs and capabilities—not the latest computer interface or software package—take center stage in training.

Perspectives on the Further Development of Training in the Bundeswehr

The innovative didactic concept in the field of distance training has made clear the degree to which modern education work in the armed forces can contribute to increased mission orientation. In this context, the Bundeswehr will pursue consistent further developments in order to accompany and actively shape the upcoming reorientation of the German armed forces. In order to do so, it is imperative to consider current developments such as the focus on competence orientation, which is already being discussed quite intensively in the field of science and vocational training, for educational work in the Bundeswehr.

By making offers for advanced training and continued education that may be continued by occupational training in the civilian sector, and that offer better opportunities for advancement, education has the potential to considerably contribute to the Bundeswehr’s attractiveness as an employer. The basis for such a permeability of education between the Bundeswehr and other fields of occupational training and continuing education is a common understanding of concepts. This is the only way to consistently represent and evaluate comparable performances at the individual level (i.e., the soldiers) as well as at the organizational level of personnel development. Not least, this is the prerequisite for improving the attractiveness of military service and, consequently, for creating an increasingly flexible personnel management system, as is being requested by the Structural Commission of the Bundeswehr. One example for the current discussion is the debate about the terms *Meister* and *Bachelor*, which is closely related to the “Bachelor Professional.” The core question is whether

a *Meister* degree acquired in the German system of vocational training is equivalent to a bachelor degree from a university, and consequently whether it can be accepted as a prerequisite for follow-on studies to obtain an academic master's degree³.

Related to this is the requirement to survey the training opportunities in the German armed forces to determine whether they offer certifiable content within the framework of the ECTS (European Transfer Credit System), which could result in the recognition of credit points. By doing so, soldiers and civilian employees could pave the way during overall course of education and training for subsequent or simultaneous follow-on training at a university. Particularly in view of the demographic developments in German society, which is seeing its population get older, this could be another important contribution to the attractiveness of the Bundeswehr as an employer.

If we expand on this idea, an extension of this point system to a level below university education (e.g., vocational training or master craftsman training) should be developed. This would clearly increase the permeability of the educational system as a whole. In cooperation with the respective authorities in the fields of science, economy, and politics, the Bundeswehr, too, could participate in the development of sustainable and innovative concepts in education.

Particularly in the emerging "battle for the talents of tomorrow," the phase of occupational orientation and transition management gains central importance. In this context, the Bundeswehr has great potential to present itself as an attractive employer to the specialists of tomorrow.

The value of qualified labor will increase in the years to come. Therefore, the cost of longer phases of absence from the workplace for individuals to participate in intensive attendance courses will increase. This implies advantages for education scenarios that flexibly and (partially) virtually reduce phases of absence of personnel while not affecting the success of the educational enterprise. In this context, the Bundeswehr's concept of distance training is absolutely up to date, as it offers adequate solution strategies and manifold potential for the further development of training, advanced training, and continued education.

³ cf. W. Müller, „Vier Thesen für Durchlässigkeit der Bildungssysteme und Anrechnung von Kompetenzen," in *Durchlässigkeit gestalten! Wege zwischen beruflicher und hochschulischer Bildung*, eds. R. Buhr, W. Freitag, E. A. Hartmann, C. Loroff, K.-H. Minks, K. Mucke, & I. Stamm-Riemer (Münster: Waxmann Verlag GmbH, 2008), p. 57.

Experts with Diverse Skills and Backgrounds: The Bundeswehr Distance Training Convention

Only jointly it is possible to meet the challenges of the future. Exchange and cooperation with others must play a central role in distance training. This applies also to the further development of our concept and to exchanges with other experts in the field of technology-based education. The Centre for Technology-based Training and Education (CTTE) has been working to develop expertise in distance training since its founding in 2002. Today a central scientific institute of the Helmut-Schmidt-University/University of the Bundeswehr in Hamburg, the CTTE was begun as a project group for distance training on the initiative of the Bundeswehr Armed Forces Office and with the approval of the competent branch of the Ministry of Defense. Within the tripartite distance training working group—the Modern Training Technologies Section of the Bundeswehr Armed Forces Office; the training branch of the Ministry of Defense (Armed Forces Staff Branch I 5); and the Centre for Technology-based Training and Education—the CTTE acts as the scientific “think tank” for developing new concepts in distance training. It cooperates with numerous scientific institutions, such as the *Bundesinstitut für Berufsbildung* (Federal Institute for Vocational Education and Training) and with the *Deutsche Gesellschaft für Evaluation* (German Evaluation Society).

In pursuit of its goals of developing future best practices in distance training, the Centre for Technology-based Training and Education (CTTE) has been holding an annual Bundeswehr Distance Training Convention at the Helmut-Schmidt-University / University of the Bundeswehr since 2004. The Distance Training Convention brings together theory and practice with a scientific conference program, an integrated trade fair, and a variety of special panels. This year, the Ninth Bundeswehr Distance Training Convention will take place from 4 – 6 September 2012.

The Arab Spring: Challenges, Obstacles and Dilemmas

By Graeme P. Herd*

Introduction

On the twentieth anniversary of the fall of the Soviet Union, long-standing authoritarian regimes in Tunisia, Egypt, and Yemen have fallen, Libya is in the final stages of a civil war that toppled the forty-year rule of Muammar Gaddafi, and the regime of Bashar al-Assad in Syria may be tottering on the brink of implosion. Through 2011, demonstrations in Bahrain and Iran have been met with force, while Morocco, Jordan, Djibouti, Iraq, Oman, and Algeria have all reported protests. The Arab Spring has not been confined to the Middle East and North Africa; rather, its effects have gone global, with analysts drawing attention to its ripples, ramifications, and the potential of “revolutionary contagion” through the greater Middle East, sub-Saharan Africa, Russia and Eurasia, as well as China and East and South East Asia. Although there is broad agreement among experts and commentators who have studied the Arab Spring itself as to the scale and importance of revolutionary change in the Middle East and North Africa (MENA) region, its causes are contested, and there is little consensus as to its likely consequences and strategic effects. As Prince Hassan of Jordan noted, “The outcome of this tectonic realignment is not just unpredictable, but unknowable.”¹

Nevertheless, we can contend that the Arab Spring is in the process of challenging many of the attitudes, values, norms, and interests that have underpinned Russian, Eurasian, U.S. and European strategic approaches to the MENA region. These transformational events have forced fundamental questions concerning the basic tenets of international relations to the fore. How stable are authoritarian regimes, how brittle and fragile? What are the limits of humanitarian intervention? Is the set of assumptions that have governed Western strategy towards the MENA region—the balance between strategic interests, norms, and values—still relevant, or should some recalibration take place? This essay will attempt to answer some of these questions.

* Graeme P. Herd is the Head of the International Security Program at the Geneva Centre for Security Policy.

¹ Cited in Ian Black, “Where the outcome of the Arab Spring will end is anyone’s guess,” *The Guardian* (U.K.) (17 June 2011).

“Arab Spring”: False Assumptions and New Realities?²

Egypt’s stability under the government of Hosni Mubarak was guaranteed by two compacts. The first was agreed between the regime and the United States: Egypt would support the peace treaty with Israel and ensure access to cheap energy; the U.S. would stay out of Egyptian internal affairs. The second compact was between the Mubarak regime and the Egyptian people: the regime would hold a monopoly on political and economic power; in exchange, societal living conditions would gradually improve. The first pact was badly damaged by the terrorist attacks of 11 September 2001; the second was frayed, ready to break after a decade of economic stagnation, exacerbated by the socio-economic effects of the global financial crisis from 2008 onwards. Food and energy price hikes, high youth unemployment (35 percent illiteracy, two-thirds of the Egyptian population are under thirty years of age, and 25 percent are unemployed), corruption, nepotism, and dignity deficits (with 40 percent of the population living on less than USD 2 a day) all served to highlight the gaps and disparities between elite regime-performance-legitimacy rhetoric and the daily realities of life in Egyptian society.³

Egypt aside, more generally the MENA region is characterized by relative deprivation—the gap between high expectations and diminishing opportunities—and uneven resource distribution (when examined through religious, ethnic, gender, or tribal prisms). A succinct list of common factors is offered by the Russian Deputy Minister of Foreign Affairs, Mikhail Bogdanov:

The lack of change in the leadership and the political elite in general, a low level of political mobility, the belatedness or complete absence of reforms that have ripened, a high level of unemployment, corruption and other social diseases—all of these conflict-generating factors have been accumulating for many years and exploded at the beginning of this year. Moreover, one must not forget that young people prevail in the Arab countries. These are modern and educated people, who comfortably use the Internet, blogs and social networks and who saw no future for themselves in the existing framework.⁴

Authoritarian regimes in the region generated unaddressed political grievances that fed societal frustration and impotence, humiliation, and demoralization. Political systems that were long thought to be self-contained and that artificially suppressed volatility in the name of stability were capable of producing existential catalytic “black

² This section borrows heavily from Graeme P. Herd, “The Great Arab Revolution: Challenges, Dilemmas and Opportunities,” *GCSP Policy Paper* No. 11 (March 2011): 1–6.

³ Charles Kenny, “Why Recessions are Good for Freedom,” *Foreign Policy* 186 (May–June 2011): 31.

⁴ *Interfax* News Agency, Moscow (in Russian), 5 July 2011.

swan”-type events that elite-dominated regimes could not begin to recognize, let alone manage. As Nassim Taleb, the sage of the “black swan” theory, wrote, “The more constrained the volatility the bigger the jump will be.”⁵ The Arab Spring appears to demonstrate that dictatorial systems of power are inherently unstable and prone to collapse: it is not a question of *if* they will fall, but *when*.

Nonetheless, until 2011 the preexisting orthodox interpretations of stability in the MENA region argued that radical transformation was a mirage: the states were too powerful, buttressed as they were by a “deep state”—i.e., “the military-security complex and state control of the economy”⁶—and Western external support. Political opposition movements were considered too divided, and the media in authoritarian states were too easily muzzled. These national security nostrums have been turned on their head. Perceptions of the loyalty, cohesion, and resiliency of a pro-regime “securitocracy”—the security and intelligence services and the military and business elites closely connected to the ruling families—have shifted radically. The pyramid of Egyptian power, which projected a seemingly stable and enduring authoritarian equilibrium, has proved to be a brittle facade that in reality was built on shifting sand: the Pharaoh had no clothes. The deft positioning of the Egyptian military, the central pillar of the establishment, as a would-be honest broker between the Mubarak regime and Egyptian society underscores this reality. So too does the speed at which fair-weather Western friends—France in the case of Tunisia, the United States with regard to Egypt, the U.K. and Italy in the Libyan instance—have abandoned at least the titular heads of erstwhile long-standing strategic partners in the region.⁷

Egypt’s society, which contains 80 million people, may be fragmented between secular, nationalist, and Islamist factions, between the ideologically motivated forces of conservatism and modernity, between pragmatists and extremists and the apolitical or simply apathetic, but events indicate that a leaderless and disunited opposition deeply rooted in Egyptian society paradoxically rendered it a more powerful force. It promoted the emergence of a hard-to-challenge key societal message delivered in demotic terms: “Game Over!” and “Bread, freedom and human dignity!” The tired paternalistic mantras of deeply unpopular incumbents could not regain control of the narrative. More practically, with whom can the incumbent regimes negotiate, decapi-

⁵ Nassim Nicholas Taleb, “The Black Swan of Cairo,” *Foreign Affairs* 90:3 (May–June 2011): 6.

⁶ “Scholars posited that Arab States with oil reserves and revenues deployed this wealth to control the economy, building patronage networks, providing social services, and directing the development of dependent private sectors.” F. Gregory Gause III, “Why Middle East Studies Missed the Arab Spring,” *Foreign Affairs* 90:4 (July–August 2011): 3.

⁷ Libya was critical for Italy in energy security terms, supplying one-quarter of Italian oil imports, and 15 percent of its gas. Alberto Negri, “Recognition Is Blessing for Italian Gas and Oil,” *Il Sole-24 Ore* website (Milan, in Italian), 16 July 2011.

tate, or co-opt if the opposition movement remains resilient, stubborn, and united—and, most importantly, leaderless?

The role of instantaneous information communication technologies has been highlighted as catalytic in the events of the Arab Spring. Indeed, the crises in Tunisia and Egypt are characterized as the first Facebook, Twitter, and YouTube social media revolutionary movements (“Gandhi 2.0”). Such online, real-time technologies serve to heighten shared awareness and belonging and help build and shape political solidarity, identity, and cohesion around a message rather than a charismatic individual. They enable peer pressure and authority operating in virtual space to coordinate and organize mass protest on the streets and squares of the capital. The state can impede but not silence the new media and plugged-in opposition: sclerotic, linear state hierarchies and apparatus staffed by apparatchiks and led by tone-deaf elite elders were outmaneuvered by a networked, educated, urbanized, and globalized new generation, proud of their traditions and heritage and desperate for change. The role of the new social media was to create the dots—the daily episodes—which mainstream Arab media outlets, (e.g., *Al Arabiya*), particularly evening news and discussion programs, as well as satellite TV networks such as *Al Jazeera*—could weave into a narrative. Its role was to amplify and resonate an existing narrative, rather than determine the outcome.

Unlike the Rose Revolution in Georgia (2003) and the Orange Revolution in Ukraine (2004), allegations that Western non-governmental organizations (NGOs), embassies, and security services were fomenting postmodern *coups d'état* in the region have not been characteristic features of the coverage from within the region or by reflective analysts from outside the region.⁸ This reflects in part the reality that the toppling of regimes in Tunisia, Yemen, Egypt, and Libya are clearly societal-led internal revolutions: “of Arabs, by Arabs, for Arabs.”

MENA Reactions and Responses: Alternative Modernization Pathways?

It is still too early ascertain which states or actors have emerged as strategic winners and which can be considered on balance strategic losers. However, seven months after the start of the Arab Spring, some lessons are beginning to emerge. What is harder to ascertain is how these lessons will be “learned.” Indications might include the recalibration of strategies, adjustments in policies or policy priorities, cutting or increasing the volume and direction of resource and budgetary allocations, and the

⁸ Yevgeny Primakov, “Egyptian Explosion: What next? The Center of Gravity is Shifting from Al-Tahrir Square to the Political Field,” *Rossiyskaya Gazeta* website (Moscow; in Russian) (9 February 2011); Vladimir Mamontov, “Egypt will wait,” *Izvestia* website (Moscow; in Russian) (7 February 2011).

elaboration of new legitimating narratives. In the immediate term, three potential alternate strategic pathways appear as models and offer road maps to the future, if not necessarily viable and sustainable governance systems. As the Arab world's largest, oldest, and deepest culture and civilization, Egypt will likely be a benchmark for the region. It is in transition, but transition to what? Interestingly, it has the potential to exemplify any of the three alternative pathways.

Option One: The Orderly Transition

First, we can posit the theoretical option of a “soft landing”—a managed “orderly transition” towards a reinvented democracy and the emergence of a prosperous and pluralistic state-building project over the longer term. Here the understanding would be that the political system will be radically restructured through free and fair parliamentary elections, with the promise that the constitution will be rewritten to address dignity deficits. The internal debates will focus on how far and how fast the process of reform should unfold, rather than the general strategic orientation and ultimate goal. The demonstration effect of the revolutions proves a powerful driver, buttressed by media reportage and raised societal expectations. For energy-rich states, higher oil prices may provide a cushion to offset social, economic, and political disruptions that cause a dip in stability (the “J-curve”) as the political system shifts from one of closed authoritarianism to open democracy.⁹ The underlying rationale is not a Damascene-like conversion to democracy, but rather a basic survival instinct and political calculation that places self-preservation above all other considerations.

Over the longer term, *sustainable* political governance systems and regimes in the MENA region will *ipso facto* be heterogeneous: acceptable to elites and the broader society; appropriate to indigenous histories, socio-political cultures, traditions and narratives; and affordable—that is, aligned to the particular state's economic realities and circumstances. Interestingly, in the case of Jordan, Morocco, and Oman, rational and pragmatic monarchies have taken the lead in driving reform, and constitutional monarchies may well be the outcome. Ekmeleddin Ihsanoglu, the head of the Organization of Islamic Cooperation (OIC), argues that since the 1950s republican regimes in the MENA region have demonstrated “less respect for democracy and human rights” than monarchial regimes: “Republican regimes brought military dictatorships or the dictatorship of party ideology. The leaders are cult figures. In monarchies you have kings as well but there are traditions that are transferred from generation to generation. In monarchies you don't have a problem of succession, for instance. In republics the leader wants his son to succeed him. How can you call this

⁹ Ian Bremmer, “The J-curve hits the Middle East,” *Financial Times* (17 February 2011): 9.

a republic?"¹⁰ Turkey benefited from particular internal preconditions (Ataturk) and a Cold War strategic context and NATO membership to facilitate a stable and successful modernization project. Change took place incrementally over decades rather than by revolution. In the sense of process and outcome, rather than specifics (i.e., an Islamist party in power), Turkey is posited as a model for the region.¹¹ Some analysts have also highlighted the post-Suharto Indonesian experience of democratization as a relevant example for some MENA states: "Back in 1998, when widespread protests here forced Suharto to step down, ending his thirty-two-year military-backed rule—which had suppressed communists and Islamists—it left the path open for political reform and free and fair elections in the Muslim-majority nation. Egypt, a key Arab ally of the West and its cornerstone of security and stability in the Middle East, faces a similar challenge."¹²

Option Two: Bureaucratic Persistence

The second potential pathway lies in the apparatus and bureaucracy of the previous regime, its institutions and personal connections bound together by shared interests, surviving phoenix-like to dominate post-revolutionary power distribution and resource allocation. This pathway derives its power from past experience and the weight of political culture. Historically, the Egyptian military has conflated the national interest with the interests of the military defense-industrial complex. Why would the Supreme Military Council not do the same? The Egyptian military and security services control large national projects, industries, and defense contracts that account for a 15 percent share of Egypt's GDP.¹³ Safety valves that allow elites to channel public anger and frustration in exchange for maintaining and reinforcing the status quo could include greater ant-Israeli/U.S. rhetoric, ethno-tribal-nationalist mobilization, and increased militarism—all paid for courtesy of higher oil prices. Given the lukewarm support for the Mubarak regime in its hour of need from the U.S. and Europe, initiating a search among the "Authoritarian International" (particularly Russia and China) for more reliable strategic partners will become a priority for those states whose regimes feel embattled. Again, debates within incumbent regimes focus on

¹⁰ Barcin Yinanc, "Arab World Faces Long, Painful Road, Says Islamic Group Head," *Hurriyet* website (Istanbul) (16 July 2011).

¹¹ Andrey Lipskiy, "Arab Dominoes," *Novaya Gazeta* website (Moscow; in Russian) (25 February 2011); Sahin Alpay, "Why Turkey, Not Iran, Inspires," *Zaman* website (Istanbul) (21 February 2011); Asli Aydintasbas, "Is it Wrong to Say 'the First Republic Has Ended'?" *Milliyet* website (Istanbul; in Turkish) (1 August 2011).

¹² "Indonesia: A Model for Change," *The Straits Times* website (Singapore) (17 February 2011).

¹³ *Yusuf Ergen, "Milbus and Arabs," Today's Zaman (27 February 2011).*

means rather than ends: how much force, where and when to apply it, which alternative strategic partners? Here the calculation is that autocracies are indeed adaptable: they can become even more autocratic.

Option Three: State Chaos

The third potential pathway for states in the Middle East and North Africa in the wake of the upheavals of the Arab Spring is the ascendancy of Al Qaeda, chaos, anarchy and civil war, or a 1979 Iranian-style Islamist takeover (reinforcing the notion of “Arab exceptionalism” and Samuel Huntington’s ‘Clash of Civilizations’ thesis). These scenarios were widely understood to constitute the types of default options that would emerge if transition traps derailed democratization efforts.¹⁴ The specter of a descent into anarchy is currently evidenced most strongly by unfolding events in Libya (“We will fight until the last man, until the last woman, until the last bullet”¹⁵), Yemen, and Syria, with gloomy prognosis the order of the day: “I see a river of blood and a plunge towards the abyss.”¹⁶ In Tunisia and Egypt, incumbent official narratives were further delegitimized precisely because extremist religious ideologies have not (yet) proved to be the default alternative to the status quo.¹⁷

¹⁴ Ahmed Rashid, “Cairo Needs Help to Avoid al-Qaeda’s Grip,” *Financial Times* (16 February 2011): 9.

¹⁵ “Gaddafi’s Son Warns of “Rivers of Blood” in Libya,” *Al Arabiya News Channel* (21 February 2011); available at <http://www.alarabiya.net/articles/2011/02/21/138515.html>.

¹⁶ Ghassan Shabril, “On the Way to the Abyss,” *Al-Hayat* website (London, in Arabic) (1 August 2011).

¹⁷ Scott Shane, “Al-Qaeda Left out in an Arab Sea of Change,” *International Herald Tribune* (1 March 2011): 4; Omer Taspinar, “CChange in the Arab World: Why Now?” *Zaman* website (21 February 2011). Indeed, while many studies reject the correlation between political reform and the rise of Islamist militant groups, the connection between frustration and political violence has not been debunked, “thus making democracy the only guarantee against radicalization in the Arab world.” Murad Batal al-Shishani, “Special Commentary: Popular Movements in the Middle East and the Role of al-Qaeda,” *The Jamestown Foundation*, 3 March 2011.

Spillover Effects: Arab Spring—Eurasian Fall?

Throughout 2011, the media and analysts in the former Soviet Union and beyond have debated the causes, course, and possible consequences of the Arab Spring, including the potential of the spillover of “revolutionary contagion” into Eurasia.¹⁸ Arguments here have focused on structural and systemic causal factors common to the MENA region and Eurasia, authoritarian regime-types and the extent to which they prove to be resilient and adaptable or prone to instability and upheaval. The commonalities between the Arab Spring in the MENA region and conditions on the ground in Eurasia are apparent: enduring inequalities and dignity deficits continue; longstanding authoritarian republicanism is in place; intra-regional transnational societal spillover potential is ever-present; and resource distribution and allocation is explained by pre-existing family, clan, tribal, ethnic, religious, and gender allegiances and animosities. These commonalities have little resonance in Ukraine, Georgia and Moldova, but are more relevant in Russia, Armenia, and Azerbaijan and are most striking in Central Asia. In Central Asia, authoritarian incumbents in Kazakhstan and Uzbekistan have held power for over twenty years. Dignity deficits are well attested: food price hikes and electricity cuts in Kyrgyzstan and Tajikistan are ongoing, and border regimes are opaque. In its most recent “Corruption Perception Index,” Transparency International ranked Kyrgyzstan 164, Kazakhstan 105, and Tajikistan 154 out of 178 states surveyed (Turkmenistan and Uzbekistan tied for 172nd place, along with Sudan).

However, important differences between conditions in the Middle East/North Africa and Central Asia can also be identified. First, the post-Soviet authoritarian equilibrium differs from that in the Arab world. The ruling elites in Central Asia—the “selectocracies”—are centered on the presidential family, business elites, and cronies, but by contrast to the MENA region they have a much lighter investment in military and security services. The symbolic role that the army enjoys in Egypt, possessing status as the core institution of the modern state the primary guardian of the Egyptian people, being simultaneously above politics and the embodiment of the state itself (despite the fact that it supplies presidents), has no analog in Central Asia, or anywhere in the post-Soviet space. In Egypt, the military as a classical state structure and institution was able to stand above the fray, maintain its legitimacy, and then intervene for the good of society to “restore order.” The role and function of elite military units in state structures in Central Asia is regime defense, and militaries have traditionally been socialized to accept civilian (if not democratic) control.

¹⁸ Aleksandr Rybin, “Will Kazakhstan Become Another Egypt...” and Zafar Abdulloyev (director of the Kontent centre for political analysis), “Social inequality and the ‘Libyan question’,” in *Biznes i Politika*, (Dushanbe, in Russian) (17 March 2011); Mikhail Dvoryanchikov, “Yermukhamet Yertysbayev: 3 April Will be a Great Day,” *Ekspress-K* (Almaty, in Russian) (4 March 2011). Yertysbayev is a presidential advisor in Kazakhstan.

Second, the idea is prevalent that the prospect of the spread of revolutionary “contagion” is slight due to an inbuilt immunity in Central Asia. This rests on the claim that there is a predisposition toward and preference for gradualist reform in Central Asia rather than revolution. The burden of history has inoculated these states and societies from revolution: Tajikistan is still suffering the effects of a recent civil war (1992–97); Kyrgyzstan had its own revolution in 2010 (indeed, President Roza Otunbaeva argues that the Kyrgyz revolution provided the model for the Arab Spring); for Uzbekistan, the massacre in Andizhan in 2005 demonstrates that what little discontent exists is localized rather than widespread and can remain contained; regime leadership change occurred already in Turkmenistan in 2007, when President Gurbanguly Berdimuhamedow took power after the death of Turkmenbashi; and President Nazerbayev of Kazakhstan opted for regime renewal with “free and fair” elections in 2011.

Finally, in contrast to the strategic approach taken by the EU, NATO and the U.S. to the MENA region, the most powerful regional actors and institutions in Eurasia—the Russian Federation/CSTO and China/SCO—cast normative shadows that support and actively uphold the status quo. This solidarity is buttressed by both the post-9/11 war on terror and the legitimizing of preexisting anti-radical Islamist narratives, and by their unified understanding of the nature of the “Color Revolutions” in Serbia, Georgia, Ukraine and Kyrgyzstan and their commitment to oppose their “export.” China in particular has responded very forcefully to the prospect that the Arab Spring could become a Eurasian Summer, or a Chinese Winter. Throughout 2011, internal Chinese security services and state authorities have tightened their control over the media, including the systematic harassment of journalists and dissidents in a manner many long-standing China analysts characterize as massive, disproportionate, and the worst crackdown since the Tiananmen Square protests in 1989. Chinese official rhetoric also stresses the fact that the Chinese themselves, through the bitter experience of history, are predisposed to accept gradualist evolutionary progress. The Cultural Revolution in the 1960s, Tiananmen in the 1980s, and uprisings and riots in Tibet in March 2008 and Xinjiang in July 2009 all demonstrate that sudden change and discontinuities bring chaos and violence. In short, the regime argues that its model of “authoritarian developmentalism,” which incorporates regime-rejuvenating measures (such as a rotating participative leadership) has proved adaptive and thus durable.¹⁹

¹⁹ Titus C. Chen, “China’s Reaction to the Colour Revolutions: Adaptive Authoritarianism in Full Swing,” *Asian Perspectives* 34:2 (2010): 5–51; Abel Polese and Donnacha Ó Beacháin, “The Color Revolution Virus and Authoritarian Antidotes: Political Protest and Regime Counterattacks on Post-Communist Spaces,” *Demokratizatsiya: The Journal of Post-Soviet Democratization* (Spring 2011).

The fear of “contagion” has shaped the domestic public policy responses of incumbent regimes in Central Asia. These responses provide a window into elite perceptions and anxieties, as well as their ability to differentiate between symptoms and causes of upheaval. They can be characterized by what we might call a combination of “soft repression” and “symbolic reform”—a Central Asian version of sticks and carrots. An increased monitoring of Islamic religious institutions and funding from foreign religious foundations is apparent, along with more stringent filtering of new social media and the Internet. Central Asian authorities have focused on Internet access and social media subscription levels, which indicate the size and vibrancy of virtual civil societies throughout the region, and have sought to restrict flows of information in various ways. The capacity and will of these authoritarian regimes to “manage,” censor, monitor, and block new social media, the Internet, CDs, and religious literature are high, particularly in Kazakhstan, Uzbekistan, and Turkmenistan.²⁰ Kyrgyztelecom has reported that Kazakh Telekom filters and restricts some Google services, while Uzbek authorities are reportedly asking information providers to inform the government about mass mailings of text messages that are “sensitive and suspicious,” clearly concerned about an SMS-Revolution.²¹ In Turkmenistan, “Some, if not all, of Turkmenistan’s young people studying abroad may be prevented from ever leaving again if they return home. The reason probably has to do with the wave of revolution sweeping across the Middle East.”²²

Eurasian leaders (or their advisors, at any rate) appear to have read Alexis de Tocqueville: “the most dangerous moment for a bad government is when it begins to reform.”²³ Symbolic reform designed to preempt an Arab Spring comes in the shape of increased elite-initiated discussions and debates on the need for political reform and renewal, though with little practical outcome. In the spring of 2011, Uzbek president Islam Karimov and his Tajik counterpart Emmamali Rahmon led debates on political modernization and structural reforms, including the idea of increasing the authority of the government and parliament. The Kazakh President Nursultan Nazarbaev most notably organized a snap presidential election on 3 April 2011 and invited foreign observers to monitor the process, while also raising the issue of power redis-

²⁰ Farangis Najibullah, “Is Kazakhstan Under Threat of Radical Islamization?” *Radio Free Europe/Radio Liberty* (30 March 2011); available at http://www.rferl.org/content/chaikhana_kazakhstan_islamization_threat/3542185.html.

²¹ Anuradha Chenoy, “Can the Events in West Asia be replicated in Central Asia?,” NewsClick Production, 1 April 2011; available at <http://newslick.in/node/2102>.

²² Muhammad Tahir, “New Dilemma for Turkmen Students Abroad,” *Radio Free Europe/Radio Liberty* (7 April 2011); available at http://www.rferl.org/content/dilemma_turkmen_students_abroad/3550259.html.

²³ Graeme Robertson, “Arab Autocrats May be Tottering, but the World’s Tyrants Aren’t All Quaking in their Steel Toed Boots,” *Foreign Policy* 186 (May–June 2011): 36–39.

tribution, strengthening the judiciary's independence, and ensuring greater freedoms for civil society.

Recalibrating Russian and Euro-Atlantic Strategic Frameworks?

For Russia, the U.S., and Europe, the reality of armed humanitarian intervention in Libya and growing pressure for external intervention in Syria, as well as regime changes and revolt throughout the region, have focused thinking on crisis management and operational issues: the emergency evacuation of foreign nationals; disclosure/freezing of incumbent assets and sovereign wealth funds; elite travel bans; the recalling of ambassadors; the redrafting of bilateral military-aid conditionality clauses; the imposition of no-fly zones; and the threat and then deployment of armed humanitarian interventions in the name of the "responsibility to protect."²⁴ However, the Arab Spring has also implicitly questioned the viability of existing Russian and Euro-Atlantic strategic approaches to the MENA region, especially the assumptions upon which these approaches rested.

In January 2005, then-U.S. Secretary of State Condoleezza Rice characterized six decades of U.S. policy towards the Middle East as having sacrificed liberty on the altar of authoritarian stability but gained neither. On the one hand, Western strategic interests (regional stability, the continuity of the Egyptian-Israeli peace treaty, and access to the Suez Canal and Egyptian airspace) were secured through long-standing strategic partnerships with autocratic security-providers. On the other hand, Western market-democratic states promoted democratic principles and values of accountability and transparency. Six years later in 2011, the question was urgent: can there be a prudent blend of power and interests with principle and values, of *realpolitik* and idealism, or do blatant double standards and hypocrisy only serve to delegitimize both? Might a new political calculus be emerging, one that recognizes that this compact is bankrupt? At its core, it is a false dichotomy to posit interests and values in opposition to each other. Western self-interest and self-respect are aligned; interests and values are now the same.²⁵

This rebalancing has its critics, not least Portuguese Foreign Minister Luis Amado: "Foreign policy is not necessarily only based on principles but also on interests. And in that sense, our foreign policy is no different from that of all those European states that currently face the same type of foreign policy developments. It is absolutely ridiculous to wish to develop ties based on the democratic conditions of each

²⁴ Iftekhar Ahmed Chowdhury and Yang Razali Kassim, "Libya and the UN: Whose Responsibility to Protect?" *RSIS Commentaries* 34/2011 (4 March 2011); available at <http://www.rsis.edu.sg/publications/Perspective/RSIS0342011.pdf>.

²⁵ Charlemagne, "No Time for Doubters," *The Economist* (26 February 2011).

country. If that were the case, we would not have ties with many countries with whom we have had ties for decades.”²⁶ Fareed Zakaria has also noted,

There are vast differences between the circumstances in Tunisia, Egypt, Libya, Syria and Saudi Arabia; American interests in those countries; and our capacity to influence events there. ... Were the administration to start clamoring for regime change in Riyadh, and were that to encourage large-scale protests (and thus instability) in the kingdom, the price of oil would skyrocket. The United States and much of the developed world would almost certainly drop into a second recession. Meanwhile, the Saudi regime, which has legitimacy, power and lots of cash that it is spending, would likely endure—only now it would be enraged at Washington. What exactly would a more “consistent” Middle Eastern policy achieve?²⁷

The extent of strategic uncertainty is underscored by the following questions that remain unanswered seven months into the Arab Spring. Will Arab states undergoing democratization projects have the capacity to contain Iran, keep the peace with Israel, and enable uninterrupted energy flows from the Middle East? If Egypt, Iraq, Jordan, Morocco, Saudi Arabia, and Yemen do not fall primarily within the West’s security system, then who fills the vacuum? Will Turkey’s custodianship, guardianship, and stabilizing role in the Middle East increase?²⁸ Where does this leave Iran and Saudi Arabia?²⁹ Is then the real choice between having stable MENA states with independent foreign and security policies or weak, fragile authoritarian Western puppet regimes?

Strategic questions focus on long-term goals and visions for the region and its relationship with external actors, rather than processes—on ends, not means, though the two are clearly linked. At what point should erstwhile external strategic partners shift their support to counter-elites when longstanding incumbent allies become albatrosses, while still ensuring a dignified, orderly transition? How can grass-roots activists demanding regime change be supported in Egypt without extending such support to

²⁶ Luis Amado, *Diario de Noticias* website (Lisbon, in Portuguese) (27 February 2011); Fareed Zakaria, “A Doctrine We Don’t Need,” *The Washington Post* (7 July 2011): A13.

²⁷ Zakaria, “A Doctrine We Don’t Need.”

²⁸ For arguments on either side, see Soner Cagaptay, “Arab Revolt Makes Turkey a Regional Power,” *Hurriyet* website (17 February 2011); Sahin Alphay, “Does the Arab Spring Mean Turkish Fall?” *Zaman* website (16 May 2011).

²⁹ Rachel Bronson, “It Can’t Happen in Saudi Arabia. Right?” *The Washington Post* (27 February 2011): B01; Sergio Romano (former Italian Ambassador), “Winners and Losers in the North African Crises,” *Corriere della Sera* (Milan, in Italian) (2 March 2011); James Kitfield, “Saudi Arabia, Iran Reorient Foreign Policy Amid Middle East Unrest of Arab Spring,” *National Journal* (21 July 2011); Andrea Riccardi, “Europe’s Distraction,” *Corriere della Sera* website (2 August 2011); Dassa Kaye and Frederic Wehrey, “Arab Spring, Persian Winter,” *Foreign Affairs* 90:4 (July–August 2011): 183–86.

all mass protests in the region? How can we avoid the unintended consequences that such external support will be used by incumbent regimes, as was the case in Iran with the “Green Revolution,” to delegitimize the very protest it seeks to bolster? As one analyst has noted: “The Syrian psyche is shaped by memories of foreign interference, something that the Assad regime did not invent, but has exploited. In Syria, anyone who calls for outside intervention is likely to be branded a traitor; any Western threat of military action would therefore hurt the opposition more than the regime.”³⁰ How then can opposition groups in Syria be supported in their efforts to gain power while avoiding sectarian massacres or external military intervention?³¹

Does the Arab Spring signify an epitaph for an age of liberal interventionism, mirroring the U.S.’s global and regional decline? Jaswant Singh, a former Indian finance, foreign, and defense minister, has argued that “to ignore the bloodshed in Syria is to give tacit recognition to Iran’s regional influence. That lack of resolve invariably diminishes Saudi Arabia’s prestige and raises even more questions within the kingdom about the reliability of U.S. protection—hence further eroding America’s regional position. The emergence of a neo-Ottoman Turkey under Prime Minister Recep Tayyip Erdogan, asserting itself in the lands of the former Ottoman Empire, attests to America’s diminished regional prestige.”³² Certainly, analysts have noted that the U.S. is now determined to “lead from behind” through adopting a supportive role (mainly by providing strategic communications, munitions supplies, and intelligence). The Arab Spring demonstrates that “the U.S. will not hesitate to lead ‘wars of necessity’ in defense of European allies. But it will not take the lead in ‘wars of choice’ in or around Europe, such as Libya.”³³ In June 2011, on the eve of his retirement, U.S. Defense Secretary Robert Gates warned that NATO could face “a dim if not dismal” future if military spending shortages and national caveats were not addressed, given that his generation’s “emotional and historical attachment to NATO” is “aging out.”³⁴

³⁰ Bassma Kodmani, “To Topple Assad, It Takes a Minority,” *The New York Times* (31 July 2011).

³¹ “Can the West, after intervening to prevent a bloodbath in Benghazi, continue to do nothing as massacres take place throughout the country? To let the Syrian cauldron boil is wrenching, but to intervene appears utterly impractical. Liberal interventionism, once again, seems undermined by its (perhaps inevitably) uneven application.” Jaswant Singh, “The End of Liberal Interventionism,” *The Toronto Star* (3 July 2011): A15.

³² Singh, “The End of Liberal Interventionism.”

³³ Tomas Valasek, “What Libya Says about the Future of the Transatlantic Alliance,” Centre for European Reform, July 2011, 2; available at http://www.cer.org.uk/pdf/essay_libya_july11.pdf. See also Ryan Lizza, “The Consequentialist: How the Arab Spring Remade Obama’s Foreign Policy,” *New Yorker* (2 May 2011); available at http://www.newyorker.com/reporting/2011/05/02/110502fa_fact_lizza.

³⁴ Robert Burns and Desmond Butler, “Gates: NATO Alliance Future could be ‘Dim, Dismal,’” *Associated Press* (10 June 2011); available at http://news.yahoo.com/s/ap/20110610/ap_on_re_eu/eu_gates_nato_doomed.

Some were quick to argue that NATO members were no longer much interested in NATO's future. NATO was brain-dead; all that remained was to switch off the life support machine and, after a respectful silence, pronounce the eulogy: "Just look at the NATO-led war in Libya in which only six out of the twenty-eight NATO countries are participating, and only three of those actually attack Libyan targets to enforce the United Nations' mandate ... after a mere eleven weeks of conflict against Libya, the 'mightiest alliance in the world' has run out of munitions, does not have enough aircraft to conduct its missions, and seems unable to prevail against a minor military power."³⁵

The Arab Spring has highlighted a collective action problem, with splits within and between the Non-Aligned Movement, Arab League, UNSC, and EU. The EU, with its twenty-seven member national governments, is in disarray over Libya, demonstrating that a preemptive humanitarian operation is much harder to legitimize than one after the fact. The EU's Big Three—France, Germany, and the U.K.—are unable to find common cause in a high-profile foreign policy challenge. Eighteen months since the Lisbon Treaty, which led to the creation of the European External Action Agency (EEAS), it is clear that "a foreign ministry' is not a foreign policy, and there is little sign that the EU will devise one anytime soon."³⁶ It is also clear that existing EU and NATO tools and policy instruments designed as alternatives to membership have failed to bring stability and development to its southern neighborhood.

Russia, along with other conservative status quo regimes in Eurasia, consistently emphasizes stability and order at home, and criticizes "humanitarian interventions" abroad. The Arab Spring indirectly questions the viability of Russia's domestic authoritarian governance model and directly highlights strategic dilemmas for its foreign policy. Political transformation and adaptation in the MENA region raises questions about political transition and power distribution in Russia. How resilient is Russia's system of authoritarian power, and how sustainable are its current legitimacy narratives? The 1990s represented a lost decade for Russia, in which the decentralization of power and authority resulted in chaos and anarchy. Putin's social contract provided stability and prosperity (guaranteed by the managerial competence and patriotism of incumbents) within a "sovereign democracy" in exchange for a continuity of power in Russia.³⁷ Variants of this narrative sustained authoritarian regimes in the MENA

³⁵ Sawar Kashmeri, "NATO's Surreal World," *New Atlanticist* blog (22 June 2011); available at http://www.acus.org/new_atlanticist/natos-surreal-world; Geoffrey Wheatcroft, "Who Needs NATO?" *New York Times* (16 June 2011); available at <http://www.nytimes.com/2011/06/16/opinion/16iht-edwheatcroft16.html>.

³⁶ Giles Merritt, "Where is Europe's Foreign Policy?" *Korea Times* (31 July 2011).

³⁷ Graeme P. Herd, "Russia's Sovereign Democracy: Interests, Identity and Instrumentalisation?" in *A Resurgent Russia and the West: The European Union, NATO and Beyond*, ed. Roger E. Kanet (Dordrecht, The Netherlands: Republic of Letters Press, 2009), 3–28.

region, just as is the case in Russia's partners in Eurasia today. However, just as with the MENA region, by 2011 this legitimacy narrative was under serious stress.

Procedural legitimacy deficits (no free and fair elections) are justified by performance outcomes, but a series of recent episodes have demonstrated that procedural legitimacy deficits are in and of themselves a cause of concern. The Russian lawyer Alex Navalny's campaign against corruption, the trial of Mikhail Khordokovsky, the revolt of the intellectuals, the arrest of opposition leader Boris Nemtsov are only the most obvious examples. The aftershocks of the 2008–09 global financial crisis have seriously undermined the Putin/Medvedev regime's performance, its bedrock source of legitimacy, although Russia has recovered with 4 percent GDP growth (relative to other BRICS, this is low; relative to Europe and the U.S. it is high). More importantly, the Russian economy's structural dependence on hydrocarbons was reinforced, as the crisis did not bite down deep or hard or long enough to cause major economic reform. The reality of political, economic, and military stagnation is hard to ignore, but so too is a military reform process that appears dead in its tracks. Of greater concern is the fact that the state's ability to maintain control over coercive force is questionable, which is a serious deficit for a *siloviki*-led law-and-order-based regime—the role of OMON (special police forces) in suppressing riots in Moscow in December 2010 is a leading indicator. Russia's third post-Soviet power transition will be marked with presidential elections in 2012. This election brings all sources of legitimacy and existing narratives into question. Indeed, it represents a potential “black swan” event for Russia.³⁸

The Arab Spring does not just raise questions relating to the sustainability of Russia's internal governance system and structures, but also about its role as an international actor, presenting a series of serious challenges to Russian foreign policy interests. NATO's humanitarian intervention in Libya raised a set of strategic dilemmas for Russia. Russia did not want to support and thus justify a humanitarian intervention in Libya, as this would only serve to advance U.S. and European interests, as well as reinforce dangerous precedents set in Kosovo and Iraq.³⁹ However, there was significant regional support for the resolution. In addition, the Obama Administration was willing to decide the issue of military intervention within the UNSC. This was a demonstration of multilateralism, and therefore a repudiation of Bush-era

³⁸ Pavel Baev, “The Prospect of Putin's Return Comes into Focus,” *Jamestown Foundation Eurasia Daily Monitor* 8:147 (1 August 2011): “The distance between this passive discontent and angry protest may turn out to be far shorter than the ruling kleptocracy assume. . . .” See also Fred Weir, “Medvedev rebuffs Gorbachev's Warning of ‘Egyptian Scenario’ in Russia. Who's Right?” *Christian Science Monitor* (22 February 2011).

³⁹ David Miliband (former U.K. foreign secretary), “Whatever you do, Mr. Obama, Don't Play Safe,” *The Times* (London) (23 May 2011): 20: the Arab Spring “sets a new legitimacy bar for the exercise of power.”

unilateralism and implicit support for the “reset” agenda in Moscow–Washington relations. For all these reasons, a veto from Russia would have sent the wrong strategic signal. Abstention from UNSCR 1973 (to create a no-fly zone over Libya) had the strategic advantage of “placing Russia in a position to benefit from whatever political outcome.”⁴⁰ By contrast, with regard to Syria, since March Russia (alongside China and other BRICS) has strongly opposed UNSC resolutions condemning violence and proposing sanctions and foreign intervention against Syria, and has threatened to veto any such UNSC resolution.⁴¹ Unrest here is considered a purely internal affair. Syria, as Russia’s one remaining strategic partner in the region, buys virtually all its weaponry from Russia, and provides Moscow with naval bases in warm waters.⁴² However, Russia has begun to soften its stance and hedge, as the Assad regime’s crackdown on dissent has become increasingly brutal. In early August, President Medvedev warned Bashar al-Assad to open dialogue with the opposition: “If he cannot do this, he will face a sad fate and at the end of the day we will also have to take some kind of decision.”⁴³ The EU presses for sanctions targeting oil exports, which constitute one-third of all of Syria’s state revenues.⁴⁴

One other set of dilemmas centers on the notion of a dichotomy between “Southern Engagement” and “Eastern Enlargement.” It is not in Russia’s interests to see the MENA region rise in strategic importance for Europe, as this will increase Eu-

⁴⁰ Roland Dannreuther, “Russia and the Arab Revolutions,” *Russian Analytical Digest* 98 (6 July 2011): 2. See also Mark Katz, “Russia and the Arab Spring,” *Russian Analytical Digest* 98 (6 July 2011): 4–6.

⁴¹ “Russia Reiterates Rejection of Foreign Interference on Syrian Affairs,” *SANA News Agency* website (Damascus, in English) (2 August 2011).

⁴² Philippe Conde, “EU-Russia: Much Ado About Nothing?” *IPRIS Viewpoints* (July 2011): 1–3. The Syrian port of Tartus, a Soviet-era naval supply and maintenance base, is being refurbished with the aim of accommodating twelve Russian warships after 2012, giving Russia an increased strategic presence in the Mediterranean Sea, and also Red Sea through the Suez Canal, and the Atlantic through the Straits of Gibraltar. See also Stephen Blank and Carol Saivetz, “Russia Watches the Arab Spring,” *Radio Free Europe* (24 June 2011).

⁴³ *Interfax News Agency* (Moscow, in Russian) (4 August 2011). Mikhail Margelov, the Russian President’s special representative for Africa, noted that the Assad regime, through its suppression of the opposition, invites sanctions: “Through the bloody reprisals Syrian President Bashar al-Assad has made a transition to a political settlement of the situation extremely difficult and caused a justified toughening of positions against the regime and himself personally both inside and outside the country. The incumbent regime has thus branded itself a bloody regime and such regimes are doomed to end in our times if not tomorrow then in the foreseeable historic perspective.” *Interfax News Agency* (Moscow, in Russian) (5 August 2011).

⁴⁴ James M. Dorsey, “Syria’s Widening Protests: Assad Increasingly Beleaguered,” *RSIS Commentaries* 118/2011 (10 August 2011).

ropean engagement and therefore influence in the region. Anders Fogh Rasmussen, NATO's Secretary-General, has stressed the need for a "free, democratic, and stable" outcome in Libya. He argues that NATO's core values are "freedom, democracy, and human rights," and that the intensification of political dialogue and new partnerships in North Africa are distinct possible outcomes.⁴⁵ The new Secretary-General of the Organization for Security and Cooperation in Europe (OSCE) Lamberto Zannier has signaled that the promotion of democracy in the MENA region will become an OSCE priority, given the regions' shared interests in oil, trade, migration, and combating terrorism.⁴⁶ However, might a certain zero-sum logic become apparent within the EU? A reinvigorated European policy of southern engagement will, in an era of financial constraints and crisis, result in less time, attention, and resources being spent on states in Europe's common neighborhood—Russia's self-declared zone of privileged interest.

Conclusions: Transatlantic and Eurasian Strategic Convergence or Divergence?

Clearly, the outcome of the political transformations that are taking place in North Africa and the Middle East will very much determine the emphasis and stress all external actors place on advancing their stated interests and norms. A pragmatic Russia would cooperate where possible with consolidated market-democratic regimes in the MENA region, though this outcome would have a demonstration effect and impact throughout the former Soviet space, implicitly challenging the normative status quo. A market-democratic outcome would undercut the Russian notion that revolutions which allow for free and fair elections will further encourage the rise of radical Islamist regimes and spread the contagion to Eurasia. Russia's state ideology—Russia as a sovereign democracy—embraces the idea that economic modernization without political liberalization enables stability. A market-democratic MENA region would undercut this notion that democracy equals instability. Should the conservative reactionary regimes return to power in the MENA region, Western rhetorical and public support for representative and participatory institutions, structures, and processes in the region, rather than elite personalities, will grow, whatever the pragmatic reality is behind the scenes.

An analysis of the Arab Spring's reception in the former Soviet space suggests that the preexisting normative frameworks and strategic interests through which the

⁴⁵ Anders Fogh Rasmussen, "NATO and the Arab Spring," *The International Herald Tribune* (2 June 2011): 6. See also Anders Fogh Rasmussen, "NATO After Libya: The Atlantic Alliance in Austere Times," *Foreign Affairs* 90:4 (July–August 2011): 2–6.

⁴⁶ "OSCE Offers Aid for Arab Spring Democratization," *AssA-Irada* (Baku) (21 July 2011).

governing elites in the post-Soviet republics uphold and propagate their power at home and abroad have been reinforced. In Europe, the preexisting presumption of regional normative hegemony is in the process of being challenged. Strategic interests are being recalibrated, with the gap between values, norms, and interests closing. The Arab Spring's transformational impact should not be underestimated. It looks set to be a major factor in shaping strategic relations throughout both the Euro-Atlantic and Eurasian zones.

Connections: The Quarterly Journal

Submission and Style Guidelines


Connections accepts manuscripts in the range of 2,000 to 5,000 words, written in a lucid style for a target audience of informed defense and security affairs practitioners and academics. All manuscripts should be submitted to the *Connections* editorial office electronically at PfPCpublications@marshallcenter.org. They should feature the author's name, current institutional affiliation, and a provisional title at the top of the first page, and should include footnotes where necessary.

Preferred themes for the FY 2012 publication year include:

- Arctic Security
- Building Integrity and Reducing Corruption
- Comprehensive Approach to Emergency Management
- Cyber Security
- Defense Education
- Future of Multilateral Security Partnerships
- Human Security and the Role of Armed Force
- Impact of Non-State Groups
- Pooling Resources and Sharing Capabilities
- Responding to Revolutions
- Recruitment and Conscription Challenges

For questions on footnotes and references, please refer to the Chicago Manual of Style, at www.chicagomanualofstyle.org/tools_citationguide.html.

Unsolicited manuscripts are accepted on a rolling basis at the discretion of the PfPC Editorial Board.



The views expressed in all CONNECTIONS publications are solely those of the contributing authors, and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

The Operations Staff of the PfP Consortium of Defense Academies and Security Studies Institutes is located at the George C. Marshall European Center for Security Studies:

**Gernackerstrasse 2
Bldg. 102, Room 306B
82467 Garmisch-Partenkirchen, Germany
Phone: +49 8821 750 2333, Major Enrico Müller
Fax: +49 8821 750 2852
E-mail: pfpcconsortium@marshallcenter.org
<http://consortium.pims.org>**

**For all information regarding CONNECTIONS please contact the PfPC Operations Staff
at:
pfpcpublications@marshallcenter.org
or by using the information above.**

ISSN 1812-1098

