Journal of Strategic Security

Volume 6
Number 4 *Volume 6, No. 4: Winter 2013*

Article 1

Russia and Countering Violent Extremism in the Internet and Social Media: Exploring Prospects for U.S.-Russia Cooperation Beyond the "Reset"

Sharyl N. Cross Dr.
St. Edwards Unviersity and the Woodrow Wilson International Center for Scholars,
sharylcross@stedwards.edu

pp. 1-24

Recommended Citation
Cross, Sharyl N. Dr.. "Russia and Countering Violent Extremism in the Internet and Social Media: Exploring Prospects for U.S.-Russia Cooperation Beyond the "Reset"." *Journal of Strategic Security* 6, no. 4 (2013) : 1-24.
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1
Available at: https://scholarcommons.usf.edu/jss/vol6/iss4/1

Russia and Countering Violent Extremism in the Internet and Social Media: Exploring Prospects for U.S.-Russia Cooperation Beyond the "Reset"

Abstract

Russia has been targeted with a series of terrorist attacks over the past several years, and there are a growing number of extremist groups operating throughout Russia's society utilizing the Internet/social media to promote their narratives and objectives. Russia's policy community has created institutional mechanisms and laws to address the challenge of violent extremism in the Internet/social media, and recognizes the importance of international cooperation toward these ends. This study, based on primary research conducted in Moscow in 2012, defines Russia's assessment of domestic and international sources violent extremist threats; explains Moscow's perspective on balancing democratic principles with the challenge of countering violent extremism in the Internet/social media; assesses existing capacities and impediments to further international collaboration with Russia in countering violent extremism in the Internet/social media spheres; defines specific initiatives that Russia, the United States, and other nations of the world community could advance to enhance international cooperation in countering violent extremism throughout the world cyber community.

*Dr. Cross wrote this article while Professor of International Security and Politics at the George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen Germany.

She would like to express appreciation for research support provided for this project by the Institute of National Security Studies (INSS) at the United States Air Force Academy.

The views expressed in this article are those of the author and do not reflect the official policy or position of the George C. Marshall European Center for Security Studies, the U.S. European Command, the Department of Defense, or the U.S. Government.

"I can tell you that in the United States, the fact that we have free Internet - or unrestricted Internet access- is a source of strength, and I think should be encouraged. I think that the more freely information flows, the stronger the society becomes, because then citizens of countries around the world can hold their own governments accountable. They can begin to think for themselves. That generates new ideas. It encourages creativity."

- Barrack Obama, President, United States

"Blocking the Internet, cutting off global communication lines, and attempting to reach agreement with one's own people by force of arms—all of this leads nowhere."

- Dmitry Medvedev, Former President and Prime Minister, Russian Federation

We need "global monitoring of the threat of extremism" to include "establishing an agreed definition of extremism, maintaining a global database of extremist groups, and countering the spread of extremism in the Internet."

- Nikolai Patrushev, Security Council, Russian Federation

Introduction

Exponential Growth of Global Internet Usage & the Violent Extremist Threat

The United Nations (UN) reported that the number of Internet users in the world reached two billion at the beginning of 2011 representing a fifty percent increase over the period of the previous five years.[1] One in three people on the planet use the Internet. Cisco estimates indicate that total global Internet traffic increased eightfold over the period 2007-2012, and will increase another 29 percent over the period 2012-2016.[2] Estimates indicate that the total number of Internet users worldwide will reach 2.8 billion by 2015.[3]

Russia has an estimated 61.5 million Internet users in 2012, ranking number seven among nations in the world in terms of Internet usage.[4] Russian officials estimate that the number of Internet users in Russia could reach ninety million by 2013.[5] In 2011, .Ru moved from sixth to fifth place ranking of the largest domains in the world.[6] The second Russian national domain .РФ

[1] "Number of Internet Users Worldwide Reaches 2 bln: UN" *APF,* January 26, 2011, available at: *http://www.google.com/hostednews/afp/article/ALeqM5iL3JD4qYM6YTkh7BSVMHUn2z7qFg.*
[2] "Cisco Visual Networking Index: Forecast and Methodology: 2011-2016," available at: *http://www.itu.int/md/dologin_md.asp?lang=en&id=S12-WTPF13IEG2-INF-0002!!PDF-E.*
[3] "Internet User Forecast by Country," *ET Forecasts*, 2012, available at: *http://www.etforecasts.com/products/ES_intusersv2.htm.*
[4] "Top 20 Countries with the Highest Number of Internet Users," *Internet World Stats*, 2012, available at: *http://www.internetworldstats.com.*
[5] "Russian Internet Users to Reach 90 million in 2013," *The Economic Times*, January 5, 2012, available at: *http://articles.economictimes.indiatimes.com/2012-01-05/news/30593023_1_internet-users-broadband-internet-access-satellite-internet-services.*
[6] "Russian Domain Space 2011: Outcomes and Development Prospects," *Coordination Center for TLD .RU/.РФ.*, October 5, 2012, available at: *http://www.cctld.ru/en/news/news_detail.php?ID=3896&sphrase_id=88245.*

also ranks among the top twenty among European nations in terms of usage.[7] Among Russian Internet users, the most popular resources are available on *Yandex.ru*, *Rambler.ru*, and *Wikipedia.ru*.

Social media and social networking has also grown exponentially. The number of *Facebook* users exceeded 800 million by 2012.[8] Social networking and blogging communities popular in Russia include *Vkontakte*, *Facebook*, *Odnoklassniki*, *Linkedin*, *My Space*, *Google*, *Twitter*, *Ushahidi*, and more. Mikhail Yakushev observes that, "…Only a couple of years ago the number of users of Internet blogs or social networks was just a fraction of what it is now.

Five years ago, these services were virtually unknown."[9] Russia's former President and Prime Minister, Dmitry Medvedev, started his own blog in 2008 engaging with the public on the popular *LiveJournal*.

Nations have not been able to keep pace with preparing and responding to the security challenges accompanying the enormous growth of the Internet and social media networks. The threat of cyber war, cyber crime, and cyber terror has become very real and potentially devastating security challenges for nations of the twenty first century international community. Recent conflicts in Estonia and Georgia demonstrated the potential employment of cyber attacks in both state-to-state and non-state warfare. The Russian security and academic communities point to the cyber attack on Iranian nuclear facilities with the STUXNET virus as representing a critical turning point revealing the vulnerability of nation-states to cyber attacks. The world community is plagued today by threats of electronic identity theft, use of cyberspace by sexual predators, and many other types of criminal activity utilizing the Internet.

One of the most serious threats we face is violent extremists' harnessing of the Internet and social media to advance their agendas. The world community must not only confront terrorists and violent extremists in our public venues, as well as in the physical war zones, but equally or potentially even more important are the presence of those perpetrating ideologies of violence in the social networking sites to advance their narratives and interests. Moreover, all trends would only point toward the Internet and social media venues continuing to grow in the future, and we must anticipate that extremists purporting violence will continue to attempt to make full use of these mediums of communication.

For Russia, and other nations of the world, 90 percent of Internet users are under the age of thirty-five. The plethora of extremist video sites available at *YouTube, Google Video*, and other venues featuring highly creative and illustrative images are widely accessed, particularly among the youth. The policy community is sorely in need of innovative and creative approaches crafted with sufficient appreciation of the dimensions of such a threat in an increasingly globalized world where information can be exchanged instantaneously and freely from any point on the earth.

[7] Ibid.
[8] "Facebook Usage and Facebook Growth Statistics by World Geographic Regions," *Internet World Statistics*, September 2012, available at: *http://www.internetworldstats.com/facebook.htm*.
[9] Mikhail Yakushev, "Internet Governance: Politics and Geopolitics," *Security Index* 16:2 (2010): 36.

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1

Al-Qaida and its affiliates and other violent extremist groups have recognized the importance of images and perceptions, and widely utilize the traditional media and online platforms to disseminate their messages. Terrorist groups have skillfully employed the Internet and social media to recruit and indoctrinate followers, disseminate literature, instantaneously broadcast beheadings and other outrageous acts of violence, and to finance and coordinate attacks. The Task Force on the Future of Terrorism formed by the United States Homeland Security's Advisory Council (HSAC) in 2007 offered the conclusion that the "Internet has become a major facilitator of terrorist activities, especially the spread of jihadist ideology…" [10] Russian terrorist expert Ekaterina Stepanova observes that the Internet, offering a means of real time exchange of information, provides the perfect mechanism for disproportionate magnification of acts of violence.[11]

Philip Seib and Dana M. Janbek have documented the development of use of the Internet by contemporary terrorist groups. The establishment of *azzam.com*, originally established in 1996, eventually came to feature reporting on the Chechen and Afghan mujahedeen and offered a forum for exchanging teachings among the AQ-affiliated network throughout the world.[12] Sites such as *Al Neda*, *Global Islamic Media Front*, *Laskar Jihad* and others have served the full range of objectives for these groups including facilitating the transfer of ideological convictions.[13] For Russia, extremist websites such as *Kavkazcenter.com* promoting the establishment of an Islamist state in the Caucasus have posed a direct challenge to the existing government. The site is banned in Russia and appears on the world terror list for the United States, but *Kvakazcenter.com* continues to operate in several languages on the Internet.

Observers have noted that the appeal of these sites stems from the fact that they are anonymous, cheap, provide global reach, and prove difficult to monitor or control. The Internet and social media arenas offer the gathering point or virtual forum for like-minded individuals with shared views, grievances, and perhaps some basis for common identity. As Sajjan Gohel notes "…the virtual world is fast becoming the most important meeting place for terrorists…. After consolidating relationships over the Internet, the recruits can then plot and plan mass casualty attacks while remaining in contact with their handlers over the World Wide Web….."[14] Johnny Ryan has observed that participation in these chat rooms and websites advancing conspiratorial or religio-identity messages and symbolism may fulfill a deep psychological need for community or identity in an otherwise existence devoid of a social network. As Ryan states: "To be a part of an elite network, particularly a conspiratorial one, might be a large part of a person's existence…." which "…..allows a connection to an amorphous community to discuss matters regarded by the wider society as subversive, to find mentors, seek out justification…."[15] "It

[10] Homeland Security Advisory Council, "Report of the Future of Terrorism Task Force," *U.S. Department of Homeland Security* (Government Printing Office: January 2007).
[11] Ekaterina Stepanova, interviewed by author, Institute of World Economy and International Relations (IMEMO), Moscow, Russia, June 26, 2012.
[12] Seib, Philip and Dana M. Janbek, *Global Terrorism and the New Media: The Post Al Qaida Generation* (London: Routeldge, 2011), 26-27.
[13] Ibid.
[14] Sajjan M. Gohel, "The Internet and its Role in Terrorist Recruitment and Operational Planning," *CTC Sentinel* 2:12 (December 2009).
[15] Johnny Ryan, "The Internet, the Perpetual Beta, and the State: The Long View of the New Medium," *Studies in Conflict and Terrorism* 33 (2010): 676-677.

allows individuals who are isolated and alienated, both physically and psychologically, to feel that they are linked, empowered and members of an international movement..”[16] Extremist groups can tailor their images for particular audiences, and they target specific groups of society to include adolescents, women, or children.

In 2011, Russia’s Interior Minister Rashid Nurgaliyev reported that approximately 7,500 websites with extremist content were active in the Russian segment of the Internet.[17] The problem of terrorism in social networks is included on the agenda of the Russian Security Council. In April 2011, then President Dmitry Medvedev held a meeting with representatives of the Internet community acknowledging the range of security challenges associated with the “…..explosive growth of the Internet/blogosphere including manifestations of extremism, terrorism, crime, and threats to personal data information…...”[18] Dmitry Medvedev emphasized the difficulties these new mediums pose for managing the “creative commons” or issues of copyright.[19] Medvedev emphasized that it was important that the President make the right decisions with respect to all social relations including the Internet.[20]

The Arab Spring, combined with the widespread protest activity that took place in Russia during the Presidential election period in Spring 2012, brought the issues of the appropriate role of social media and regulation of these sources to center stage in Russia. Reflecting on concerns about the role of social media in revolutions, Oleg Demidov notes that, “…A harmless technology designed to help people socialize…is being portrayed as something of a weapon of mass destruction which poses a threat to the stability and security of individual nations and the international community as a whole.”[21] In July 2011, Demidov had organized a major conference entitled “Social networking Services in the Contexts of National and International Security” bringing together officials of the secretariat of the Russian government, Russian Ministry of Communication, U.S. Embassy in Moscow, Russian Foreign Ministry’s MGIMO, and other representatives of the security of social media communities to discuss Internet security and social media.[22] One of the main questions explored was whether social networking services could represent a national security threat.

While the state controls much of the television and news media in Russia, citizens in contemporary Russian society have been able to rely on the Internet as a source of information and communication with few restrictions. Many in society are quite anxious today about the potential for increasing government regulation and monitoring of the Internet and social media.

The United States will have to work together with partners throughout the world in finding the proper balance between protecting freedom of information and expression and security in

[16] Ibid.
[17] “About 7,500 Extremist Websites Active in Russia – Interior Min.,” *RIA Novosti*, March 8, 2011, available at: *http://en.ria.ru/russia/20110803/165530471.html*.
[18] “Meeting with Representatives of the Online Community,” *Meeting Summary: Office of the President [Kremlin.Ru]*, Moscow, April 29, 201.
[19] Ibid.
[20] Ibid.
[21] Oleg Demidov, “Social Networks in International and National Security,” *Security Index* 18:1 (2011): 23.
[22] “Social Networks: Security Threat or Asset?” *Conference summary: PIR Center Information* (Moscow: Bulletin PIR Press, 2012): 5.

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1

managing the threat from violent extremists. At what point do nations undermine the basis for a democratic society in attempting to manage violent extremism in the Internet or social media arenas? How far can nations go in regulating websites, for example, in instances when those sites are used to recruit terrorists and organize violent attacks? Should we be concerned that nations might exploit the threat of extremism to thwart democratic freedom and development? The new media venues will continue to present challenges for democratic societies in considering imposition of various levels of regulation when the technology is manipulated for purposes of fostering violence and harm to society.

Prospects for U.S.-Russia Security Cooperation on Countering Violent Extremism: Beyond the 'Re-set'

When then Senator Barack Obama assumed the Presidency, the state of U.S.-Russian relations in the immediate aftermath of the Russo-Georgian war was more strained than at any period during Russia's post-Soviet experience. At the Munich Security Conference in February 2009, U.S. Vice President Joseph Biden signaled early on that the new Administration sought to "press the re-set button" with Moscow, suggesting there are "many areas" where the United States "can and should be working together with Russia."[23]

In June 2010, following bilateral meetings held in Washington, President Obama suggested that he and Russia's President Dmitry Medvedev had "succeeded in re-setting" the U.S.-Russian relationship.[24] Obama noted that the two leaders discussed issues of disagreement to include Moscow's conflict with Georgia, and at the same time agreed to broaden cooperation in other critical areas. Significantly, in a period of only a few months, the United States and Russia succeeded in concluding a Strategic Arms Limitation Treaty (START) agreeing to mutual reductions and inspections. In addition, Russia is providing transit support for NATO's International Security Assistance Forces (ISAF) critical for the Afghan war effort, and the United States and Russia have expanded cooperation in the counter narcotics area working collaboratively in Afghanistan. The "re-set" was also accompanied by the creation of several U.S.-Russian presidential-mandated defense and military-to-military working groups aimed toward further deepening of security cooperation. Included among these are the U.S.-Russia working group on counterterrorism co-chaired by Daniel Benjamin (United States) and Alexander Zmeyevskiy (Russia), establishing countering violent extremism among the priorities. Both the United States and Russia have agreed that the issue of countering violent extremism requires additional active collaboration on the part of both nations and their counterterrorism partners.

Initial accomplishments in the U.S.-Russia "re-set" were accompanied by progress in the NATO-Russia relationship. While consultations in the NATO-Russia Council (NRC) had been suspended in the aftermath of the Georgian War, the exchanges were resumed with both parties emphasizing that the NRC must remain operative even in times of serious tension to ensure continued exchange of information and problem solving. In January 2011, the twenty-nine Chiefs of Defense of the NATO-Russia Council met in Brussels and concluded a Work Plan for

[23] "Biden Vows Break with Bush Era Foreign Policy," *Reuters*, February 7, 2009.
[24] "Obama, Medvedev Say 'Re-set' US-Russia Relations," *Associated Press*, June 24, 2010.

2011 covering several areas of security cooperation to include counterterrorism.[25] In November 2012, NATO and Russia completed the Joint Review of Twenty First Century Common Security Challenges that further defined the extensive range of shared security challenges faced by NATO and Russia, and identified priority areas for deepening cooperation in counterterrorism and other priority security issues.

Although the "re-set" initially appeared to reverse the downward spiral in U.S.-Russian relations, two issues tended to dampen prospects continuing to deepen bilateral cooperation. First, despite initial expectations that the success of forging an agreement on European missile defense could serve as a "game changer" shifting the U.S.-Russia relationship to a genuine "strategic partnership," the United States-NATO nations continue to remain deadlocked in failing to reach an agreement with Russia in this area. Russia's President Medvedev had initially proposed a "sector approach" whereby Russia would be responsible for intercepting missiles over Russia's territory bound for NATO nations. The Obama Administration rejected the proposal outright noting that NATO could never rely on non-NATO countries to include Russia for protecting the security of Alliance members. The Moscow leadership responded by threatening counter-measures including deployment of *Iskander* missiles in Kaliningrad.

A second major issue was Russia's parliamentary and presidential elections in 2011-2012. The reaction to Putin's re-election again was not received positively in Western capitals. Putin went to great lengths to create the perception of fairness in the election process including installing video cameras to monitor polling stations throughout the country for irregularities. However, the suppression of protest movements and storming the homes and confiscating money and equipment of opposition leaders crossed the line. The lack of a strong organized opposition virtually ensured Putin's election yet again with the potential that he would serve as Russia's President for two more six-year terms. U.S. Secretary of State Hillary Clinton was particularly sharp in her criticism of both the parliamentary and presidential election process expressing "serious concerns" about the conduct of elections and the arrests of peaceful protesters furthering aggravating the U.S. relationship with Moscow. [26] Putin responded suggesting that U.S. Secretary of State Clinton was trying to "stoke political unrest in Russia" with her accusations. Many in the West and among Russia's intellectuals were dismayed at what appeared to fall far short of standards for European-style democratic practice. [27]

Achieving further progress in the "re-set" in U.S.-Russia relations was also complicated by the Arab Spring. Concerns were raised regarding the potential spread of such movements into the Caucasus, Central Asia, and to the territory of the Russian Federation. Suggestions that the United States was somehow behind these uprisings were prevalent in policy and academic circles in Russia. The barrage of anti-U.S. coverage in Russia's state-owned television stations became even more prevalent in the aftermath of the Arab Spring and during Russia's elections. There was wide speculation in Russia that the United States was instigating or backing the revolutions

[25] "NATO-Russia Council Chiefs of Defence Approve the Work Plan for 2011," *NATO/Brussels*, January 26, 2011, available at: *http://www.nato.int/cps/en/natolive/news_70086,htm*.
[26] Elise Labott, "Clinton cites 'Serious Concerns' about Russian election," *CNN.com*, December 6, 2011, available at: *http://www.cnn.com/2011/12/06/world/europe/russia-elections-clinton/*.
[27] David M. Herszenhorn, "Despite Kremlin's Signal, U.S. Ties Remain Strained After Russia's Election," *New York Times*, March 6, 2012, available at*: http://www.nytimes.com/2012/03/07/world/europe/ties-with-us-remain-strained-after-russian-election.html?pagewanted=all&_r=0*.

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1

in North Africa and the Middle East. One analyst suggested that the Arab revolutions contributed to prompting deliberate attempts to further erode America's image among the Russian public through media sources so as to make it increasingly difficult for the United States to effectively assist opposition groups during Russia's presidential election period.[28]

Vladimir Putin might have intended to signal a certain distance from the United States by traveling to China during the election period. Many Western analysts viewed Putin's overtures toward China and the proposed Eurasian Union as evidence that he hopes to build a bloc among nations of the Shanghai Cooperation Organization (SCO) and the Collective Security Treaty Organization (CSTO) in order to counter U.S. influence.

Vladimir Putin's first meeting with President Obama following his re-election to the Presidency of Russia omitted any discussion of "partnership" and instead included only references to "cooperation." At the same time, during this first presidential meeting held in July 2012 in Los Cabos, Mexico, the two leaders again affirmed that, "…The United States of America and the Russian Federation are committed to furthering our multifaceted cooperation in counter terrorism. Both our nations face persistent and evolving domestic and transnational terrorist threats..."[29] Most recently, it was also encouraging that Russia granted ISAF permission to use the Ulyanovsk air base on Russian territory which will be especially important in supporting the withdrawal of NATO forces from the region.

Within the Kremlin, there are those who desire greater democratization in Russia, those who do not, and those who are not sure. With respect to the U.S.-Russia "re-set," there are influential forces in Russia's foreign policy community that view this as a "one time flip of switch" doomed only to result in another cycle of confrontation, and those who believe that the "re-set" was simply the first step in what should be a long-term process of building greater security cooperation.

While the United States and Russia share many common strategic interests, the perspectives and outlooks of both countries differ on a number of levels. The Russian leadership is determined to assert influence in the contemporary Middle East, and the Syrian case is perhaps one of the obvious illustrations of the differences in perspectives. Syria hosts the only Russian military base outside the Commonwealth of Independent States (CIS) at the port of Tartus, and military sales between the countries have been significant. Russia and China have held to a position of non-interference in Syrian internal affairs, while the United States and other NATO nations have called for the use of force in the crisis prompted by the objective of ending the human rights abuses of Bashar al-Assad's regime.

Putin appears to be clearly set on a path of "strategic independence," rather than integration with the Western security community. Putin's recollection of Russia's diminished status and influence during the period of the 1990s certainly contributes to making him quite determined to interact

[28] Mikhail Troitsky, interviewed by author, Moscow, Russia, June 23, 2012.
[29] "Joint Statement by the President of the United States of America Barack Obama and the President of the Russian Federation Vladimir Putin," *The White House, Office of the Press Secretary*, June 18, 2012, available at: *http://www.whitehouse.gov/the-press-office/2012/06/18/joint-statement-president-united-states-america-barack-obama-and-preside*.

with the United States from a position of strength rather than weakness. At the same time, Putin needs the United States and other Western nations for Russia's economic growth and modernization. U.S. support for Russia's admission to the World Trade Organization (WTO), and measures underway for visa liberalization would support these economic development objectives.

The Arab Spring and the recent presidential election have also complicated prospects for U.S. – Russian cooperation in countering violent extremism as an aspect of the U.S.-Russia post- "re-set" strategic relationship. Concerns among Russia's leadership that unlimited freedom in the social networking and media arenas could fuel similar upheaval among Russia's neighbors or in Russian society makes it difficult to find common ground in addressing the violent extremist challenge.

Perceptions of the Terrorist and Violent Extremist Challenge in Russia

Russia's central priority with the terrorist challenge has tended to concentrate on the threat emanating from Chechnya and the surrounding regions of the North Caucasus. Violence emanating from the Makhachkala region within Dagestan territory has been a priority concern in Russia's counter terrorist efforts. While there has been no single assault in Russia resulting in the loss of thousands of lives, such as the September eleven attacks in the United States, the nation has suffered a series of terrorist incidents over the past several years. Bombings of apartment buildings, theaters, subways, airlines, the school hostage incident in Beslan in 2004, and the more recent attack at the Domodedovo airport in January 2011 perhaps captured the most international attention and demonstrated Russia's vulnerability to the terrorist threat.

The violent extremist threat in Russia spans the gamut from Islamist extremists to militant ultra-nationalists. There are no official statistics on the number of Muslims in Russia. Figures range of three million to thirty million, with most sources estimating between eighteen and twenty million geographically concentrated in the large cities of the Volga-Ural and North Caucasus regions. Demographic trends indicating declining birth rates among Orthodox ethnic Russians compared with the relative growth among Russia's Muslim population suggests the potential for shifting political and social influence in the future. While the bulk of Muslims in Russia, primarily of the Sunni, Hanafist, and Sufi traditions, simply seek to practice their faith in peace, adherents of the anti-Sufi New Islamic Movement and radical Shahidists and Salafists share the objective of imposing a fundamentalist Islamic state under sharia law. Sharia courts operate today on Russia's territory in Dagestan, Ingushetia, and Chechnya. While some observers consider the influence of Wahhabism and Salafism a more recent phenomenon in the North Caucasus, the writings of Dagestini scholar Yaseen (Makhach) Rasulov and leader of the Sharia Jamaat group who was killed in 2006 traces the origins of to the anti-Russian resistance movements of the 18th century.[30] Socio-economic problems, unemployment, lack of opportunity, and corruption provide a fertile ground for recruiting followers in the region. Concerns with maintaining the territorial integrity of the Russian Federation have generated speculation about a potential contagion effect

[30] Andrei Smirnov, "Yaseen Rasulov: Dagestan's Rebel Scholar," *Jamestown Foundation Chechnya Weekly* 7:3 (January 18, 2007); Rasulov contended that Chechen Sheikh Mansur in the 18th century and Dagestani Imams Kazi-Mukhammad and Imam Shamil in the 19th century—were Salafists and Wahhibists.

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1

of the Arab revolutions that might inspire young people who have become disenchanted with traditional Islam in the North Caucasus, Tatarstan, and Bashkortostan.

Russia includes the Muslim Brotherhood among terrorist organizations, and a number of Islamist or Salafist publications have been banned in the country. Prosecutors in Birsk in Russia's Republic of Bashkortostan shut down a website during Summer 2012 for publishing a news portal entitled "Wake Up Tatar!" which was described as containing extremist ethnic and religious content.[31] Islamist groups that do not purport the use of violence such as Hizb-ut-Tahrir have also been targeted and banned.[32]

At the same time, the Russian government maintains constructive relations with the mainstream Islamic community in the country and abroad. Russian officials have engaged the Islamic community to combat extremism. Over the past several years, the office of the Russian President has held conferences involving the participation of foreign policy officials with Islamic religious clerics and leaders of other faiths in combating terrorism and extremism.[33] Russia holds observer status in the Organization of Islamic Cooperation (OIC), and does not include Hamas and Hezbollah as terrorist organizations as does the United States and other Western countries. At times, the Russian foreign policy community has suggested that Moscow could serve as a "bridge" between the Islamic and Western worlds emphasizing the importance of avoiding any "clash of civilizations" or religions in addressing the contemporary global terrorist challenge. [34]

Extreme nationalist groups have become more widespread in Russia over the past two decades and are a source of greater concern.[35] Riots in Manezhnaya square in December 2010 highlighted the problem when some 5,000 sports fans and nationalists groups went to the street in response to the death of a Spartak Moscow supporter who was killed in ethnic clashes with migrants of the North Caucasus. Vladimir Putin offered the observation that extremists used soccer fans as "cannon fodder" urging the necessity for "cracking down on all extremist organizations."[36] Putin noted: "…A person from the Caucasus should not be afraid to go out in the streets of Moscow, and our ethnic Slavic citizens should not be afraid to live in the North Caucasus republics..."[37] In responding to the riots, Deputy Prosecutor General Alexander Buksman emphasized that "those

[31] RFE/RL's Tatar-Bashkir Service, "Prosecutors in Bashkortostan Sue Tatar Website for 'Extremism,'" *Radio Free Europe/Radio Liberty*, August 2, 2012, available at: *http://www.rferl.org/content/prosecutors-in-bashkortostan-sue-tatar-website/24664411.html*.
[32] Alexander Verkhovsky, "Inappropriate Enforcement of Anti-Extremist Legislation in Russia 2011," *SOVA Center for Information and Analysis Report*, April 27, 2012, available at: *http://www.sova-center.ru/en/misuse/reports-analyses/2012/04/d24302/.*
[33] ITAR-TASS News Agency, "Moscow to Host Conference 'Islam Against Terrorism,' 3 June 2004 and conference held in July 2008 entitled 'Islam Will Conquer Terrorism'," available at: *http://www.muslim.ru*.
[34] Mikhail Titarenko, "The Islamic World and Russian Foreign Policy," *International Affairs (Moscow)* 4 (2005).
[35] For discussion of challenges of ultra-nationalism in Russia see Anastasia Mitrofanova, "The New Nationalism in Russia," unpublished paper, 2011; For an excellent background source on political and ethnic extremism in Russia see Emil A. Pain, "Xenophobia and Ethnopolitical Extremism in Post-Soviet Russia: Dynamics and Growth Factors," *Nationalities Papers* 35:5 (November 2007).
[36] "Putin Urges Crackdown on Extremism" *RIA Novosti*, December 16, 2010, available at: *http://en.ria.ru/russia/20101216/161801084.html.*
[37] Ibid.

who disseminate extremist ideology" have made "the best use of the Internet."[38] Recent new migration laws to support labor needs have also fueled inter-ethnic enmity and clashes.

Ultra-nationalist groups such as "Slavyansky Soyuz" or "Slavyanskaya Sila" (Slavic Union or Slavic Force) headed by Dmitri Demushkin [www.demushkin.com www.ns-88.org] also color the contemporary gamut of Russia's extremist political mosaic.[39] Extremist youth groups exist in almost all regions of the Russian Federation rallying under the banner of "Russia for the Russians," "skinheads," and others.[40] Fascism has also grown in recent years in terms of those affiliated with groups such as "Blood and Honor" (the Russian branch of the international neo-Nazi organization), "Russisky Kulak" (Russian Fist), "Nationalist Socialist Group 88," "Skinlegion," and others. Russia's President Vladimir Putin acknowledges the problem noting that "…Even in our country that did so much to vanquish Fascism we see, unfortunately, manifestations that are cause for shame."[41] These groups have become increasingly technologically competent developing websites to aid their recruitment efforts, and engaging in hacking to promote their objectives. Demushkin's "Slavyansky Soyuz" boasts an "information warfare department" pledging to close down websites of their so-called "enemies."[42]

Russia's political parties throughout the spectrum promote the importance of Russian values, culture, tradition—or the "Russian" as opposed to the "Western" model as the path most suited for their country. Pro-Kremlin groups for example champion themes characterizing the "West" as the "Other" and "Russia" as "Nashi" (Ours), whereas ultra- nationalist right wing groups trumpet references to "Great Russia" and racial superiority. As such, mainstream messages of patriotic national identity can at times become blurred with extreme ultra-nationalism. Russia's authorities have consistently spoken out against terrorism, extremism, xenophobia, and racism. However, Emil Pain makes the important point that Russian law enforcement authorities have been much more willing to employ force against Chechen nationalists and Islamist fundamentalists in the Republics of the North Caucasus, than to use coercive action in responding to extreme ultra- nationalist elements of the native populations.[43]

Russia's most recent National Security Strategy (to 2020) specifically identifies the threat of terrorism and extremism and vulnerabilities created by the "global information struggle." The document states:

> "The global information struggle will intensify, threats will increase to the stability of industrialized and developing countries, their socio-economic development and

[38] "Extremist youth groups widespread in Russia deputy prosecutor general," *RIA Novosti*, December 15, 2010, available at: *http://en.ria.ru/russia/20101215/161787991.html*.
[39] For discussion of recent activities of Demushkin's group, see SOVA Center for Information Analysis, "Spring 2012: Ultra-Right on the Streets, Law Enforcement on the Web," July 27, 2012, available at: *http://www.sova-center.ru*.
[40] *RIA Novosti*, December 15, 2010.
[41] "Speech of the Russian President Vladimir Putin at the Forum 'Let My People Live!' Commemorating the Memory of the Victims of Auschwitz," *Russian Kremlin Archives*, January 27, 2005, available at: *http://archive.kremlin.ru/eng/speeches/2005/01/27/2206_type82912type127286_83117.shtml*.
[42] See *http://www.demushkin.com* or *http:///www.ns-88.org*.
[43] Pain, *Nationalities Papers*, November 2007.

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1

> democratic institutions. Nationalist sentiments, xenophobia, separatism and violent extremism will grow, including under the banner of religious radicalism."[44]

Member of Russia's Security Council Nikolai Patrushev has called for the creation of a "global watchdog" to monitor violent extremism and terrorism in the Internet.[45] In an interview published in *Kraznaya Zvezda* following the 2012 Presidential elections, Patrushev offered the following observation on the relationship between terrorism, extremism, and information security:

> "At the threshold of the 21st century the primary threats to international peace and security have "shifted" to the information sphere. The intensive development of information and telecommunication technologies (IKT), the globalization of the information infrastructure and the information space along with its positive component also have the opposite side. In present-day conditions, the hostile use of IKT for criminal and terrorist purposes is becoming a real threat to international security."[46]

Patrushev continues underscoring the importance of international cooperation in information security: "...in modern conditions effectively providing national and international security and stability is impossible without strengthening security in the informational sphere, or as they are now saying, international information security..."[47]

The Moscow Patriarchate of the Russian Orthodox Church has expressed concern about the frequency of attacks made on religious leaders who resist extremism. Following a recent car bombing incident resulting in seriously injuring Mufti Ildus Faizov, Chief of the Synodal Information Department of the Russian Orthodox Church Vladimir Legoyda expressed concerns regarding increasing attacks against those "who resist extremism and preach the rejection of violence, and peaceful and balanced ways of dealing with problems…"[48] He continued emphasizing that: "…Fighting religious extremism is an acute problem facing the public in Russia..."[49] Archpriest Vsevold Chaplin has suggested that Russia and European countries should "adopt a law banning expansion of religious extremism, which results in deaths….."[50] He suggested that international organizations (Council of Europe and others) should equate the ban on religious extremism to the ban on Nazism, and noted that while "…Western ideologists believe a ban on spreading ideas is impossible. I am sure there is a need to restrict the expansion of such ideas as they justify the killing of civilians..."[51]

Russia's academic community has also addressed the terrorist and extremist information threats. For example, with support of the Russian government and the private sector, the Lomonosov Institute at Moscow State University has sponsored a series of conferences over the past several

---

[44] "Russia's National Security Strategy to 2020," *Rustrans*, September 17, 2012, available at: *http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020*.
[45] "Russia Calls for Global Extremism Watchdog," *RIA Novosti*, September 21, 2011.
[46] "Interview of the Russian Security Council Secretary Nikolai Patrushev," *Kraznaya Zvezda*, June 1, 2012.
[47] Ibid.
[48] "Terrorist Attack Rocks Tatarstan't Religious Community," *Russia Behind the Headlines*, July 19, 2012.
[49] Ibid.
[50] "Russian Orthodox Church Urges Law Banning Religious Extremism," *RIA Novosti*, April 29, 2012.
[51] Ibid.

years bringing together academics and security officials from many nations to examine the challenges related to information security in the cyber era. This initiative has led to breaking new ground in research, defining similarities and difference in perspectives among nations, and efforts to contribute to policy formation at the global level.

Russia: Legal Foundations on Countering Terrorism & Violent Extremism

In terms of building an international response, policy officials and scholars have been exploring the challenges for establishing legal foundations to meet the Common Vulnerabilities and Exposure (CVE) threat in the World Wide Web. The United Nations establishes a legal foundation for responding to terrorism in UN Security Council Resolution (UNSCR) 1373 and UNSCR 1624. While UNSCR 1373 made no mention of terrorist use of the Internet, UNSCR 1624 did address the expanded range of challenges posed by terrorism stemming from the Internet domain.

In the United States, the First Amendment protects freedom of expression, a major factor often impeding prosecution of suspected terrorists within the Internet and social media spheres where speech or even intended incitement of violence is insufficient basis for legal action. The United Kingdom is not bound by the same constitutional restrictions as the U.S., and has been more willing to prosecute terrorists in the Internet domain on the basis of intent to incite violence. The U.K.'s Terrorism Act of 2006 for example provided for broadening the government's authority to deal with those who seek to provoke terrorist acts to include regulation or dissemination of violent extremist publications.

Beyond the U.S. and U.K., one finds variations in the legislation or legal regulations to counter terrorist activity online. Turkish laws on terrorism demonstrate the variance among national legislation. Turkey's 1991 law on terrorism imposed restrictions on the publication of leaflets, periodicals, and forming associations. Turkey has no law specifically governing the Internet, though the law enforcement bodies have attempted to apply the Turkish Press Law to restrict the use of the Internet. Jordan was the first country in the Middle East to endorse anti-terrorism legislation that was similar to most European nations. Jordan's Anti Terrorism Law was implemented in 2006 following a series of suicide bombing attacks carried out by an al Qaida affiliate in Amman in 2005. In March 2008, Jordan began to impose additional restrictions in Internet cafes requiring owners to collect personal information on Internet users and to install cameras to be used for monitoring Internet usage.

In Russia, the tragic Beslan school hostage attack was a major catalyst for increasing centralization of government decision making and enhanced powers and accountability for law enforcement and security forces in combating terrorism. In 2006, a new anti-terror law came into force in Russia permitting Russia's security services sweeping powers to act against suspected militants and their supporters. Russian officials and lawmakers have pressed for stricter laws to regulate Internet usage both at home and in cooperation with other nations of the world community. Following the March 2010 subway bombings in Moscow, President Medvedev ordered that even tighter anti-terror laws be implemented. Articles 73 and 81 of the Criminal

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1

Procedure Code were adopted into federal law to enhance the effectiveness of measures to fight terrorism and extremism in April 2011. [52]

Russia's Federal Law "On Combating Extremist Activity" describes extremism as "activities of organizations or physical persons in planning, organizing, and carrying out acts aimed at inciting national, racial, or religious hatred."[53] While this law has been used to combat the dissemination of material that might incite violence, racial hatred, pornography, it has not been without considerable controversy. The law does not require establishing the threat of the use of inciting violence for prosecution. Russia's anti-extremism law has increasingly been used against peaceful religious groups and individuals deeming their activities as security threats. Non-traditional religious groups such as Jehovah Witnesses, Hare Kirshnas, and Scientologists in Russia have been repeatedly targeted under the law on extremism.[54] Stepanova makes the point that definitions are further complicated by the fact that terrorism and extremism are frequently defined in Russia as anything that can be deemed pro-separatist.[55]

Since 2007, the Ministry of Justice of the Russian Federation has compiled a list publications and materials deemed "extremist" and thus banned in the country.[56] As of mid-2013, there were more than 1,500 titles banned as "extremist" in Russia, with the bulk of the material coming from Islamic literature. Some of the more controversial banned materials have included the work of Turkish theologian Said Nursi, Elmir Kuliyev's "The Path of the Koran," Ibn Kathir's "History of the Prophets from Adam to Muhammed" or Sufi leaders Sefik Can's "Fundamentals of Rumi's Thought: A Mevlevi Sufi Perspective." The recent wave of bans on Islamic materials has been deemed as "absurd," and Islamic scholars and clerics have called for challenging court decisions restricting these materials.[57] Questions have also arisen as to whether the law on extremism might be used increasingly to stifle the activities and publications of the opponents of the Putin's United Russia party.

National Level Responses/Issues

Issues related to extremism on the Internet are managed by the Russian Federation's Security Council, Ministry of Interior, and Federal Supervision Agency for Information Technology. In 2011, then Russian President Dmitry Medvedev created an interdepartmental commission based in the Ministry of Interior responsible for combating extremism in Russia. Russia's Information Security Doctrine (2000) formed more than a decade ago is still in effect, and at the time the original strategy was conceived social media had not been developed.

---

[52] "Draft Law on Combating Terrorism and Extremism," *President of Russia Website*, April 30, 2011, available at: *http://eng.kremlin.ru/news/2155*.
[53] "Federal Law No. 114 FZ on Counteracting Extremist Activity (2002)," Adopted by the State Duma 27 June 2002, Approved by the Council of the Federation 10 July 2002, *Legislationline*, July 25, 2002, available at: *http://www.legislationline.org/documents/id/4368*.
[54] "Jehovah's Witnesses Charged with Extremism," *The Moscow Times*, July 31, 2012, Geraldine Fagan "Russia: 'Extremism' Religious Freedom Survey," *Forum 18 News Service*, July 23, 2012, available at: *http://www.forum18.org/archive.php?article_id=1724*.
[55] Ekaterina Stepanova Inteview, June 26, 2012.
[56] "Federal List of Extremist Materials," *Ministry of Justice of the Russian Federation*, 2012, available at: *http://minjust.ru/ru/extremist-materials*.
[57] Felix Corley "Russia: 'Absurd Bans," *Forum 18, News Service*, Norway, July 30, 2012; "Misuse of Anti-Extremism in June 2012," *SOVA Center for Information Analysis*, July 10, 2012.

Those working these issues in Russia's governmental structures devote the bulk of their attention to issues of education, crime, and especially to combating child pornography. Observers note that the Russian government relies heavily on Internet providers to counter the activity of extremism in online forums, but the providers are obviously not always able to effectively manage the posting of objectionable or criminal material online. Mikhail Yakushev notes that Russia's approach to Internet governance has taken two forms including technical management issues such as procedures for domain name registration and rules for allocation of Internet Protocol (IP) numbers, and a broader approach encompassing humanitarian, economic, and political dimensions to prevent the Internet from being used for harmful purposes.[58]

The Russian federal agency, Roskomnadzor, has been established to monitor Internet and media activities.[59] The agency scans the Internet and other media sources and issues warnings to Internet providers in the event that written or visual material posted online is deemed extremist or harmful content. The system functions as a robot with the task of vigilantly monitoring online sources for objectionable material. Internet providers are provided with a notice to remove objectionable content within twenty-four hours, and failure to do so can result in fines or other reprisals such as suspending the service.

During the summer of 2012, the Russian Duma passed three laws that were widely perceived as establishing a foundation that could be used to curb criticism of the government. The laws which came into force in November 2012, provided provisions for criminalizing slander, requiring non-profits receiving funding from abroad to declare themselves "foreign agents" and provide additional financial information, and a final law sanctioning the blocking of websites featuring content that "could threaten children's lives, health, and development..."[60] Major Internet providers in Russia, *Yandex*, *LiveJournal*, *Google Russia*, and the Russian branch of *Wikipedia*, immediately protested the new law claiming that it was passed in order to censor the Internet.

Since the laws came into effect November 1, 2012, the Mass Media Inspection Service has been permitted to block sites with objectionable content to include those promoting child pornography, suicide, or substance abuse, without the need for a court decision. Cases thus far on the Runet "blacklist" included *Absurdopedia* on one of the largest Russian language sites *Rutracker.org* for an article entitled "how to commit suicide the right way….", and imposing a block on *Lurkmore.ru* for posting material on marijuana use.[61] The Mass Media Inspection Service was reported to have issued a warning to *Newsland.ru* calling for removal of a fragment of the film "Innocence of Muslims" posted on its site.[62]

While the government owns and exerts control on the main television and media outlets in Russia, Russia's Internet users have enjoyed freedom of access to information from all over the world. Imposing legal and technical measures to regulate the Internet creates concern that it could be a first step in instituting a system of censorship of the media in Russia resembling the "Great Chinese Firewall" which blocks vast sections of the Internet from China's population.

[58] Yakushev, *Security Index*, 2010.
[59] "Robot to Search Internet for Extremism," *The Moscow News*, February 11, 2011; "Content Containment: Russian Blacklist of Outlawed Website in Force," *Russia Today (RT),* July 30, 2012.
[60] "Shutting Down Slanderers," *The Moscow News*, July 16, 2012.
[61] "Russia Begins to Introduce Censorship in Russian Internet Segment," *ITAR-TASS*, November 13, 2012.
[62] "Internet Censorship Faces Obstacles," *The Moscow Times*, November 14, 2012.

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1

Russia's Internet community and civic society has expressed concern that these measures would slow Internet service and freedom throughout the entire Runet. Leading academics worry that the new measures could limit academic freedom or the full access to information for research that they have enjoyed in the most recent decades. Activists in Russia's blogosphere who freely criticize leading political leaders on websites and social media are concerned about potential pressure, censorship, or intimidation resulting from such posts.[63] Some observers have argued that the creation of an Internet "blacklist" could ultimately lead to widespread censorship.

Russia's Minister of Interior, Rashid Nurgaliyev, suggested that monitoring of mass media to include *Youtube* and *Facebook* was necessary to manage "hate-mongering" and "extremism."[64] Director of Roskomnadzor, Mikhail Vorobyev, maintains that the creation of the Internet "black list" was necessary because the number of Internet media outlets was expanding.[65] The spokesman for Roskomnadzor Vladimir Panin noted that the "nasty things filling the Internet must be dealt with in some way..."[66] Russian officials have repeatedly offered reassurance that the ban on "harmful information" would specifically include web pages advocating suicide, substance abuse, child pornography, etc.[67] At the same time, Roskomnadzor would continue to monitor the web for other "unlawful information" that would "instigate national and religious hatred or war propaganda" leaving considerable room for defining these types of threats.[68]

The public response to the recent decision to permit ISAF access to the Ulyanovsk base for transit from Afghanistan is an interesting case in this regard. While Putin's leadership evidently realizes that such support would contribute to achieving a desired outcome in Afghanistan, there was considerable opposition in Russian society to permitting NATO access to the Ulyanovsk base on Russian soil. Local courts in Russia blocked popular web services *LiveInternet.ru* and *Tartala.ru* for uploading nationalist videos opposing the government decision to allow NATO to use the Ulyanovsk base.

It is important to note that leaders of European democracies have also favored imposing some restrictions on the Internet in the interest of societal security. For example, former French President Nicolas Sarkozy had called for a "civilized Internet" supporting the imposition of controls in the interest of making the Internet safe for children, commerce, and so forth. [69] The question still remains whether these new measures will ultimately lead to wide scale censorship of Russia's Internet and social media. Imposing such restrictions, given the culture of freedom of the Internet that has existed in Russia, will not be easy even if this is the ultimate intention. Russia's leadership has often underscored the importance of maintaining freedom of the Internet. In 2011, Vladimir Putin made the point in his annual address to the Duma that he opposed placing limitation on the Internet stating that there would be no "snip-snapping" [referencing a

[63] "Russian Duma Adopts 'Web Blacklist' Bill Despite SOPA-Style Censorship Outcry," *Russia Today (RT),* July 11, 2012; "Russia's 'Internet Blacklist' Law Sparks Fear for Freedoms" *Financial Times*, July 12, 2012.
[64] "Russia's Interior Minister Pushes for Extreme Internet Censorship Measures," *Gazeta.ru*, March 30, 2012.
[65] Ibid.
[66] Ibid.
[67] "Russian Duma Adopts 'Web Blacklist' Bill Despite SOPA-Style Censorship Outcry," July 11, 2012.
[68] Ibid.
[69] "Chaos of Internet Will Meet French Sense of Order," *New York Times*, May 20, 2011.

popular Soviet era anecdote about the Cheka secret police] or censorship of Internet.[70] President Medvedev made the point that "Russia will not support initiatives that put in doubt freedom in the Internet, freedom which is based on the requirements for morality and law."[71] He stated further that: "Blocking the Internet, cutting off global communication lines and attempting to reach agreement with one's own people by force of arms….all this leads nowhere…."[72] In the meeting with representatives of Russia's online community held in 2011, Medvedev suggested that each nation must "find their own balance" in "regulating extremism or criminal activities and freedom" based on the particular values, traditions, and decisions of the country.[73] Medvedev also noted that in comparison with other countries, Russia did not try to regulate everything.[74]

Global and Regional Level Responses/Issues

International agreements clearly delineating responsibilities for addressing the challenges presented by the use of the Internet and social media to disseminate extremist material or to indoctrinate recruits for the purposes of ultimately inciting violence might certainly be desirable. However, identifying common ground or establishing the basis for a unified international approach is fraught with difficulties as illustrated by the divergence among constitutional and legal provisions, and varying social-cultural expectations regarding the restrictions of freedom of expression and communication.

The Internet Governance Forum (IGF) was created to serve as an international platform for managing the World Wide Web. Russian officials have often expressed concerns regarding "ideological domination" of the cyber sphere.[75] Russians suggest that the United States maintains a leading competitive or even dominant position in the Internet with a disproportionate share of Domain Name System (DNS) servers and the leading Internet companies. Russians prefer a stronger role for the United Nations in governing the Internet holding the view that the current Internet Corporation for Assigned Numbers and Names (ICANN) establishes a dominant influence for the United States and other Western nations in the management of the Internet. In November 2012, Russia's Prime Minister Dmitry Medvedev suggested that laws should be developed "by all mankind" for the governances of the Internet, and complained that the United States does not want to participate since the United States "controls many things" in the Internet.[76] Medvedev stated: "Is this fair or not? It is unfair. I believe that, if we look at the future of the Internet, for example, there should be common rules developed by all states, not by just one country or group of countries."[77] Medvedev continued noting that while it is necessary to

[70] "Russia's PM Vladimir Putin Won't Snip-Snap Russian Internet," *publicity.ru*, April 22, 2011; see also "Internet Censorship Faces Obstacles," *The Moscow Times*, November 14, 2012.
[71] 2011 Davos World Economic Forum, "Russia supports non-restriction of Internet-Medvedev," *RIA Novosti*, January 26, 2011, available at: *http://en.ria.ru/russia/20110126/162320144.html*.
[72] "Medvedev warns against Internet shutdown over 'extremism'," *RIA Novosti*, February 22, 2011, available at: *http://en.ria.ru/russia/20110222/162718203.html*.
[73] "Meeting with Representatives of the Online Community," April 29, 2011.
[74] Ibid.
[75] Oleg Demidov, interviewed by author, Moscow, Russia, June 20, 2012.
[76] "Russian Premier Chides USA over 'Unfair' Internet Policy, Urges 'Common Rules,'" *Interfax*, November 2, 2012.
[77] Ibid.

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1

discuss creation of "global principles" for the world wide web, that it would be pointless to attempt to "monitor Internet content thoroughly" offering the observation that "if a topic became taboo in a particular state, the corresponding website is closed, the domain is closed, but an hour later is appears on a mirror website in another country…"[78]

The United States and Russia prefer different terms and place different priorities in addressing the security in the Internet and the dissemination of violent extremist material online. While the United States uses the term "cybersecurity" defined as securing computer networks and promoting the free flow of information, Russia employs the reference to "information security" which encompasses managing Internet and social media content that could result in destabilizing a government.

During the United Nations General Assembly in September 2011, Russia introduced a proposal entitled "International Code of Conduct for International Security" together with China, Tajikistan and Uzbekistan proposing a twelve point code of conduct based on the "need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security and adversely affect the integrity of infrastructure within states…"[79] The document also called for pledges to curb "the dissemination of information that incites terrorism, secessionism, or extremism that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."[80] Nikolai Patrushev has stressed the importance of reaching an international agreement on the definition of "extremism," but with a definition that would include "any attempt to subvert the state, take power by force or carry out terrorist activities."[81]

Many observers reacted to the proposal introduced by Russia and China in the UN suggesting that it could lead to censorship of international communication for any reason or filtering out communication that governments found objectionable. The U.S. approach placed priority on curbing cyber crime while ensuring free flow of information, but Russia and China clearly seek to limit cross-border information exchange that could result in destabilizing societies.[82] Michele Markoff, State Department Senior Advisor on Cyber Affairs, described the aims of the Russia-China proposal as intended "to justify the establishment of sovereign government control over Internet resources and over freedom of expression in order to maintain the security of their state."[83]

Nations of the Shanghai Cooperation Organization concluded an agreement in 2008 defining dissemination of "information harmful to social and political, social and economic systems, as well as spiritual, moral, and cultural spheres…" as among the main threats in the field of

[78] Ibid.
[79] "Russia's 'Draft Convention on International Information Security'," *Conflict Studies Research Centre (Oxford) and Institute of Information Security Issues,* Moscow State University, April 2012.
[80] Ibid.
[81] "Russia Calls for Global Extremism Watchdog," *RIA Novosti*, September 22, 2011.
[82] Jason Healey, "Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms," *Atlantic Council*, September 21, 2011.
[83] "State Department Official Accuses Russia and China of Seeking Greater Internet Control," *Huffington Post*, September 27, 2011.

"ensuring international information security."[84] Following the Arab Spring, concerns about the role of social media in playing an integral role in the uprisings ousting of longstanding dictatorships led nations of the CSTO to call for additional measures to combat extremism. At a CSTO meeting held in Bishkek in early 2011, Nikolai Bordyuzha, Secretary General of CSTO stated that "extremism is manifested in almost all CSTO countries, and we need to fight it, using common efforts." [85] Kazakhstan's President Nursultan Nazarbayev recommended joint study of the sources of extremism, and suggested regulating extremist material in the Internet that could "endanger governments." [86]

Members of the U.S. Congress across the political spectrum along with many private companies in the telecommunication and information/communication technology sector (ICTs) have objected to yielding greater control over the Internet to the United Nations. Russia, together with China, Brazil, and India, support shifting oversight of the Internet from the non-government ICANN to United Nations regulation. In December 2012, the World Conference on International Telecommunication (WCIT) met in Dubai with the mandate to review the International Telecommunications Regulations (ITRs). Ambassador Terry Kramer, Head of the U.S. delegation, addressed the conference rejecting measures to insert government control over the Internet, and instead emphasizing the importance of continuing to maintain the multi-stakeholder model of Internet governance.[87] In this regard, the U.S. position was in direct opposition to Russian proposals that would transfer management of the Internet to the government.[88]

Analysts have suggested that Russia's proposal on the "International Code of Conduct for International Security" does offer several important areas where common ground could be established within Western nations including protection of critical infrastructure from cyber attacks, enhancing cyber capacity among nations of the world, cooperation in monitoring violent security threats, and continuing to develop international norms for managing the cyber arena. At the same time, Jason Healey rightly observes that critical differences remain noting that while the United States and the United Kingdom pledged that the laws of armed conflict would apply in the cyber arena, Russia (and China) have yet to agree to be bound by these provisions.[89]

[84] Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, December 2, 2008, available at: *http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf*; "President Hu Visits 3 Nations, Attends SCO Summit," *Xinhua*, August 28, 2012; "International Experts Positively Assess Results of SCO Summit Ended in Beijing," *Penza News*, June 18, 2012.
[85] "The CSTO Member States Call to Fight Extremism Together," *Institute of Human Rights and Prevention of Extremism and Xenophobia*, February 16, 2011.
[86] "CSTO Members Should Cooperate in Resistance to Religious Extremism," *Trend*, December 20, 2011.
[87] Remarks by Terry Kramer, Ambassador U.S. Head of Delegation, World Conference on International Telecommunications, U.S. Department of State, Dubai, United Arab Emirates, December 13, 2012.
[88] "Drafters of Communications Treaty Are Split on Issue of Internet Governance," *New York Times*, December 6, 2012; "U.S. Ambassador on WCIT: Keep the Internet Out of This Conference," *ZDNet Government*, December 6, 2012.
[89] Healey, *Atlantic Council*, September 21, 2011.

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1

Conclusion

Challenges and Potential Opportunities for Engaging Russia on Countering Violent Extremism Post "Re-set"

Nations must recognize the magnitude of the task in attempting to manage the Internet and social media mediums for preventing the promotion of violent extremist ideology. The sheer volume of communication passing through the Internet and social media arenas would render attempts to monitor or impose restrictions on communication through these channels overwhelming. National or international government efforts to censor or filter sites or chat rooms have not been effective. Officials in Saudi Arabia have been among the most direct in complaining that while they may be successful at shutting down a website promulgating a violent message in their country, it will not be effective if the same user can find a willing Internet Service Provider (ISP) host in another nation. It has been frequently the case that Western ISP's can end up hosting these same sites without realizing it only because of the language barriers.

It is equally daunting to consider the challenge of building standards acceptable to all nations of the international community for regulating the Internet and social media of the twenty first century. Even for two countries sharing the most common values, the United States and the United Kingdom, there are differences in the level of public and societal tolerance for freedom of speech and unhindered communication. Building commonly accepted standards and norms for managing these new mediums among the diverse global community has proved quite difficult in the United Nations, and may never be fully realized.

Both the United States and Russia place a priority on countering terrorism and sources of violent extremism. However, as indicated, Russia's perspective on "information security" differs fundamentally with the U.S. approach resting on commitment to preserving freedom of information in the Internet and social media. In fact, the U.S. State Department has gone so far as to pledge to "undermine repressive governments" that seek to silence segments of society by "censoring or shutting down telecommunications networks…"[90]

Again, concerns on the part of Russia's leadership regarding the potential destabilizing impact of mass societal movements of the Arab Spring have complicated challenges for working with Russia on CVE. The role of the Internet and social networks in the Arab Spring upheavals has led governments throughout Eurasia including Russia to be even more determined to seek additional safeguards in protecting their regimes from the free exchange of information on the Internet. Reprisals against members of the political opposition during Russia's Spring 2012 elections, and new legislation establishing an institutional structure for potentially limiting information in the Internet arena has created additional barriers in achieving common ground with the Russians in the CVE area. Russia's current Prime Minister, Dmitry Medvedev, was correct in suggesting that nations will find their own balance concerning standards of freedom of information and providing security or between regulating extremism or criminal activities and freedom, and it remains to be see how far the Russian leadership will go in imposing new restrictions in managing the flow of information in Russia's Internet and news media arenas.

[90] James Glanz and John Markoff, "U.S. Underwrites Internet Detour Around Censors," *New York Times*, June 12, 2011, available at: *http://query.nytimes.com/gst/fullpage.html?res=9A00E4DC123EF931A25755C0A9679D8B63*.

The CVE issue strikes at the foundation of the value system for any country. It will be critical to continue to share perspectives at the national and global levels as Russia and other Counterterrorism (CT) partner nations sort through these issues in the years ahead. We should make every attempt to maintain dialogue with Russia's government and ministries and continue to engage with them at the official and academic levels to consider the interplay of societal values and strategies for effectively addressing the violent extremist challenge in the Internet and social media networks. The alternative is to refuse to engage on the issue with both countries potentially developing opposing strategies that can undermine effectiveness in this area. The challenges and differences notwithstanding, because of the priorities both countries place on countering terrorism and violent extremism, the CVE area still holds some potential as a part of a broad long-term sustained agenda for U.S.-Russia security collaboration post-"re-set."

In terms of specific recommendations, we must recognize that not only local or national, but also global engagement and collaboration are critical in countering violent extremism. The Obama Administration's strategy entitled "Empowering Local Partners to Prevent Violent Extremism in the United States" recognizes the critical role of local community partnerships and resources to combat extremism, but the United States approach does not discount the vital role that international partners play in combating the CVE threat that transcends borders.[91] In fact, as observers have noted, the U.S. counter terrorism strategy has been more global in focus, whereas other nations including Russia have tended to concentrate greater attention and resources on countering domestic sources of terrorism. The United States should continue to direct resources toward engaging Russia and other CT partner nations in exchanging "best practices" on countering violent extremism. Exchanges should include government, security and law enforcement, non-governmental organization (NGO), private sector, and academic expert communities across nations. Such collaboration is important for building trust and effective international responses on CVE. It is also important to exchange perspectives on areas of disagreement with the hope of reaching greater common ground. Community based approaches also form a vital component of an overall strategy reaching into local societies to ascertain causes of violence, and to compare similarities and differences for the drivers of radicalization across various contexts within or among nations.

As a priority element of U.S. engagement with Russia and other global partners on CVE, we should encourage the exchange of perspectives and experiences in developing national strategies for addressing the CVE challenge. As noted, Russia is still referencing an Information Strategy (2000) that was formed nearly thirteen years ago before social media had become prevalent throughout the Internet. Officials and specialists in Russia working in this area have acknowledged that Russia is in need of further development of approaches, and could benefit by considering the elements of national strategies of other nations. Many countries of the world community still do not have strategies for cyber security and CVE, and not all countries have included sufficient consideration to CVE issues and implications for security in social media in articulating their national approaches. Again, given the transnational nature of this challenge, any national strategy will have to be coordinated globally in order to be effective.

[91] Office of the Press Secretary, "Empowering Local Partners to Prevent Violent Extremism in the United States," *The White House*, Washington DC, August 3, 2011, available at: *http://www.whitehouse.gov/the-press-office/2011/08/03/empowering-local-partners-prevent-violent-extremism-united-states*.

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1

In addition, at the national level, the United States should share the importance of communication among various relevant ministries or agencies in assuming responsibility for cyber security and meeting the CVE challenges present on the Internet. Many nations suffer the problem of lack of communication among various ministries in developing approaches on CVE. Oleg Demidov and others have acknowledged that traditions of conservatism and secrecy among Russia's ministries can hamper effective responsiveness in this area.[92] In addition, observers in Russia's academic security community have noted that there is still a lack of clarity and transparency within Russia regarding appropriate agencies for managing the CVE challenge, and willingness on the part of some officials to share information regarding their responsibilities and approaches. [93] Twenty-first century communication among relevant entities at the national and global levels is critical for addressing the security challenges presented throughout the Internet and social media arenas.

Experts in Russia working on Internet security and terrorist use of the Internet and social media to promote their agendas suggest one area for potential cooperation would include support for ongoing efforts to establish standards for appropriate user identification. Terrorists have exploited the feature of anonymity in the Internet to disseminate narratives. Establishing reliable means to identify users may be an important measure for addressing this challenge. Lax measures for user registration will be exploited by those purporting violence and other crimes, and we should encourage discussion of the issues surrounding standards for user identification in the Internet on an international level.

Overall, Russians have more readily moved to simply shut down objectionable websites, rather than to permit such sites to remain functional for purposes of monitoring as in the United States. The Obama Administration strategy openly acknowledges the important role for monitoring the activities of violent extremists. The August 2011 CVE strategy states: "…We will continue to closely monitor the important role the Internet and social networking sites play in advancing violent extremist narratives…"[94] Anders Breivik, who carried out the mass bombing and shooting attacks in Norway in 2011, evidently had contact with ultra-nationalist groups in Russia via *Facebook*.[95] Intelligence agencies have certainly benefited by monitoring these sites and chat rooms providing opportunities to learn more about the ideology and tactics of violent groups, followers, and so forth. Russia's security community has cooperated with the United States and other Western countries in monitoring and exchanging information on violent extremist threats in the Internet. There are obvious potential benefits for joint monitoring of such activities in the Internet, and international collaboration will be important for prevention of deadly attacks in the future.

Governments of the twenty first century must recognize the power of the Internet and social media network and be prepared to engage in these communities in promulgating their narratives; otherwise terrorists or violent extremists will surely gain ground in the so-called information wars. At the governmental level, the Obama Administration has emphasized the importance of offering counter-narratives for the messages of those motivated by ideologies of violent

[92] Demidov, *Security Index*, 34.
[93] General Pavel Zolotarev, interviewed by author, Moscow, Russia, June 25, 2012.
[94] "Empowering Local Partners to Prevent Violent Extremism in the United States," August 2011.
[95] Anastasia Mitrofanova, interviewed by author, Moscow, Russia, June 22, 2012.

extremism, and then leaving it to the public to weigh different positions to reach their own conclusions on issues. The U.S. State Department has developed a team of bloggers in the Department's Counterterrorism Communication Center to counter false stories and disinformation in a number of languages.

In 2012, Russia's Foreign Ministry opened a *Facebook* account and stepped up contributions on *Twitter* in recognition of the need to communicate positions to the public.[96] Russia's President Vladimir Putin appears to recognize the importance of official communication on the Internet using social media stating that "…You must explain our points of view again and again, on various platforms and using new technologies until the message gets across…"[97] The Kremlin has enlisted bloggers in the North Caucasus and Chechnya to counter the messages of extremists, but these individuals can be identified with the government and thus can suffer a lack of credibility among the local target communities.

The Internet, new social media sites, and real time communication forums in chat rooms or blogs provide significant venues for officials to engage directly with the public and the youth, and potentially greater transparency and better understanding of particular policy responses. National communication responses must make full use of the most sophisticated new technologies of the information revolution. It is critical that the potential audience for violent extremist movements not perceive government communication as attempts to manipulate societies or practice ideological "spin. To be effective, public diplomacy efforts and the messages delivered must be consistent with substantive policy and behavior. The importance of trusting the messenger can never be underestimated. Rather, an honest, open, and reliable communication holds the greater promise for effectiveness.

Nations committed to combating terrorism and violent extremism must continue to devote attention and resources to addressing the underlying societal forces that create the environments that fuel terrorism. Much of the appeal of the Muslim Brotherhood, Hamas or Hezbollah results from their ability to meet the desperate social service needs in poor communities or war-ravaged societies. Governments must realize the importance of providing potential recruits with better options than joining the ranks of terrorist movements.

It is important to recognize that legitimate religious authorities possess the greatest potential for discrediting the Islamist violent extremist narrative. All investigations with respect to addressing this problem point to the critical role that religious authorities can offer in de-legitimizing the militant extremist narratives and messaging. The publication of the Amman Declaration on the official website of the Jordanian government, and in many other Internet sites, featuring official religious denunciation of violence has been quite significant in discrediting the violent extremist agenda. The Saudi Sakinah campaign that engages Islamic clerics online to turn extremists away from violence has demonstrated results, and offers a promising approach for the future. This program enables Imams to enter social media venues with a well-supported counter narrative denouncing the path of violence by specific reference to religious teachings. Directing resources toward amplifying the speeches of clerics who renounce violence are surely among the most effective strategies for addressing this problem.

[96] "Foreign Ministry Embraces E-Diplomacy," *The Moscow Times*, July 16, 2012.
[97] Ibid.

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1

Communication and narratives must continue to reinforce rejections of any notion of a "clash of cultures" or "clash of civilizations." The visual messages featured on the websites of violent extremists often couple imagery of heaven and virtue with the violent cause. Communication at every level should challenge messages depicting death, destruction, and hate with promoting the will of God and human advancement. In an effort to de-legitimize the ideological underpinnings of militant extremist ideology, it is critical to use the Internet and social media arenas to expose the vision offered by al Qaida and its affiliates for the future of the international order. The imposition of a fanatic totalitarian theocratic order hardly seems like a realistic or appealing prospect for today's international community, or for most of the world's Muslim population. The fact is that the militant radical message is largely rejected within the Muslim world as inconsistent with the most fundamental teachings and values of Islam and lacking relevance to the realities of modern life. The recent uprisings sweeping Arab nations reflected the legitimate democratic aspirations of these societies and desire for greater economic opportunity and quality of life, not to promote the vision of a totalitarian global caliphate envisioned by al Qaida and its affiliates for the future of nations or the world community.

The efforts of the Russian government and the Russian Orthodox Church to engage Russia's Islamic clerics in condemning violence and violent extremism are promising and should be encouraged. Dmitry Medvedev made the point that: "It is important to create our own websites, extend our presence in the networks, create religious sites, giving Muslim preachers and all persons concerned an opportunity to speak up…"[98] There should be further opportunities for engaging the religious communities in the United States and Russia in inter-religious dialogue and collaboration in countering terrorist and violent extremist narratives through the Internet and social network sites.

As a part of the overall strategy to counter violent extremism, it is important for governments to consider partnership with the private sector on multiple levels. The United States, Russia, and other CT partner nations should pursue all options in cooperating with the private sector to develop Internet and social media initiatives targeting those vulnerable to the militant agenda, and contribute to developing alternatively more productive paths. The 2011 *Summit Against Violent Extremist*, hosted by Google Ideas bringing together former extremists across the spectrum to share perspectives, is a good example of the potential positive contributions to addressing the CVE challenge from the private sector.[99]

Educational efforts on every level are obviously critical to combating the terrorist and violent extremist narratives. The Internet and social media arenas can provide major sources of information and knowledge resources, and should be fully appreciated and utilized in positive directions in pursuit of learning. Engaging the younger generation through these channels has become, and is likely to be even more important for the future. On a societal level, it is important that early education includes knowledge of the Internet, user agreements, social networks etc.[100]

---

[98] Ibid.
[99] "Ex-terrorist Network? 'Facebook' for Former Extremists," *Russia Today (RT),* April 27, 2012.
[100] Mikhail Yakushev has stressed the importance of education in his assessment of Internet security; "Meeting with Representatives of the Online Community," April 29, 2011.

At advanced educational levels, nations will require highly skilled technical and linguistic expertise to manage Internet and social networking security. Those in the government charged with responsibilities for Internet security must have the appropriate training and skills. This is often a problem because the frequently better incentives for employment in the private sector can continue to draw the most able experts away of the public sphere.

The United States and Russia should encourage continued joint research collaboration on countering violent extremism. Since 9-11, we have made considerable progress in strengthening research resources and collaboration on terrorism throughout the world. In 2007, the Marshall Center collaborated with NATO's Center for Excellence-Defense Against Terrorism (COE-DAT) and the NATO-Russia Council to hold a five-day conference in Ankara on societal sources of violent extremism. Several specialists from the United States, Russia, and Turkey contributed expertise to exploring the CVE issue from security, political, social, and cultural perspectives. Such initiatives contribute to building knowledge and common understanding of these complex challenges. The United States, Russia, and other CT partner nations can benefit by developing additional methods and objective case studies for unraveling the sources of radicalization. Comparative studies of websites and chat rooms in different languages also provide valuable resources for domestic and international intelligence agencies or those responsible for countering the terrorist narratives.

Finally, the United States should continue to emphasize in discussions with the Russians in the CVE working group and other channels the importance of cultivating mechanisms for democratic participation as a means for countering the violent extremist appeals. Particularly for nations with diverse multi-cultural populations, cultivating a strong sense of citizenship rather than ethnic affinity is essential for national cohesion. Russia's success in managing the challenges of diversity will be critical for the future development of the nation. The violent Islamist agenda threatens the United States, Russia, and many other nations throughout the world. At the same time, threats from radical ultra-nationalists should also not be underestimated. Legitimate channels for participating in the political process or resolving grievances available in established democratic systems provide appropriate and effective alternatives to violence and terrorism for those seeking to achieve political objectives. The tsunami of violent upheaval sweeping Arab nations was to no small extent fueled by the Internet and social media savvy of young people who sought freedom and opportunities for self expression in governance after decades of suffering, and who could no longer continue to tolerate entrenched authoritarian repression and lack of opportunity. Hence, commitment to maintaining democratic values and institutions, protecting freedom of information, ensuring human rights for all citizens are some of the most potent weapons in countering the agenda of violent extremists across the political spectrum.

https://scholarcommons.usf.edu/jss/vol6/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.6.4.1