THIRD WAY

PRIMER *Published May 24, 2016 • 5 minute read*

Country Brief: Russia

Gary Ashcroft
2016 Fellow for National Security

David Forscey
Fellow, National Security Program

Takeaways

Russia's aggressive moves in cyberspace and efforts to undermine European solidarity mean it remains a security challenge, despite its crumbling economy. A tough and smart Russia policy means using various aspects of U.S. power to push back against Putin in cyberspace and Eastern Europe, while keeping an open line to Moscow on issues that require cooperation, including:

- Counterterrorism and the civil war in Syria
- Reducing the threat of nuclear weapons
- Access to Afghanistan
- Space cooperation

Russia maintains the world's largest nuclear arsenal, and is the sole country—other than the United States—with the capability to completely destroy the planet. Its once-decrepit military has undergone significant modernization, outmatching U.S. forces in some areas.[1] Russia remains an influential international actor. With its permanent seat on the United Nations Security Council (UNSC), Russia can veto U.S. proposals. In almost every area that is of concern to U.S. national security, U.S. officials must contend with Russia. Most often, that means dealing with Russian President Vladimir Putin, who controls state media, eliminates or silences his political opponents, and maintains an iron grip on political power.

Getting Tough On Eastern Europe and NATO

Russian aggression has revived NATO's purpose: countering Russia. Putin's military intervention in Eastern Ukraine has convinced Eastern European governments to boost defense spending and forge closer ties with the United States. In December 2015, NATO grew to include Montenegro, adding its first new member since 2009. Other European nations, like Finland and Sweden, have moved to strengthen their ties with NATO.[2]

Nevertheless, Russia benefits from close proximity to NATO allies, in particular Estonia, Latvia, and Lithuania. Russian forces could capture substantial territory in a surprise invasion.[3] The United States and its allies are hardening their defenses and updating war plans to address new Russian tactics,[4] but in the short-term, we must avoid giving Russia a pretext to escalate tensions.

Being Smart on ISIS and Syria

In September 2015, Russian military forces began attacking Syrian rebels to help guarantee the survival of the Assad regime. Since then, Russia has continued to conduct operations in Syria and has even bombed humanitarian aid convoys supplying rebel-held areas.[5] Russia's military involvement and commitment to the Assad government[6] mean that any political solution to the civil war will likely require cooperation between Washington and Moscow. Although the U.S. and Russia worked together to broker ceasefires in February and September of 2016, those truces have frequently been violated by actors on both sides of the conflict.[7]

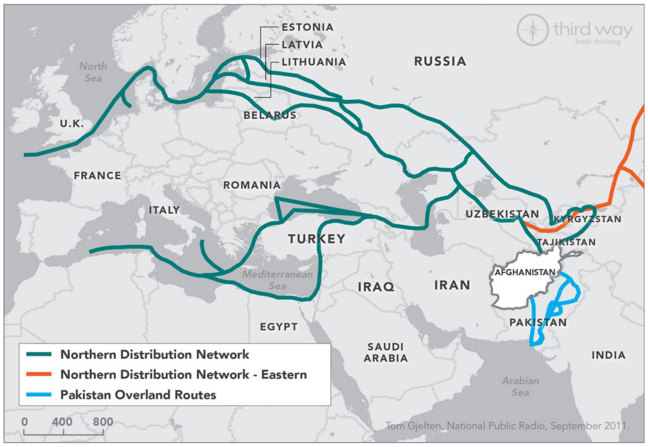
While ceasefires have been largely unsuccessful, the U.S. and Russia should continue to communicate to avoid confrontations between their air forces operating in Syria[8] and work toward a future political solution to the conflict. In addition, any U.S. response to Russian actions in the Middle East must be mindful of the U.S. objectives of defeating ISIS and getting rid of Assad.[9]

Being Smart on Nuclear Weapons

Russia is indispensable to preventing the spread of nuclear weapons, securing stockpiles of nuclear materials, and preventing nuclear terrorism. The United States and Russia have shared this commitment through various arms control agreements, including the New START Treaty. Russian cooperation has been and will continue to be essential to enforcing the terms of the 2015 nuclear agreement with Iran, the Joint Comprehensive Plan of Action (JCPOA). Russia was responsible for removing 25,000 pounds of enriched uranium from Iran, effectively reducing Iran's stockpile to 300 kilograms - as required under the JCPOA.[10] Russia will be a necessary player in any nuclear negotiations with North Korea as well.

Both the United States and Russia are modernizing their nuclear arsenals[11] and must work closely to maintain transparency into their weapons development. The U.S. and Russia signed the Intermediate-Range Nuclear Forces (INF) Treaty in 1987 in an effort to ban certain nuclear and conventional land-based missiles. In 2013, the U.S. reported that Russia was in violation of this treaty.[12] Although the U.S. has brought this violation to Russia’s attention, nothing of consequence has been done. The United States and Russia should revive previous cooperation to secure loose nuclear fuel, which they have all but abandoned, and continue to pursue efforts that prevent the proliferation of nuclear weapons.[13]

Being Smart on Afghanistan



Tom Gjelten, National Public Radio, September 2011.

Cooperation with Russia is necessary to assist the U.S. mission in Afghanistan. Currently, the U.S. plans to keep 8,400 U.S. troops in Afghanistan until the end of Obama's term,[14] and special operations forces will also remain for the foreseeable future. Flying supplies into Afghanistan is expensive, so U.S. forces need ground access into the landlocked country. Convoys traveling through Pakistan (in blue) are exposed to insurgent attacks, and Pakistan has occasionally cut off access. The United States may need to depend on railroads running through Russia (in green) to supply U.S. troops in Afghanistan. Washington should not allow chilly relations with Moscow to put our military at risk and impede efforts against terrorists.

Being Smart on Space

The U.S. and Russia work closely on space exploration. Until 2017, when NASA plans to deploy its Orion space capsule, the Russian space agency will bring American astronauts to the International Space Station (ISS). Many of the space rockets used by American companies to loft U.S.

satellites into orbit use Russian rocket engines, although the U.S. military cannot use them.[15] The United States is working to reduce reliance on Russia for its space activities, but until that time, we must ensure that tensions on Earth do not affect our operations in space. Furthermore, as the two most experienced space-faring nations, the United States and Russia must work together to mitigate the impact of space debris that can damage or destroy space assets.

Getting Tough on Russian Hacking

Russia-based hackers have been tied to attacks on the Democratic National Committee,[16] the penetration of voter registration systems in Arizona and Illinois,[17] and even espionage operations against the U.S.'s power grid.[18] Russian hackers have also targeted pro-U.S. governments – they crippled Ukraine's vote-tallying network before a crucial election,[19] attacked NATO member Estonia's banking and telecom systems,[20] and assaulted Georgian servers as a prelude to Russia's invasion of that country.[21]

Though some believe the U.S. should respond in kind to Russian cyberattacks, such an approach should be reserved for attacks on critical infrastructure and voting systems. Using cyber weapons against Russia might provoke an "arms race" that could harm the U.S. technology sector and consume taxpayer resources.[22] Rather, many cyber experts have suggested that the U.S. deploy an interdisciplinary response[23] to Russian aggression by using targeted sanctions,[24] prosecutions of enemy hackers,[25] and enhanced government cooperation with the private sector.[26] In addition, Russian cyber aggression may be checked by increases in funding for cybersecurity outlined in Defense Secretary Ash Carter's recent budget request.[27]

TOPICS

FOREIGN RELATIONS 115

END NOTES

1. Sydney J. Freedberg, “Army Electronic Warfare Investment Lags Russian Threat,” *Breaking Defense*, March 21, 2016. Accessed April 29, 2016. Available at: http://breakingdefense.com/2016/03/army-electronic-warfare-investment-lags-rhetoric-russians/.

2. Sweden and Finland Upgrade NATO Relations, *EU Observer*, May 20, 2016. Accessed September 19, 2016. Available at: https://euobserver.com/nordic/133493.

3. David A. Shlapak amd Michael Johnson, “Reinforcing Deterrence on NATO’s Eastern Flank,” *RAND Corporation*, 2016. Accessed September 20, 2016. Available at: http://www.rand.org/pubs/research_reports/RR1253.html.

4. Julia Iofee, “Exclusive: The Pentagon is Preparing New War Plans for a Baltic Battle against Russia,” *Foreign Policy*, September 18, 2015. Accessed September 20, 2016. Available at: http://foreignpolicy.com/2015/09/18/exclusive-the-pentagon-is-preparing-new-war-plans-for-a-baltic-battle-against-russia/.

5. Pierre Vaux, “This is How Russia Bombed the U.N. Convoy,” *The Daily Beast*, September 21, 2016. Accessed September 27, 2016. Available at: http://www.thedailybeast.com/articles/2016/09/21/this-is-how-russia-bombed-the-un-convoy.html.

6. Matthew Bodner, “Russia Digging in for Long Haul in Syria,” *Defense News*, December 14, 2015. Accessed May 3, 2016. Available at: http://www.defensenews.com/story/defense/policy-budget/warfare/2015/12/13/russia-digging-long-haul-syria/77148866/.

[7] *See* Angela Dewan, “Syrian Airstrikes Kill 23; Russia, US Allege Violations,” *CNN*, September 15, 2016. Accessed September 27, 2016. Available at: http://www.cnn.com/2016/09/15/middleeast/syria-ceasefire/; *see also* “Syrian War: Russia and Opposition Allege Truce Breaches,” *BBC News*, February 28, 2016. Accessed September 27, 2016. Available at: http://www.bbc.com/news/world-middle-east-35681256.

[8] *See* David Axe, “U.S. and Russian Jets Clash Over Syria,” *The Daily Beast*, June 19, 2016. Accessed September 27, 2016. Available at: http://www.thedailybeast.com/articles/2016/06/19/u-s-and-russian-jets-clash-over-syria.html.

[9] Matthew Rosenberg and Neil MacFarquhar, “U.S. and Russia Find Common Goals on Syria, if Not on Assad,” *The New York Times*, October 23, 2015. Accessed September 27, 2016. Available at: http://www.nytimes.com/2015/10/24/world/middleeast/us-and-russia-find-common-goals-on-syria-if-not-on-assad.html?_r=0.

[10] Laura Wagner, “Iran Ships over 25k Pounds of Uranium to Russia as Part of Nuke Deal,” *National Public Radio*, December 28, 2015. Accessed April 29, 2016. Available at: http://www.npr.org/sections/thetwo-way/2015/12/28/461302481/iran-ships-more-than-25-000-pounds-of-uranium-to-russia-as-part-of-nuclear-deal.

[11] Steven Pifer, “Who Needs a New Nuclear Air-Launched Cruise Missile Anyway?,” *Brookings*, December 10, 2015. Accessed April 29, 2016. Available at: http://www.brookings.edu/blogs/order-from-chaos/posts/2015/12/10-long-range-stand-off-weapon-unnecessary-pifer.

[12] Mike Eckel, “NATO Chief: Russia Tested Missile Last Month in Violation of INF Treaty,” *Radio Free Europe*, October 31, 2015. Accessed May 3, 2016. Available at: http://www.rferl.org/content/nato-chief-breedlove-russia-tested-missile-last-month-violation-inf-treaty/27336937.html.

13. Rachel Oswald, “Chill with Russia Brings Nuclear Insecurity,” *Pulitzer Center on Crisis Reporting*, November 20, 2015. Accessed April 29, 2016. Available at: http://pulitzercenter.org/reporting/chill-russia-brings-nuclear-insecurity.

14. Missy Ryan and Karen DeYoung, “Obama Alters Afghanistan Exit Plan Once More, Will Leave 8,400 Troops,” *The Washington Post*, July 6, 2016. Accessed September 19, 2016. Available at: https://www.washingtonpost.com/world/national-security/obama-alters-afghanistan-exit-plan-once-more/2016/07/06/466c54f2-4380-11e6-88d0-6adee48be8bc_story.html.

15. Andrea Shalal, “ULA Orders 20 More RD-180 Rocket Engines,” *Space News*, December 23, 2015. Accessed April 29, 2016. Available at: http://spacenews.com/ula-orders-20-more-rd-180-rocket-engines/.

16. Ellen Nakashima, “Russian Government Hackers Penetrated DNC, Stole Opposition Research on Trump,” *The Washington Post*, June 14, 2016. Accessed September 19, 2016. Available at: https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?hpid=hp_hp-banner-main_dnc-hackers-1145a-banner%3Ahomepage%2Fstory.

17. Ellen Nakashima, “Russian Hackers Targeted Arizona Election System,” *The Washington Post*, August 29, 2016. Accessed September 19, 2016. Available at: https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html.

18. Siobhan Gorman, “Electricity Grid in U.S. Penetrated by Spies,” *The Wall Street Journal*, April 8, 2009. Accessed September 19, 2016. Available at: http://www.wsj.com/articles/SB123914805204099085.

19. Margaret Coker and Paul Sonne, “Ukraine: Cyberwar’s Hottest Front,” *The Wall Street Journal*, November 9, 2015. Accessed September 27, 2016. Available at: http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671.

20. Joshua Davis, “Hackers Take Down the Most Wired Country in Europe,” *Wired*, August 21, 2007. Accessed September 27, 2016. Available at: https://www.wired.com/2007/08/ff-estonia/.

21. John Markoff, “Before the Gunfire, Cyberattacks,” *The New York Times*, August 12, 2008. Accessed September 27, 2016. Available at: http://www.nytimes.com/2008/08/13/technology/13cyber.html.

22. *See* “Obama Warns of Cyber ‘Arms Race’ with Russia,” *Politico*, September 5, 2016. Accessed September 19, 2016. Available at: http://www.politico.com/story/2016/09/obama-russia-cyber-arms-race-227732.

23. *See* United States, Senate. Committee on Armed Services, “Encryption and Cyber Matters,” Testimony, By Mike Rogers, 114th Congress, 2nd Session, September 13, 2016. Accessed September 19, 2016. Available at: http://www.armed-services.senate.gov/hearings/16-09-13-encryption-and-cyber-matters.

24. *See* Brian Bennett, “Responding to Cyberattacks, Obama Orders Sanctions for Foreign Hackers,” *LA Times*, April 1, 2015. Accessed September 19, 2016. Available at: http://www.latimes.com/nation/nationnow/la-na-cyber-sanctions-20150401-story.html.

25. United States, Department of Justice, Office of Public Affairs, “U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage,” Press Release, May 19, 2014. Accessed September 19, 2016. Available at: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

26. Ian Wallace, “The Military Role in National Cybersecurity Governance,” *The Brookings Institution*, December 16, 2013. Accessed September 19, 2016. Available at: https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/.

27. *See* Ash Carter, “Remarks by Secretary Carter on the Budget at the Economic Club of Washington, D.C.,” Speech, February 2, 2016. Accessed September 19, 2016. Available at: http://www.defense.gov/News/Transcripts/Transcript-View/Article/648901/remarks-by-secretary-carter-on-the-budget-at-the-economic-club-of-washington-dc.