Chechnya (& Kosovo)

Longstanding enmity between Russia and recalcitrant near abroad republics found expression in the Internet battles for narrative control during conflicts in the 1990s and early 2000s. Russia's misjudgement about the intensity of military resistance against its effort to reclaim Chechnya was mirrored in the cyber domain. Chechen loyalists repeatedly thwarted Russian strategic planners' effort to control the information environment by launching attacks against Russian state media, and re-launching or re-locating websites with content that competed with Russian portrayals of the war.[1] The Chechen insurgency and online ingenuity no doubt raised costs for Russia, but cyber operations were not pivotal because they operated as an adjunct to covert and conventional military operations. Russia judged intervention to be the most efficient way to prosecute war in Chechnya, and eventually prevailed; disinformation and disruption propagated in the cyber domain were not decisive. But Chechnya and Kosovo are significant cases in the history of Russian cyber campaigns for occurring at a time when Russia appeared to be testing a new conceptualization of cyber-enabled conflict requiring *fewer elements* of power to achieve political-security objectives, the defining feature of grey zone conflict (p 7).

The targeting of websites sympathetic to Chechnya, and defacement of NATO websites during the intervention in Kosovo, appear to fulfill a vision of contemporary conflict taking shape around the time Vladimir Putin ascended the Russian presidency. In late 1999, deputy chief of the Russian Security Council, Vladimir Vasilyev pronounced, "[i]t is clear that today a fight is going on over public opinion both inside the country and abroad, and that whoever gets to shape it, to direct it, is going to be winning in this process."[2] In 2001, while Putin defended Russia's policy in Chechnya during a special Internet interview livestreamed by the BBC his spokesman explained, "We wanted to show that we understand that the Internet is an important part of forming public opinion."[3] If the dividends of capturing public opinion match those gained from capturing territory and come at much lower cost, then it would be optimal for an initiator to advance political objectives by operating primarily in the grey zone.[4] Becoming

[1] Oliver Bullough, "Russians Wage Cyber War on Chechen Websites.," *Reuters News*, November 14, 2002, http://global.factiva.com/redir/default.aspx?P=sa&an=lba0000020021114dybe00ph2&cat=a&ep=ASE.

[2] "Broadcasting Review of 1999.," *BBC Monitoring Media*, December 14, 1999, http://global.factiva.com/redir/default.aspx?P=sa&an=bbcmm00020010901dvce002c7&cat=a&ep=ASE.

[3] Patrick E. Tyler, "A Talkative Putin Demonstrates Value of Cyberspace," *The New York Times*, March 7, 2001, sec. World, https://www.nytimes.com/2001/03/07/world/a-talkative-putin-demonstrates-value-of-cyberspace.html.

[4] Maria Snegovaya, "Putin's Information Warfare In Ukraine: Soviet Origins of Russia's Hybrid Warfare," September 2015, http://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

proficient in grey zone operations, an initiator could alter the status quo without waging war, and foreclose target state justifications for responding with conventional deterrence measures.[5]

Estonia

The familiar 2007 case from Estonia reflects a cautious Russian effort in the grey zone constrained by general NATO deterrence. The retributory cyber rioting that took place after a Soviet-era statue was relocated from the center of Tallinn to its outskirts temporarily altered the status quo in Russia's favour without eliciting punishment. All sides – belligerents, their agents, and the targets – were relatively inexperienced with cyber operations at scale in 2007. The combination of immature organizational processes for dealing with hostile cyber operations, risk of over-reaction by the recipient state, or its allies, could have led to miscalculation, and unintended escalation into the conventional warfighting domains, where NATO maintained escalation dominance.[6] These risks and the cross-domain threats arrayed against Russia likely motivated the choice to engage by limited means.

Though sometimes cast as a Russian victory, the Estonia event was highly visible, and galvanized states to begin thinking through the implications of operational cyberspace. As Western governments and alliances began hardening networks against vulnerabilities exposed by the crippling Internet traffic directed into Estonia, it appears that the space for effective ad hoc grey zone cyber operations narrowed. Policy actions and the establishment of new institutions raised the profile and resources of cyber defence capability, eliminating some of Russia's leverage over its neighbor. NATO's network resiliency built up since 2007 through a combination of technical defence and efforts to overhaul member states' defences, provide training, and deploy rapid network repair teams confers deterrent reputational effects on the Alliance. Lindsay and Gartzke (forthcoming) point out that, "skilled cyber defence, above and beyond the ability simply to detect threats, enhances deterrence by denial."[7] As a consequence, cyber operations from 2007 onward exhibit more planning; the potency of more mature cyber toolkits was proven just a year later in Georgia.

[Estonia Alternative Explanation: efficiency]

However, efficiency might also have informed the choice to enter the grey zone, as networks were relatively vulnerable to weak assaults in 2007. The fact that Estonian

[5] Herb Lin, "The Operational Doctrine of Hybrid Conflict as It Relates to Cyber Conflict - A Speculation," Lawfare, September 17, 2015, https://www.lawfareblog.com/operational-doctrine-hybrid-conflict-it-relates-cyber-conflict-speculation.

[6] Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (January 2017): 72–109, https://doi.org/10.1162/ISEC_a_00267.

[7] Kelly Greenhill and Peter Krause, eds., *COERCION: The Power to Hurt in International Politics.* (New York: Oxford University Press, 2018).

leaders lobbied for invocation of Article V of the Washington Treaty points to a counterfactual in conformity with the theoretical prediction that responding to grey zone activity motivated by efficiency risks conflict escalation.

Georgia

Deepening US and NATO interests in post-revolutionary Georgia led Russian leadership to pursue conflict short of war as an optimal strategy for altering the status quo of frozen conflicts within Georgian territory. Protections conferred by Georgia's nascent Western alliances held despite information operations designed to shape favourable international response to deployment of Russian military forces inside Georgia, and extensive grey zone activity.[8] After months of provocation, Russia seized the opportunity to intervene militarily when Georgia launched a missile strike against pro-Russia agitators inside South Ossetia. Russian troops were deployed on August 8 on grounds of protecting Russians under threat from a hostile Georgian regime,[9] which was unable to hold onto secession-oriented South Ossetia or Abkhazia, or mount an effective defense due to cyber-induced C4ISR impairment and information interdiction.[10]

The Georgian conflict is unique for having two distinct phases. Initial Russian grey zone activity was governed a logic of deterrence, but transformed into a conventional military conflict coinciding with crippling cyber disruption activity orders of magnitude larger than those seen a year earlier in Estonia. Unlike previous Russian cyber campaigns, the Georgia case also revealed evidence of advance preparation, now a common feature of Russia's more sophisticated cyber operations.[11] But some important features of the Georgia case resemble Estonia: cyber activities were self-organized and highly dispersed, suggesting involvement of informal, social, patriotic hacker, and possibly

[8] United Nations General Assembly Security Council, "Identical Letters Dated 5 May 2008 from the Permanent Representative of Georgia to the United Nations Addressed to the Secretary-General and the President of the Security Council," May 6, 2008, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2008/299.

[9] "Medvedev Vows to Protect Compatriots in South Ossetia," *Reuters*, August 8, 2008, https://www.reuters.com/article/us-georgia-ossetia-medvedev-idUSL863997220080808.

[10] Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (February 2012): 3–24, https://doi.org/10.1177/0967010611431079.

[11] John Bumgarner and Scott Borg, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008" (US Cyber Consequences Unit, August 2009), http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

criminal networks in prosecuting cyberattacks,[12] hacking kits were posted online,[13] and the conflict was internationalized in the same way seen a year before.[14]

Despite gaining territory and revealing the weakness of Georgia's Western alliances,[15] Russia subjected the campaign to systematic after action review. Two outcomes of the exercise highlight Russian grey zone priorities and capabilities developed after 2008. First, basic operational shortcomings prompted an overhaul of both the armed forces and defense industry, with a particular focus on digitization and automating command and control networks.[16] Second, frustration over the depiction of the Georgian conflict in the Western press provoked Prime Minister Putin just weeks after the Georgian ceasefire to pronounce, "the media's coverage was utterly preposterous, yet they managed to get away with it. This can be possible only in a situation where people are very persuadable, where the man in the street does not keep track of events, and eagerly accepts other's point of view."[17] The combination of enhanced technological capability and media mobilization has paid off in grey zone operations against Ukraine and the US.

[12] Jeremy Reimer, "Conflicting Accounts of Who Is behind Cyber-Attack on Estonia (Updated)," Ars Technica, June 6, 2007, https://arstechnica.com/information-technology/2007/06/conflicting-accounts-of-who-is-behind-cyber-attack-on-estonia/.

[13] F-Secure, "Threat Summaries 2011-2007," accessed October 27, 2017, https://www.f-secure.com/documents/996508/1030743/threat_summaries_2011_2007.pdf.

[14] Jose Nazario and Andre DiMino, "BTF8: An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008," October 2008, https://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf.

[15] Jesse Driscoll and Daniel Maliniak, "With Friends Like These: Brinkmanship and Chain-Ganging in Russia's Near Abroad," *Security Studies* 25, no. 4 (October 1, 2016): 585–607, https://doi.org/10.1080/09636412.2016.1220208.

[16] Keir Giles, "With Russia and Ukraine, Is All Really Quiet on the Cyber Front?," Ars Technica, March 11, 2014, https://arstechnica.com/tech-policy/2014/03/with-russia-and-ukraine-is-all-really-quiet-on-the-cyber-front/.

[17] Timothy L. Thomas, "The Bear Went Through the Mountain: Russia Appraises Its Five-Day War in South Ossetia," *The Journal of Slavic Military Studies* 22, no. 1 (March 4, 2009): 31–67, https://doi.org/10.1080/13518040802695241.