Cyberwar Case Study: Georgia 2008

by David Hollis

Cyberwar Case Study: Georgia 2008

The Russian-Georgian War in August of 2008 represented a long history of geostrategic conflict between the two nations and was based on many complex factors: geopolitical, legal, cultural, and economic. The 1992 South Ossetia War and the 1993 Abkhazian War resulted in the loss of the regions from Georgia to internationally unrecognized, pro-Russian local governments. Tensions had been building in the region for several years prior to the initiation of conflict in August 2008. The war officially started on 7 August 2008 after several weeks of growing arguments over the future of the South Ossetian territory. Georgian troops initiated a military attack against South Ossetia and began a massive shelling of the town of Tskhinvali in response to alleged Russian provocation. Russia deployed additional combat troops to South Ossetia and retaliated with bombing raids into Georgian territory. Russia deployed naval forces to formally blockade Georgia and landed naval infantry (marines) on Abkhaz coast (near Georgia). The decisive ground combat operation of the campaign resulted in mechanized Russian military and Ossetian militia forces defeating the more lightly armed Georgian military forces in the only large-scale major ground combat of the war (battle for the town of Tskhinvali). Georgian tactical military defeat at the battle of Tskhinvali, operational defeat via Russian uncontested invasion of the western part of Georgia, unchallenged naval blockade of Georgia, and Georgian difficulty getting their media message out to the world, led to Georgia's strategic defeat in the war. The conflict forced approximately 25,000 Georgian residents to flee from ground combat as refugees into internal displacement. The two countries signed a ceasefire agreement a week later but tensions remain high to this day. Russia has failed to implement some of the terms of the ceasefire agreement, resulting in further loss of Georgian territory to Russian occupation.

As wars historically go, it wasn't very big, did not involve vast amounts of military forces, nor did it last long. One might argue that it was more of a typical battle or campaign framed in an on-going long term geopolitical cold war between the combatants, a cold war punctuated with occasional outbreaks of small to large scale violence. On the surface, it represents one of many cold wars (with periodic renewals of formal national-level military conflict) fought every day on the "near abroad" of the Russian periphery. A conflict which may not end for a very, very long time. But while much of that is true, a deeper analysis of the cyberspace domain operations conducted by both sides in this conflict indicate that image is illusory and incomplete. The Russian-Georgian war was quite historic and precedent setting for several reasons.

Download The Full Article: Cyberwar Case Study: Georgia 2008
David M. Hollis is a Senior Policy Analyst with the Office of the Undersecretary of Defense for Intelligence (OUSD(I)). He has spent a total of four years on the OSD staff with three as Cyberspace Security Division Chief for the ASD NII/DoD CIO’s office prior to working at OUSD(I). He is also a drilling USAR officer with US Cyberspace Command (USCYBERCOM); currently the senior USAR officer responsible for 25 USAR personnel supporting a wide range of USCYBERCOM J-codes and projects, and was previously a Joint Plans Officer with the USCYBERCOM J5. He was with the Army’s 1st Information Operations Command from 2000 to 2006 as Red Team Chief, S2/Chief of the Army’s CyberIntelligence Center, and Senior Operations Planner. He has previously published cyberwarfare articles in the Joint Forces Quarterly and Armed Forces Journal magazines.

About the Author

David M. Hollis

David M. Hollis is a GG-15 Senior Policy Analyst/Planner with the Office of the Undersecretary of Defense for Intelligence’s (USD(I)) Cyberspace, Warfighter Integration, and Strategic Engagement Division (CWISE). Prior to this position, he was the Chief of the Cyberspace Security Division for the Office of the Assistant Secretary of Defense for Network & Information Integration /DoD Chief Information Officer (ASD NII/DoD CIO). Lieutenant Colonel David M. Hollis, (USAR, MI) is also currently serving as the Senior USAR officer & USAR Element OIC for the Joint USCYBERCOM. He was previously a drilling Joint Plans Officer with the USSTRATCOM Joint Functional Component Command for Network Warfare (JFCC-NW) J5. Prior to his current USAR assignment, LTC Hollis was assigned/mobilized with the Army 1st Information Operations Command as Senior Operations Planner, S2/Chief of the Army CyberIntelligence Center, and Army Red Team Chief. Prior to 1st IOC, he was the Senior VP at Cryptek Secure Communications and Director of Federal Operations at Secure Computing Corporation. His background encompasses almost 30 years of government, military and private sector/commercial cyberspace experience starting in 1982 as a GS-4 communications engineering technician with the Naval Electronic Systems Command. He was commissioned through ROTC at Old Dominion University in 1985 with an undergraduate degree in engineering and earned an MBA from Strayer University in 1998. He is a graduate of the Army’s Command and General Staff College and the Joint Forces Staff College’s Advanced Joint Professional Military Education. He has previously written four articles on cyberspace domain operations for Joint Forces Quarterly, Armed Forces Journal, and Small Wars Journal; and one article for a Civil War magazine/blog on the strategic effect of railroads during the Civil War.

Available online at: http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

Links:

Copyright © 2015, Small Wars Foundation.
Select uses allowed by Creative Commons BY-NC-SA 3.0 license per our Terms of Use.
Please help us support the Small Wars Community.