

# Invited Talk: Russian Cyber Warfare and the Magic of Misdirection

Jeffrey Carr, Founder & Principal  
*Greylogic*

**T**HE way that the Kremlin conducts its cyber warfare operations is akin to the way a magician fools his audience - through the use of misdirection. When Lee Siegel was researching his book *Net of Magic* in India, he noted in his field notes a frequent exchange that occurred with the locals: "I'm writing a book on magic," I explain, and I'm asked, "Real magic?" By real magic people mean miracles, thaumaturgical acts, and supernatural powers. "No," I answer: "Conjuring tricks, not real magic." Real magic, in other words, refers to the magic that is not real, while the magic that is real, that can actually be done, is not real magic." (Siegel, *Net of Magic*, Univ of Chicago Press, 1991, p. 425)

This upside-down illustration of what is perceived as 'real' and what isn't, lays the groundwork for one of the most important principles in magic and military operations – the art of misdirection. It also happens to be the key to the Russian Federation's strategy in conducting Information warfare, otherwise known as International Information Security. We know it as 'Cyber Warfare'. This presentation will include a survey of Russian military doctrine (A. Burutin, P. Koayesov, I. N. Dylevsky, S. A. Komov, S. V. Korotkov, S. N. Rodionov, and A. V. Fedorov) related to information warfare including a Russian Colonel's recounting of the Georgian cyber campaign of 2008. It will particularly examine the careful use of words as a tool of misdirection and compare it with the same technique used in "The Tuned Deck" as described in Daniel Dennett's paper "The Magic of Consciousness" (*Journal of Cultural and Evolutionary Psychology*, 1(2003)1, 7.19).

This presentation will also explore the misdirection of a free Russian Internet with the reality of an aggressive anti-Kremlin counter-research operation whose remit from Moscow is to "Ensure the domination of pro-Kremlin view on the Internet" and how that policy is enforced through the enlistment of Russian youth organizations; the same organization that was involved in the Estonia and Georgia cyber conflicts. Finally, this presentation will detail how one anti-Georgia Web forum was deliberately designed to obfuscate GRU/FSB involvement through the use of blacklisted hosts and Spam servers. The success of Russia's use of misdirection continues today as many Western security experts struggle to attribute the work of Russian hackers back to the Kremlin.