computer "worm" designed to disrupt the Iranian nuclear program, Deibert lays out the disturbing implications of this resort to destructive force in cyberspace. Its real significance Deibert notes lies "in the threshold that it crossed: major governments taking at least implicit credit for a cyber weapon that sabotaged a critical infrastructure facility through computer coding". In this domain, where potential weaponry is cheap and a countervailing normative structure largely absent, the risks of proliferation and escalation of offensive action are real and frightening.

Having alarmed his readers with disturbing portraits of the dark forces in cyberspace, what does Deibert offer by way of prescriptions for corrective action? In a concluding chapter Deibert sets out two core concepts which he suggests can reconcile the security versus openness dichotomy. The first is "distributed security" with origins in the "checks and balances" systems developed by America's founding fathers. Distributed security is concerned with "building structures that rein in and tie down political power, both domestically and internationally, as a way to secure rights and freedoms". Deibert advocates the development of oversight and accountability mechanisms to ensure that national security programs are consistent with legal and human rights standards. The second concept is that of "stewardship" which Deibert sees as particularly relevant to the human-created environment of cyberspace. Deibert rejects the notion of a single global body taking on the stewardship role and favours a decentralized network in which the scientists and engineers who have developed and maintained cyberspace should play a central role. While Deibert offers no precise blueprint for the construction of such a decentralized governance arrangement for cyberspace, he clearly sees an inclusive approach as vital. He also views a civil society-animated stewardship as necessary to "moderate the dangerously escalating exercise of state power in cyberspace by defining limits and setting thresholds of accountability and mutual restraint". In both the domestic and foreign spheres, Deibert argues it is urgent for those who support liberal democratic values "to articulate a compelling counter-narrative to reflexive state and corporate control over cyberspace". In *Black Code*, Ron Deibert has made a major contribution to the development of such a narrative.

***Paul Meyer** retired in 2010 after a 35 year career in Canada's Foreign Service. He is currently a Fellow in International Security at Simon Fraser University's Centre for Dialogue and a Senior Fellow at the Simons Foundation in Vancouver.*

The Dogs Are Eating Them Now, Our War in Afghanistan

reviewed by Stuart Hughes

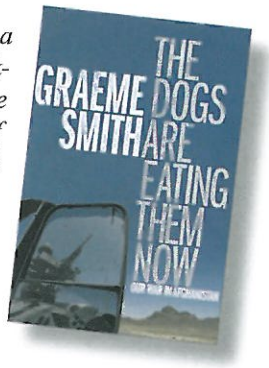
THE DOGS ARE EATING THEM NOW, OUR WAR IN AFGHANISTAN
by Graeme Smith, Alfred A. Knopf Canada, 2013, 299 pp., $32.00 CDN.

At a recent gathering at CIPS (the Centre for International Policy Studies of the University of Ottawa), Graeme Smith spoke candidly about his years from 2006 to 2009 as the correspondent for the *Globe and Mail* in Kandahar. Self-deprecating, he emphasized that he was still a very young journalist during his assignment in Afghanistan and hadn't lingered over-long in university before it. He also spoke somewhat apologetically about the book, almost dismissing it as a "300 page rant". The title, *The Dogs Are Eating Them Now, Our War in Afghanistan*, is a grim reference to the fate of bodies left in the field.

Smith's modesty is disarming, but don't be fooled. The book is not about an innocent coming of age, it is about a thoroughly professional reporter and guarded idealist become an often chagrined and exasperated realist. Neither foolhardy nor risk averse, he set about relentlessly collecting facts on the ground – increasingly dangerous work in Afghanistan and neighbouring Pakistan. The keen observation and pointed questions that are the journalist's métier soon had him seeing things as they are, and not as western politicians and their spin doctors would have us see them. Some of them will not like this account, perhaps a few of our own diplomats included. However, he never quite abandons his idealism and concludes his narrative on a hopeful note that Afghanistan's government may prove more resilient than we suppose.

From the diplomat's perspective, there is much to like in Smith's book. He has a gift for capturing the subtleties of situations many of us may have witnessed ourselves:

"The war attracted young professionals who saw themselves in a heroic role, saving locals from misery, or fighting the evil darkness of terrorism, or perhaps both at the same time. Somehow those glamorous pursuits also required lots of alcohol...



There was often a grimness to the drinking, a deliberate grinding down of consciousness, but occasionally women would show up in something shimmery, or sparkly, or wearing a tiara. This added a frisson to the dancing, and gave momentum to the evenings beyond the need to blur awareness. By the end of the night you could see the disappointment on the faces of the people who realized they could not drink themselves out of Afghanistan."

Smith does not simply recap his many articles hoping that the sum would be greater than it parts. As an eyewitness and non-combatant participant, he documents the events and times that gave rise to his reporting and places the whole in a broad and thoughtful context. Underlying questions came sharply into focus as security conditions worsened, the pervasive climate

Black Code: Inside the Battle for Cyberspace

reviewed by Paul Meyer

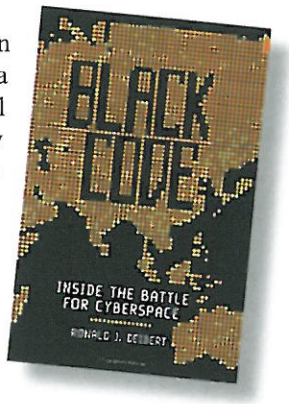
BLACK CODE: INSIDE THE BATTLE FOR CYBERSPACE by Ronald J. Deibert, McClelland & Stewart Random House of Canada, 2013, 298 pp., $32.99 CDN.

The term "cyberspace" was coined by the Vancouver science-fiction writer William Gibson. In his 1984 novel *Neuromancer*, he defined it as "a consensual hallucination experienced daily by billions..." This prescient metaphor has become a household term in a world increasingly engaged in an on-line existence. This omnipresent cyber world is not without its dark forces however and these are well illuminated in a timely and insightful work by Ron Deibert, Director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto. As he explains in the preface Citizen Lab was born out of a desire to study cyberspace from an international security perspective while working to sustain it as an open and secure commons for all. This led to an unorthodox combination of technical investigation, field research and social science analysis being brought to bear under academic auspices with a mission to "watch the watchers" and report its findings to the public. What Deibert and his colleagues at the Lab uncovered was disturbing and its retelling, in a refreshing and largely jargon-free style, constitutes the core of the book.

In order to properly appreciate the dangers to cyberspace one has to have an understanding of its scope and importance. Deibert sets out, often via anecdotes derived from actual investigations undertaken by Citizen Lab, a series of facts that serve to put the current threats to cyberspace freedoms into context. It is estimated that there are over 10 billion devices connected to the Internet. Once dominated by Western actors, by 2012 two-thirds of Internet users were outside of North America and Europe, with over one-quarter residing in China. The volume of the metadata being generated in cyberspace is mind-blowing. Deibert cites IBM research which concluded that humanity produced from the dawn of time to the year 2003 some five exabytes of data (one exabyte = a billion gigabytes) and estimated that by 2013 an equivalent amount will be produced every ten minutes. This immense data store and its exploitation is an underlying theme of the book. Deibert outlines the political economy of cyberspace that is based on the collecting, analysis and dissemination of what he jokingly refers to as "our digital droppings". The fact that this mining of metadata occurs essentially outside of our awareness and with the dubious authorization of "I agree" activation based on lengthy and obtuse text is one of the realities Deibert expounds upon. He notes that this business model creates significant vulnerabilities for the consumer with respect to privacy. Moreover, as the same techniques for amassing and exploiting this data are employed by official as well as commercial actors, these processes can result in abuse of civil rights.

The chief threats to cyberspace and its users, enumerated by Deibert, originate in the corporate, criminal and state realms. The tendencies of corporate players to increase the data collected from users and to erode privacy limits is decried. Deibert at one point compares Facebook to a giant python that "captures, swallows and slowly digests its users". Corporate transgressions pale, however, in comparison with the actions of criminal gangs. Deibert describes how the Citizen Lab team exposed a cyber crime syndicate called Koobface that operated out of St. Petersburg, Russia. This gang had control of some 800,000 computers worldwide having compromised them through a variety of on-line tricks and used this "botnet" to amass millions through taking advantage of legitimate "pay per click" and "pay per install" schemes. With a solid dossier in hand as to Koobface illicit actions Deibert tried to interest the RCMP in the affair, but to no avail as the problems of jurisdiction, differing legal codes and limited capacity for international cooperation rendered any prosecution of the culprits extremely unlikely.

The most ominous of the threats that *Black Code* discusses is that originating with state authorities. This in turn reflects the "securitization of cyberspace" a concept that Deibert explains means: "the slow transformation of an issue into a matter of national security, with new policies and controls attached." It follows therefore that authoritarian regimes, which consider any dissent against the existing order a threat to national security, are quick to employ cyber surveillance tools to identify and repress activists. Deibert laments the fact that the Internet has not always proven to be an effective counter to authoritarian regimes and some of these have successfully employed sophisticated control techniques to neutralize opposition groups and instill a climate of fear and self-censorship. Deibert effectively illustrates these actions, drawing from Citizen Lab studies of Chinese cyber espionage campaigns directed at Tibetan and other dissident groups as well as foreign governmental entities. But "securitization" is not only a process that favours authoritarian regimes, it also provides a justification for those in democratic states who support extensive and intrusive surveillance of individuals in the interests of "national security". As Deibert notes: "Securitization opens the door to clandestine arrangements, overclassification, and lack of accountability". Although published prior to the revelations of Edward Snowden regarding the massive collection programs of the National Security Agency, Deibert has identified the inherent risks to open societies when their "protectors" assume secret and far-reaching powers.



If states exploit cyberspace for surveillance of their own and foreign citizens, they also increasingly have the capacity to deploy offensive cyber weapons and conduct cyber warfare. Although self-restraint has been practiced by the major powers there is clearly a danger that cyberspace could readily be turned into another battleground for warring states to the detriment of all. In a chapter devoted to the Stuxnet cyber weapon, a sophisticated