CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES | Middle East Program

November 14, 2012

SUMMARY - GULF ROUNDTABLE SERIES

PARTICIPATING SCHOLARS

James Andrew Lewis is a senior fellow and director of the Technology and Public Policy Program at CSIS. Before joining CSIS, he worked at the Departments of State and Commerce. Lewis's recent work on cybersecurity includes the groundbreaking report "Cybersecurity for the 44th Presidency." Other recent publications include "Escape from Iraq and American Decline" (CSIS, 2012) and "Cybersecurity After Two Years" (CSIS, 2011). His current research examines the political effect of the Internet, competition, and innovation. Lewis appears frequently in the media and has testified numerous times before Congress. He received a Ph.D. from the University of Chicago. ■

Cyber Conflict in the Gulf

With Iran's heightened activities, the Gulf region is at the center of global developments in cyber conflict. Jim Lewis, director and senior fellow of CSIS's Technology and Public Policy Program, discussed evolving cyber capabilities in the Gulf, the U.S. and allied responses to these threats, and emerging fault lines in global cyber conflict. Lewis delivered his remarks at a Gulf Roundtable at CSIS on November 14, 2012.

Iran has been aggressively developing its offensive cyber capabilities over the last five years, Lewis said. It has developed a robust institutional framework for thinking about these issues, seeming to take as its strategic model China's approach of building asymmetric international advantages while controlling internal dissent. Iran's High Council of Cyber Space reportedly created a "cyber army" of civilians that can carry out actions at the behest of the state without directly implicating Iranian leadership. There is also speculation that the Iranian Revolutionary Guard is working to develop offensive capabilities. Last August, a computer virus linked to Iran named Shamoon wiped the data from 30,000 computers belonging to the Saudi national oil company, Aramco. While Shamoon was not technically sophisticated, it was deployed in an innovative way and caused widespread damage.

Attacks such as Shamoon have the potential to affect both public and private sector networks. The Shamoon virus was seemingly a test of Iranian capabilities aimed at a "safe" target. Banks in Lebanon and around the region have also been targets of virus attacks. Some private companies are eager to launch their own cyber attacks in retaliation, a step which Lewis argued would be destabilizing.

Iran also targets its cyber capabilities at internal dissent. For example, Iran has crafted extensive internal Internet monitoring capabilities, even developing a "spoof" Gmail website where individuals who thought they were logged on to their Gmail accounts were actually sending information to the Iranian government. Iran is working toward developing its own national search engine to rival Google as well as a closed, independent Internet system that would isolate high-value Iranian networks from the outside world. Lewis suggested that where Iran excels is not in the sophistication of

THE GULF ROUNDTABLE SERIES

The CSIS Middle East Program launched the Gulf Roundtable in April 2007 to examine the strategic importance of a broad range of social, political, and economic trends in the Gulf region and to identify opportunities for constructive U.S. engagement. The roundtable defines the Gulf as the United Arab Emirates, Saudi Arabia, Oman, Qatar, Bahrain, Kuwait, Iraq, and Iran. The roundtable convenes monthly, assembling a diverse group of regional experts, policymakers, academics, and business leaders seeking to build a greater understanding of the complexities of the region. Topics for discussion include the role of Islamist movements in politics, the war on terror, democratization and the limits of civil society, the strategic importance of Gulf energy, media trends, trade liberalization, and prospects for greater regional integration. The Gulf Roundtable series is made possible in part through the generous support of the Embassy of the United Arab Emirates.■

its technology, but in the innovative ways that it deploys rather basic tools.

Lewis argued that the Iranians are not the only ones active in the cyber domain in the Gulf. For example, China has a keen economic interest in energy markets, and it has allegedly conducted cyber-espionage campaigns against energy companies in the Gulf. Malware designed to collect information covertly has been found repeatedly on oil and gas company computers, originating from servers with IP addresses traced back to Beijing.

Israel also has a robust cyber warfare capability, and analysts have linked it to two viruses that were reportedly developed in cooperation with the United States. The Stuxnet virus attacked specific centrifuges that Iran was using for uranium enrichment, and the Flame virus collected massive amounts of information about Iranian computer networks.

More globally, cyber attacks complicate a security landscape that is accustomed to armed forces and the hardware that accompanies them. It is difficult to detect the existence of programs designed to infiltrate networks, collect surveillance, or cause destruction, let alone uncover who created them. Attacks have allegedly originated from China, Russia, Iran, Israel, and the United States, although governments deny knowledge of or responsibility for them. For example, Lewis discussed September's distributed denial of service (DDOS) attacks on major U.S. banks, five of which have experienced day-long shut downs that rendered them unreachable for customers. The attacks resembled protests more than assaults, but their development and implementation likely involved Iran. Cyber conflict poses other fundamental challenges. Lewis stressed that we still do not understand how actions in cyber space parallel those in the physical world, which is the traditional domain of conflict. We do not understand how such conflicts might escalate, or how they might affect diplomacy.

Another challenge is the possibility that some attacks that are intended to be targeted are in fact indiscriminate. Stuxnet, for example, was designed to limit collateral damage (many systems were infected but only one was damaged), but other attackers may not be so careful.

While state-sponsored cyber espionage is increasingly common, there has also been an increase in cyber attacks by non-state actors targeting banks for personal financial gain. Costly "cyber bank robberies" have become commonplace. In June 2012, a cyber attack stole $75 million from 10 banks across North and South America, and 60 million euros were stolen from over 60 banks across the world in the largest cyber bank robbery in history. Many attacks go unreported because banks prefer to absorb the losses rather than admit they were the victim of an attack.

A comprehensive, international cyber security framework is still likely years away. International steps to stabilize cyber activity tend to be piecemeal, with a focus on achieving agreement on norms and advancing confidence-building measures but not on politically sensitive enforcement mechanisms. Although cyber capabilities are developing quickly and cyber attacks are increasingly common, our understanding of them and our framework for defending against them has been considerably slower to develop.

U.S. officials are increasingly attuned to the threat of cyber warfare. An October speech by Secretary of Defense Leon Panetta made public previously classified examples of cyber warfare and linked them to Iran. While it is difficult for cyber attacks to cause death directly, Panetta expressed concern that programs such as Shamoon could cause casualties if released against targets like hospitals. He outlined a clear chain of command for U.S. cyber defense efforts and a willingness to preemptively block attacks—presumably intending to send deterring signals to Iranian decision-makers who might escalate conflict. ■

The Gulf Roundtable Summary is an electronic newsletter produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions; accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s). © 2012 by the Center for Strategic and International Studies.

The CSIS Middle East Program

Jon B. Alterman
Director and Zbigniew Brzezinski Chair in Global Security and Geostrategy

Haim Malka
Deputy Director and Senior Fellow

Carolyn Barnett
Research Fellow

Rebecka Shirazi
Program Coordinator/Research Associate

Daniel Brunner
Jennifer Cunningham
Adel El-Adawy
Ramzi Habayeb
Interns