WebMemo

Published by The Heritage Foundation

No. 2022
August 13, 2008

When Electrons Attack: Cyber-Strikes on Georgia a Wake-Up Call for Congress

James Jay Carafano, Ph.D.

Bombs and bullets are not the only things flying around in the Russia-Georgia war that broke out over the weekend. There is a flurry of battling electrons as well. According to a news story first reported in *The Telegraph*, the Georgian Ministry of Foreign Affairs claimed that a "cyberwarfare campaign by Russia is seriously disrupting many Georgian Web sites, including that of the Ministry of Foreign Affairs." How these contributed to the country's crushing defeat and the extent of deliberate Russian "cyber-warfare" remains to be determined. This incident, however, is the latest reminder that Washington needs to get serious about systematically developing the cyber-strategic leaders in the public and private sector who are skilled in dealing with the complex issues of deliberate attacks in cyberspace.

War Online. It has been reported in *The New York Times* and elsewhere that weeks before the Russian invasion, "denial of service attacks" (where Web sites are flooded with useless data) and other malicious acts were targeted against Georgian government computer sites. Some speculate these were a prelude to a preplanned assault on Georgian territory. In addition, it is clear that government and business Web sites were intentionally disrupted during the invasion. How much has been directed by the Russian government, individual hackers, and Russian criminal elements (some with alleged ties to Russian government agencies) remains to be sorted out.

That is not the first time that Russia has been accused of cyberwarfare. A widely publicized cyberassault against Estonia in 2007 increased suspicion that Russia is using online malicious activity as a tool of national policy. The assault disrupted public and private Estonian information networks with massive denial-of-service attacks. The attacks targeted the Web sites of Estonian banks, telecommunication companies, media outlets, and government agencies. Estonia's defense minister described the attacks as "a national security situation.… It can effectively be compared to when your ports are shut to the sea." The Estonian and Georgian attacks testify to the disruptive power of a coordinated cyber offensive.

Russia is not the only one threatening other countries. And many countries, including America, are their targets. U.S. government information systems are attacked every day from sources within the country and around the world. China uses "cyberspying" as a matter of course, and America is one of their prime targets. Some of these intrusions have been extremely serious, compromising security and costing millions of dollars. Penetration of computer networks at the National Defense University proved so pervasive that the university was forced to take the entire computer network offline and install new information system defenses.

This paper, in its entirety, can be found at:
www.heritage.org/Research/NationalSecurity/wm2022.cfm

Produced by the Douglas and Sarah Allison
Center for Foreign Policy Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

These attacks come from states, criminal networks, "hacktivists" (online political activists), and other malicious actors. In addition, bad people exploit the freedom of the Internet—terrorists included. They go online to gather intelligence, raise money, share tradecraft in chat rooms, and coordinate propaganda messages.

Time for Leadership. The lesson for the United States is to take the challenge of cyber threats seriously. The initiatives that will likely best serve the United States and its international partners in the cyber conflicts of the 21st century are those derived from private sector experience, emerging military and intelligence capabilities for conducting information warfare, and law enforcement measures for combating cybercrime.

Cyberwar is like real war, a competition of action and reaction between two thinking, determined enemies. Technology, which evolves every day, is *the* "wild card" that keeps changing the nature of the battlefield. Like war on an escalator, there is no standing still. Thus, there is no quick fix or "silver bullet" solution that will make America safe. What is called for is dynamic, informed national leadership in the public and private sector that understands how to compete in the cyber-strategic environment. America needs cyber-strategic leaders that know how to:

- **Ensure adoption of best practices.** Ensuring that these are refreshed and applied should be a priority.
- **Know how to employ risk-based approaches.** All information programs must include assessments of criticality, threat, and vulnerability as well as measures to efficiently and effectively reduce risks.
- **Foster teamwork.** Cybersecurity is a national responsibility requiring international cooperation. The United States must maintain effective bilateral and multinational partnerships to combat cyber threats.
- **Exploit emergent private sector capabilities.** Government and industry must become more agile consumers of cutting-edge commercial capabilities.
- **Manage cyber systems.** Most programs underperform because, due to inattentive senior leadership, they lack clear requirements and hold unrealistic projections of the resources required to implement those requirements.
- **Know how to protect, defend, and respond to cyber threats.** Targets of malicious acts by either state or non-state threats should respond by using the full range of military, intelligence, law enforcement, diplomatic, and economic means.

What is needed, however, is not massive reorganization, massive government bureaucracy, massive infusions of government cash, or massive intrusions into the marketplace and the lives of Americans. What is needed is long-term commitment and sound initiatives based on better and faster acquisition of commercial services; better and smarter management of military, intelligence, and information technology programs; and better and sustained professional development of federal, state, local, and private-sector leaders.

Congress can help develop the leaders America needs to respond to cyber threats. In part this can be accomplished by establishing effective interagency programs for professional development, particularly in regard to cyber skills. Much of this can be accomplished by modest initiatives that require federal interagency education, assignment, and accreditation programs, one that in particular addresses the preparing cyber-strategic leaders. This framework should include:

- **Education.** A program of education, assignment, and accreditation that cuts across all levels of government and the private sector with national and homeland security responsibilities (especially cyber security) has to start with professional schools specifically designed to teach interagency skills. No suitable institutions exist in Washington, academia, or elsewhere. The government will have to establish them.
- **Assignment.** Qualification will also require interagency assignments in which individuals can practice and hone their skills. These assignments should be at the "operational" level where leaders learn how to make things happen, not just set policies. Identifying the right organizations and

assignments and ensuring that they are filled by promising leaders should be a priority.

- **Accreditation.** Accreditation and congressional involvement are crucial to ensuring that programs are successful and sustainable. Before leaders are selected for critical (non-politically appointed) positions in national and homeland security, they should be accredited by a board of professionals in accordance with broad guidelines established by Congress.

Critical components of good governance, such as establishing long-term professional programs for developing cyber-strategic leaders, are often shunted aside as important but not pressing—something to be done later. But later never comes. The latest cyberwar should serve as a wake-up call that this is unacceptable for critical national security activities such as cyber-strategic leadership that require building interagency competencies that are not broadly extant in government.

—James Jay Carafano, Ph.D., is Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation.