AppSec Asia Conference 2009
November 17, 2009

On State and Non-State Actors in Global Cyber Threatscape

Presented by Jeffrey Carr
CEO, GreyLogic, Inc. | Principal Investigator, Project Grey Goose

jeffreyc@greylogic.us | 360 437-7620

Jeff Carr presenting "*Russian Cyber Warfare Strategy and the Art of Misdirection*" at the NATO CCDCOE Conference on Cyber Warfare, Tallinn, Estonia July 17, 2009

Bio:

Jeff Carr is the CEO of GreyLogic, Inc., the Founder and Principal Investigator of Project Grey Goose, and the author of "Inside Cyber Warfare" (O'Reilly Media, 2010).

Mr. Carr has provided briefings on Russian cyber warfare strategy and the strategic risks and advantages of social networks for Moscow and Washington DC to various agencies within the U.S. Intelligence Community.

Invited speaker:

- Palantir Government Conference (April, 09)
- ASIA 09 / NYS Conference on Cyber Security (May, 09)
- NATO CCDCOE Conference on Cyber Warfare (June, 09)
- Defense Intelligence Agency (Analytic Speaker Series July, 09)
- Open Source Center Workshop on the Russian Internet (Sep, 09)
- IC Agency event focusing on Social Network threats (Nov, 09)

Attribution Analysis

(1) Technical analysis of the attack

(2) Social network analysis

(3) Geo-political analysis

(4) Military doctrine

(5) Military and civilian research labs

Alexandr Burutin

(Deputy Chief of the General Staff)

"Information weapons ... do not require specialized manufacturing facilities and a complex infrastructure. A small group or even one expert can develop and carry out an act of destruction while not having to physically cross borders and expose human lives to risk."

- Speech, Info-Forum 10, February 2008

Vladislav Surkov

(First Deputy Chief of Staff to the President of Russia)

"August 2008 was the starting point of the virtual reality of conflicts and the moment of recognition of the need to wage war in the information field too."

- "Information Warfare Chronicles" (Yevropa, 2009)

RF Military Policy in the Area of IO

"The target of a cyber attack, while in the process of repelling it, will be unable to qualify what is going on as a criminal, terrorist or military-political act. The more so that sources of cyber attacks can be easily given a legend as criminal or terrorist actions."

- S.A. Komov, et al, Moscow Military Thought, 31 MAR 07

The RF's 3 Tier Model of Information Warfare (aka Cyber Warfare)

First Tier - Kremlin Leadership and the Security Services

Second Tier - Russian Youth Organizations

Third Tier - Hacktivists

Internet as Attack Platform

Strategic Principles for Defeating a Technologically Superior Adversary

- Avoid direct confrontation in force-on-force battle.
- Seize the initiative early.
- Use the element of surprise.
- Make a preemptive strike.

Source: Lu Linzhi, “Preemptive Strikes Crucial in Limited High-Tech Wars,” Jiefangjun Bao, February 14, 1996, p. 6. In Foreign Broadcast Information Service as “Preemptive Strikes Endorsed for Limited High-Tech War,” February 14, 1996

China's Information Warfare Strategy

"In the final analysis, information warfare is conducted by people. One aspect is to cultivate talent in information science and technology. The development and resolution of information warfare can be predicted to a great degree in the laboratory.
Information science and technology talent are the forerunners of science and technology research."

From **THE CHALLENGE OF INFORMATION WARFARE (1995) by** *Major General Wang Pufeng*

Security Vulnerabilities and Research Labs

NSFC funds research on U.S. power grid vulnerabilities

Two researchers from the People's Republic of China address the question of how best to create a cascading failure in the Western U.S. electrical power grid in their paper "Cascade-based Attack Vulnerability on the U.S. power grid" published in the journal Safety Science.

In 2006, new funding guidelines were established under the auspices of the National Guideline on Medium- and Long-Term Program for Science and Technology Development (2006-2020) .

One of the tenets of that program was for China to establish a new mechanism to coordinate the military and civilian basic research and integrate the research and development forces for high technology.

Case Study: Intel and Scientific Technical Center (STC) Atlas

Since 2002 Intel Corporation has sponsored a laboratory on wireless technology at Nizhny Novgorod State University (NNGU). The laboratory, located in the Department of Radiophysics, benefits from NNGU's decades long experience with Russia's defense industry, especially the radar and air defense sector.

According to BusinessWeek, the lab was working on security software for high-speed wireless applications.

The laboratory's activity is overseen by a guidance board that includes Leonid Yurevich Rotkov, the head of the Center for Security of Information Systems and Telecommunications Facilities at NNGU and a security consultant to the Federal Security Service (FSB).

Until around 2008, the Center's website stated that it was sponsored by the Federal Security Service (FSB). This statement has been removed. However, the faculty listing for the Center includes one individual who is also an employee of the Nizhny Novgorod Branch of Scientific Technical Center (STC) Atlas. STC Atlas was previously directly subordinate to the FSB, however, it is now a Federal State Unitary Enterprise (government owned) research institute that still works on IT security. The Nizhny Novgorod branch is one of four major STC Atlas research facilities. STC Atlas is currently certified by FSB for work on security issues including cryptology and "special studies."

Research Scientists are more likely to be targeted than Executives

- Research scientists frequently collaborate with colleagues from other States, even States with opposing interests.
- Commitment to research is paramount. Everything else is subordinate, including security.
- Research culture is traditionally open and embracing.

Related Source:

Higher Education Contribution to the National Strategy to Secure Cyberspace

Thank you

GreyLogic provides a weekly intelligence briefing on the global cyber threatscape:

IntelFusion FLASH Traffic

Contact information for Jeffrey Carr:

E-mail: greylogic.carr@gmail.com
Website: greylogic.us
Blog: intelfusion.net