

FW: Preliminary Lessons and Thoughts

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2001-09/0040.html>

From: Russ (Russ.Cooper@RC.ON.CA)

Date: 09/21/01

Message-ID: <E9A01F52DC939448BBDE44ED2E1C468F1F1658@muskie.rc.on.ca>

Date: Fri, 21 Sep 2001 16:27:40 -0400

From: Russ <Russ.Cooper@RC.ON.CA>

Subject: FW: Preliminary Lessons and Thoughts

To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

An insightful message I received from my good friend Bill Murray. Without inferring he's aged, he's been around forever and his experience and observations are well worth considering by anyone who thinks they know security.

From: William Hugh Murray [<mailto:whmurray@sprynet.com>]

Sent: Friday, September 21, 2001 10:42 AM

Subject: Preliminary Lessons and Thoughts

Preliminary lessons:

We have an incredibly determined adversary. He is willing to lay down his life in his cause. While his resources are adequate to his plan, they are not unlimited, not those of a nation state. He can be expected to hit very hard but sparsely.

His modus operandi, not to say his objective, is to sow fear, uncertainty, and doubt.

Our adversary is an uncommon criminal, not a nation state. He may well have been armed and trained by nation states, including us, but has no loyalty to such states. He does not fear retaliation; he leaves behind no hostages to fortune or war. Indeed, he intends to provoke his victims into irrational and self-destructive behavior.

Traditional intelligence gathering and analysis techniques, e.g., SIGINT, Echelon, spies, used against nation states, will not work against him. He is far more likely to be vulnerable to those techniques, e.g., paid informants and large public rewards, used against common criminals.

When we respond by inefficient security, our adversary wins. For example, if we cripple our air travel industry with expensive, if ineffective, security measures, he wins. Note that in the current situation we are responding by tightening security over means, i.e., air transport, rather than targets, i.e., concentrations of people.

The network is not likely to be high on his list of targets. It is far more likely to be high on his list of means. He will use it to communicate, cooperate, and coordinate. He may use it to attack such