Webinar Questions and Answers

Targeting U.S. Technologies:

A Trend Analysis of Cleared Industry Reporting

Webinar guests submitted several questions before and during the September 12th Targeting U.S. Technologies session. The following responses are provided by the Center for Development of Security Excellence (CDSE).

Question: Can you give examples of electronics that are being targeted?

Answer: In FY2012 commonly targeted electronics included:

-Radiation hardened electronics (space qualified)

-Traveling wave tubes

-Monolithic microwave integrated circuits

-Communications equipment

-Electronic warfare and SIGINT equipment - cognitive radios, digital receivers and decoders, demodulators, signal processing components, and direction finding antenna.

Question: Can we have the speaker tell us the name of the report he is referring to regarding the STATS of missile technology?

Answer: The missile technology discussion is from the 2013 Targeting U.S. Technologies report available at http://www.dss.mil/

Question: In this 2013 report SCRs were 657, what were they in 2012?

Answer: In fiscal year 2012 other government agencies initiated 657 investigations or operations based on DSS SCRs. Not every SCR reveals sufficient information to initiate an investigation or operation and the number of investigations is limited by availability of resources. DSS analyzes all SCRs in the process of compiling the statistics for the annual Trends report. In FY 2012 DSS received over 25,000 SCRs from cleared industry or other government

agencies. In FY 2011 other government agencies initiated 485 investigation or operations, from about 20,000 DSS SCRs.

Question: Specifically what do you want us to report--Email found in my spam folder? other??

Answer: DSS CI has informational brochures that provide examples of reportable activities. The brochures are available at: http://www.dss.mil/isp/count_intell/ci_brochures.html

Of particular interest are the Reporting the Threat, Counterintelligence Awareness, and the Cyber Security brochures.

Question: Is there a classified copy of the "Trends" publication?

Answer: Yes, your local DSS Field Counterintelligence Specialist (FCIS) has a limited supply of hardcopies of the classified document. Also, for facilities with access to the SIPRNET, it is available at the DSS SIPRNET website.

Question: During the webinar you mentioned Rad-Hard circuits, what are these and why are they so valuable?

Answer: Radiation hardening, by process or design, protects microelectronics and electronic systems from the effects of ionizing radiation. Ionizing radiation affects these systems during high-altitude flights and space operations, in particle accelerators, and in the proximity of fission or fusion reactions. In environments of high ionizing radiation, non radiation-hardened microelectronics or insufficiently rad-hard microelectronics operationally degrade or fail due to single-event effects. Rad -hard microelectronics are in high demand by countries and companies involved in space programs, research, energy sector, telecommunications, and the military.

Question: In the outlook you seemed to link the increase in SNA to the increase in the number of incidents attributed to government entities, what is the connection?

Answer: Over the past few years the government and cleared industry has improved the ability to identify intrusions into their networks. So, naturally the number of incidents of SNA reported by industry and the government has increased. Much of this has been attributed to cyber actors referred to as advanced persistent threat. DSS assesses that much of this SNA activity originates with government actors, so there is a link between the number of SNA and the number of incidents we attribute to government entities. It is not a one-for-one relationship. It is almost certain that some of this activity originates with commercial and other entities also.