



(U//FOUO) DNE, DNI, and CNE (repost)

FROM: [REDACTED]
Deputy Director for Data Acquisition
Run Date: 12/30/2003

(U) Note from SIGINT Communications: This article appeared on July 16th.

(U//FOUO) DNE, DNI and CNE are interrelated acronyms used extensively in SIGINT that are often confused:

- (S) Digital Network Exploitation (DNE) - **Extracting target intelligence** that requires processing multiple layers of computer protocols that contain multiple types of digitally represented information (voice, fax, video, images, documents, formatted data, emails, messages, etc.) **from any device on the digital global network.**
- (S) Digital Network Intelligence (DNI) - Encompasses the set of facts, inferences and relationships that describe target intelligence extracted from communications residing on the digital global network. **DNI is the resultant intelligence that DNE produces.**
- (TS//SI) Computer Network Exploitation (CNE) - Active or "end-point" collection, which involves **the surreptitious infiltration and mastery of computers and other network components.** Once a device or network has been infiltrated, data of interest can be extracted directly or the targeted system's operation can be modified to facilitate mid-point collection (for instance, by covertly tagging data of interest, rerouting data along accessible links, subtly weakening encryption, etc.).

(TS//SI) DNE is independent of the type of access: the collection can either be end-point or mid-point, active or passive, may (or may not) use CNE methods/techniques. Collection is not limited to a computer; it can be against any system or device in the digital environment.

(S//SI) As our targets continue to migrate toward communications that use the digital global network, DNE increasingly becomes the center of our SIGINT business. This is evidenced by approximately half of our current SID Strategic Objectives directly addressing our need to improve DNE. The 3 V's (volume, velocity, variety) present tremendous challenges in DNE. Our targets are moving from fixed narrowband transmissions to shared, re-routable, extremely wideband, multiplexed, multi-formatted transmissions. Each day, new types of protocols and application formats appear in our targets' communications. Finally, our targets communications are increasingly buried by millions of non-target communications.

(TS//SI) The primary focus of SID's recent transformation efforts is to improve our DNE. Fortunately, the business of DNE has some great opportunities for improvement. The fact there is a global network allows the concept of CNE collection. This allows us to actively hunt the target instead of sifting through the chaff. Also, most communications on the global network include some set of labels about the source, destination and path of the information. This labeling supports new SIGINT development methodology. Using DNE, with the improved labeling, we can quickly map the social, logical and physical networks of our target space. Finally, the continued growth of standards and their widespread use in the global network will allow us to use Commercial-Off-The-Shelf (COTS) tools to portray the communications exactly the same way the target sees it.

(S) In conclusion, DNE is an on-going challenge that has already produced extremely valuable intelligence with great continued promise. Through the coming months and years, we will accelerate our exploitation of DNI and track targets through their migration onto the global network.

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121 ([DL sid comms](#))."

DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL
DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007 DECLASSIFY ON: 20320108