Media/NIT News Articles/ Prior Public Disclosures:

1. ***JustSecurity.Org*** (Ahmed Ghappour article 9/16/14) (Cite along with *Cottom* filings and Wired.Com reports re. Operation Torpedo to show general NIT hacking methods previously disclosed and long known in cybersecutiry circles)

- “A Department of Justice proposal to amend Rule 41 of the Federal Rules of Criminal Procedure would make it easier for domestic law enforcement to hack into computers of people attempting to protect their anonymity on the Internet. The DOJ has explicitly stated that the amendment is not meant to give courts the power to issue warrants that authorize searches in foreign countries—but the practical reality of the underlying technology means doing so is almost unavoidable. The result? Possibly the broadest expansion of extraterritorial surveillance power since the FBI’s inception.”

- **The FBI brand of hacking: Network Investigative Techniques.**

“Broadly, the term “Network Investigative Techniques,” (NIT) describes a method of surveillance that entails “hacking,” or the remote access of a computer to install malicious software without the knowledge or permission of the owner/operator. Once installed, malware controls the target computer. The right Network Investigative Technique can cause a computer to perform any task the computer is capable of—covertly upload files, photographs and stored e-mails to an FBI controlled server, use a computer’s camera or microphone to gather images and sound at any time the FBI chooses, or even take over computers which associate with the target (e.g. by accessing a website hosted on a server the FBI secretly controls and has programmed to infect any computer that accesses it). Network Investigative Techniques are especially handy in the pursuit of targets on the anonymous Internet—defined for the purposes of this post as those using Tor, a popular and robust privacy software, in order to obscure their location (and other identifying information), and to utilize so-called “hidden” websites on servers whose physical locations are theoretically untraceable. Since Network Investigative Techniques work by sending surveillance software over the Internet (at 9), the physical locationof the target computer is not essential to the execution of the search. Indeed, the DOJ proposal is justified as the only reasonable way to confront the use of anonymizing software, “because the target of the search has deliberately disguised the location of the media or information to be searched.” (at 9).

**The DOJ Proposal**

The proposed amendment addresses a jurisdictional limitation in the current version of Rule 41(b)(1) that prevents a judge from issuing a warrant unless the target is known to be located within her district.

(6) a magistrate judge with authority in any districtwhere activities related to crime may have occurred hasauthority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information *located within oroutside of that district* if (A) the district where the media or information is located has been concealed through technological means F.R.Cr.P. Rule 41(b)(6)(A)(proposed) (emphasis added).”

2. “***Mail Online***” article 7/7/15:

- Site had more than 214,000 members

- Server located in NC.

- Operated on Tor.

- Seized on 2/20

- Warrant issued in Va.

- “Authorized [the FBI] to use a technique that would cause a computer to send it anytime a user logged on.”

2. ***Ars Technica*** (online computer news magazine) 7/16/15:

- “A newly unsealed FBI search warrant application illustrates yet another example of how the government deploysmalware and uses sophisticated exploits in an attempt to bust up child pornography rings. A newly unsealed FBI search warrant application illustrates yet another example of how the government deploys malware and uses sophisticated exploits in an attempt to bust up child pornography rings.”

- **Contains link to *Ferrel* SW affidavit**.

- "This is another example of the FBI obtaining a warrant that they are not yet authorized to obtain or execute based on ***the lack of technical expertise of the judiciary***," Ahmed Ghappour, a law professor at the University of California, Hastings, told Ars.

3. ***Ferrel* residential warrant application** (15M 534 EDNY, filed 6/10/15, now unsealed).

- Like Michaud app., describes how Tor works & describes Website A.

- **Discloses specific NIT methodology** (*see Ferrel* at para.).

4.  ***Escobosa* complaint (**MJ15- 00813 EDNY, filed 9/23/15).

- Para. 4: “On or about February 20, 2015, the computer server hosting Website A was seized from a web-hosting facility in Lenoir, North Carolina. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of Website A.”

- Para 20: Reveals name of target site = “**Playpen**.”

5. ***Staten Island Advocate*** re. *Escobosa* (9/30/15)

- “***Escobosa*** , whose age and home community were not released by federal authorities, joined a web sitedescribed in court documents as ‘Website A’ and ‘Playpen’ on Feb. 4 of this year, prosecutors allege.”

- Article describes site = 2/20 seizure by FBI, located in Lenoir, N.C..

- Does *not* discus NIT.

6. ***Orlando “News 6”*** video & article (re. *Hughes* Case in Florida) 10/27/15:

- FBI “taking over web sites” and keeping them running to catch targets in the act.

- “Brought to light new investigative techniques”

- Hughes attorney: “As a citizen I was shocked”

- “Details came out during detention hearing.” - audio of agent.

- Investigation of dark web; agents used “a program that pierces anonymity.”

7. ***SC Magazine*** (IT Security News), 10/15/15;

- Reports on *Escobosa*; “The FBI used spyware, or as the agency prefers to call it, Network Investigative Techniques (NIT), to ensnare an alleged collector and watcher of child pornography earlier this month.”

- “[FBI Atent Shahrani wrote [in an unsealed complaint] that a *Tor-based* website, called “Playpen,” was previously in operation and wasdedicated to “the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including the safety and security of individuals who seek tosexually exploit children online.”

- “After the *FBI* identified the website’s onion address, or Tor specific URL, it moved to seize the computer server hosting it. At that point, the agency deployed a NIT.”