Notes for Dutch SIGINT/Cyber Analytic Exchange

[redacted], MIVD
[redacted], AIVD
[redacted], AIVD
[redacted], MIVD
[redacted] MIVD
[redacted], AIVD
[redacted] AIVD
[redacted] AIVD
[redacted] AIVD

14 February 2013

Organization of Cyber in the Netherlands (U)

(S//SI//REL TO USA, NLD) The meeting began with a briefing from the Dutch about their reorganization and the creation of the new SIGINT and Cyber Division and Single Point of Contact (SPoC). [redacted] noted that Project [redacted] to create this new division appears to be on track, with MIVD and AIVD technical specialists starting to be pulled out of their original locations to join the new division, located at AIVD HQ in Zoetermeer. This new division will be headed by a steering committee comprised of MIVD Director Pieter Bindt and AIVD Director Rob Bertholee. Under them will be the SPoC, headed by [redacted] //as a sidenote, plans are under way for [redacted] to visit NSA at the end of May//. Slide 7 includes a couple of abbreviations: AS = MIVD's SIGINT Division, SOM = AIVD's Special Investigating Committee, QMO = the support organization. The SPoC technical specialists will work closely with the analysts (including [redacted] branch), who will remain in AIVD outside the new entity. NLNCSA (the Dutch equivalent of IAD) will probably also be pulled into the new entity.

(S//SI//REL TO USA, NLD) The Dutch created the National Cyber Security Center (NCSC) in Jan 2012 to cover general (not military) cyber issues, and this center is still dealing with growing pains. It is having difficulty filling all its vacancies, it still lacks a legal framework, and private companies fight any public notification that cyber attacks have taken place. When asked where to turn for help in the case of an intrusion on a commercial entity, the answer was that it depends—if the help needed is technical, then AIVD; otherwise, NCSC. [redacted] averred that AIVD has good relations with companies. The national police (KLPD) has a liaison with NCSC also.

(S//SI//REL TO USA, NLD) The National Detection Network (NDN) governs Dutch sensors. This network is DEVELOPING—some sensors are public and some are private, some entities have their own [redacted], and they tie into the NCSC. [redacted]

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20301012

[redacted]

(S//SI//REL TO USA, NLD) Some other notes:

- The Dutch do not have red or blue teaming yet
- AIVD is concerned with espionage, not crime
- The Dutch are working toward having only one IP point where all government agencies touch the internet, because this will be easier to monitor/defend
- 80 percent of NSA tools used to find malware are commercial, while 100 percent of Dutch tools are
- In the cyber realm, there is no ONE government agency in charge yet, but it will eventually be the NCSC
- There is still no cable access yet, but the laws may be changed in the next year or two. However, Dutch lawyers believe that they can tap it now if it is for DEFENSIVE measures only

Webfora and the Onion Router (TOR) (U)

(S//SI//REL TO USA, NLD) The web forum discussion was of greater interest. The Dutch provided an overview of their data presentation tool (at a very high level). They acquire mySQL databases via CNE access, [redacted] They're looking at marrying up the forum

data with other social network info, and trying to figure out good ways to mine the data that they have.

(S//SI//REL TO USA, NLD) Questions the Dutch had were based on our analytic tradecraft. [redacted] noted that we use keywords to some extent, and outlined the division of effort between [redacted] and sustained targeting. If that partner engagement is of interest (from [redacted] perspective, it is in that we want to track their activities on [redacted] and maximize their exploitation of that data), [redacted] suspects we can focus on tradecraft and general analytic philosophy and build quite a bit of credibility that way.

(S//SI//REL TO USA, NLD) [redacted] gave a brief update on our efforts with Tor, noting that the multi-national effort seemed the best avenue for a sustained capability at present and we are actively working our legal processes to make progress.

ACTION ITEMS FROM 14 FEBRUARY 2013 MEETINGS ON SIGINT/CYBER
(These action items have also been sent separately)

1) (S//SI) CDO/IAD and NTOC: Draft a cyber MOU for Dutch review
--CDO/SIGINT to inform DIRNSA that MOU will be drafted (DIRNSA and AIVD Director both informed; NTOC will draft MOU)

2) (S//SI) CDO/SIGINT: Seek preview of public version of [redacted] message and convey to [redacted] that having a preview in the future in time to alert Dutch CERTS would be ideal (done—not enough time to obtain preview for this round, but the idea for the future has been conveyed)

[redacted]

4) (S//SI) CDO/SIGINT: Will try to obtain updated version of [redacted] for Dutch (done)

5) (S//SI) [redacted] Will share information, handles, etc, on hackers

6) (S//SI) CDO/SIGINT: Will create Cyber forum on [redacted]; will forward Tutelage and Malware presentations, Webfora article, and agenda via [redacted] (briefings sent, but awaiting list of which U.S. personnel to put in Cyber forum)