CRYPTOME

8 October 2013

Canadian Communications Security Establishment Spied BR Ministry

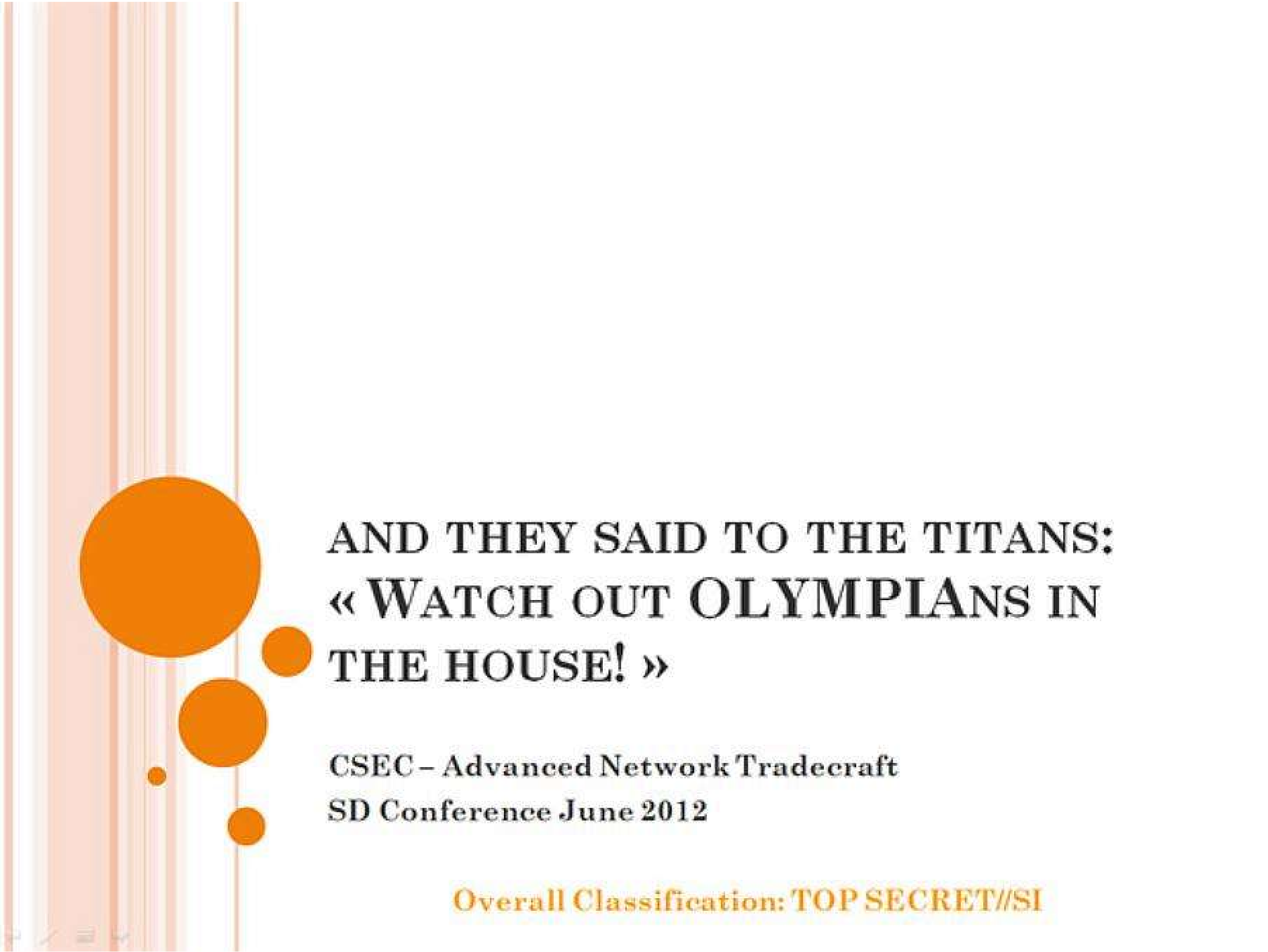
Google translation.

http://m.g1.globo.com/fantastico/noticia/2013/10/ministerio-das-minas-e-energia-esta-na-mira-de-espioes-americanos-e-canadenses.html

Ministry of Mines and Energy is in the crosshairs of American spies and Canadian

Fantastico had exclusive access to a document leaked by Edward Snowden, a former analyst at the National Security Agency of the USA.

10/06/2013 22h23 - Updated 07 / 10/2013 19h33



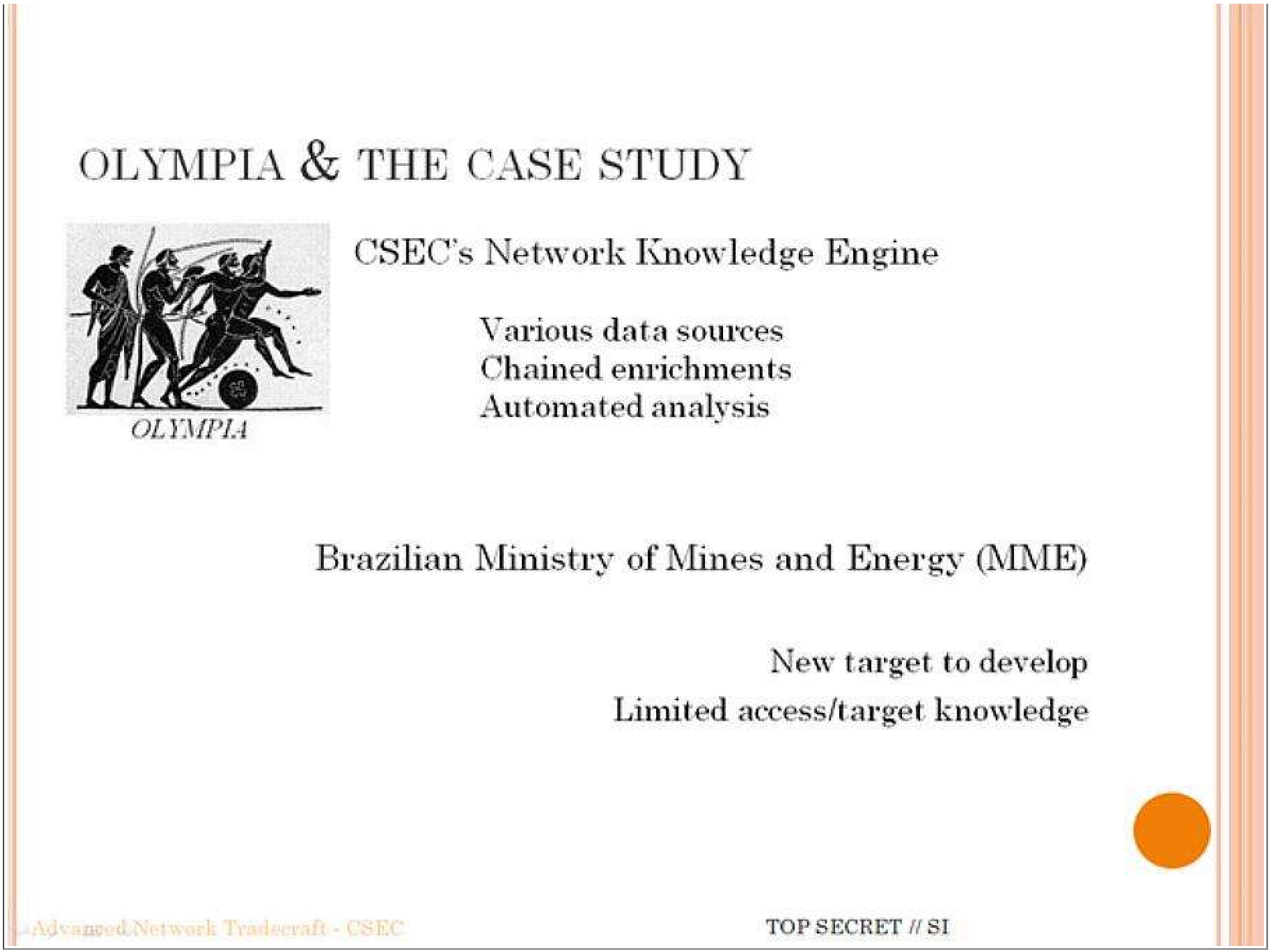
AND THEY SAID TO THE TITANS: « WATCH OUT OLYMPIANs IN THE HOUSE! »

CSEC – Advanced Network Tradecraft

SD Conference June 2012

Overall Classification: TOP SECRET//SI

In this slide below, the introduction to the topic of the presentation: the Olympia program and a case study. Tool Knowledge Network of CSEC, Multiple Information Sources, enrichments Chained, Automated Analysis. Ministry of Mines and Energy (MME). A new target to be developed. Limited access. Knowledge of target.



OLYMPIA & THE CASE STUDY

OLYMPIA

CSEC's Network Knowledge Engine

Various data sources
Chained enrichments
Automated analysis

Brazilian Ministry of Mines and Energy (MME)

New target to develop
Limited access/target knowledge

Advanced Network Tradecraft - CSEC

TOP SECRET // SI

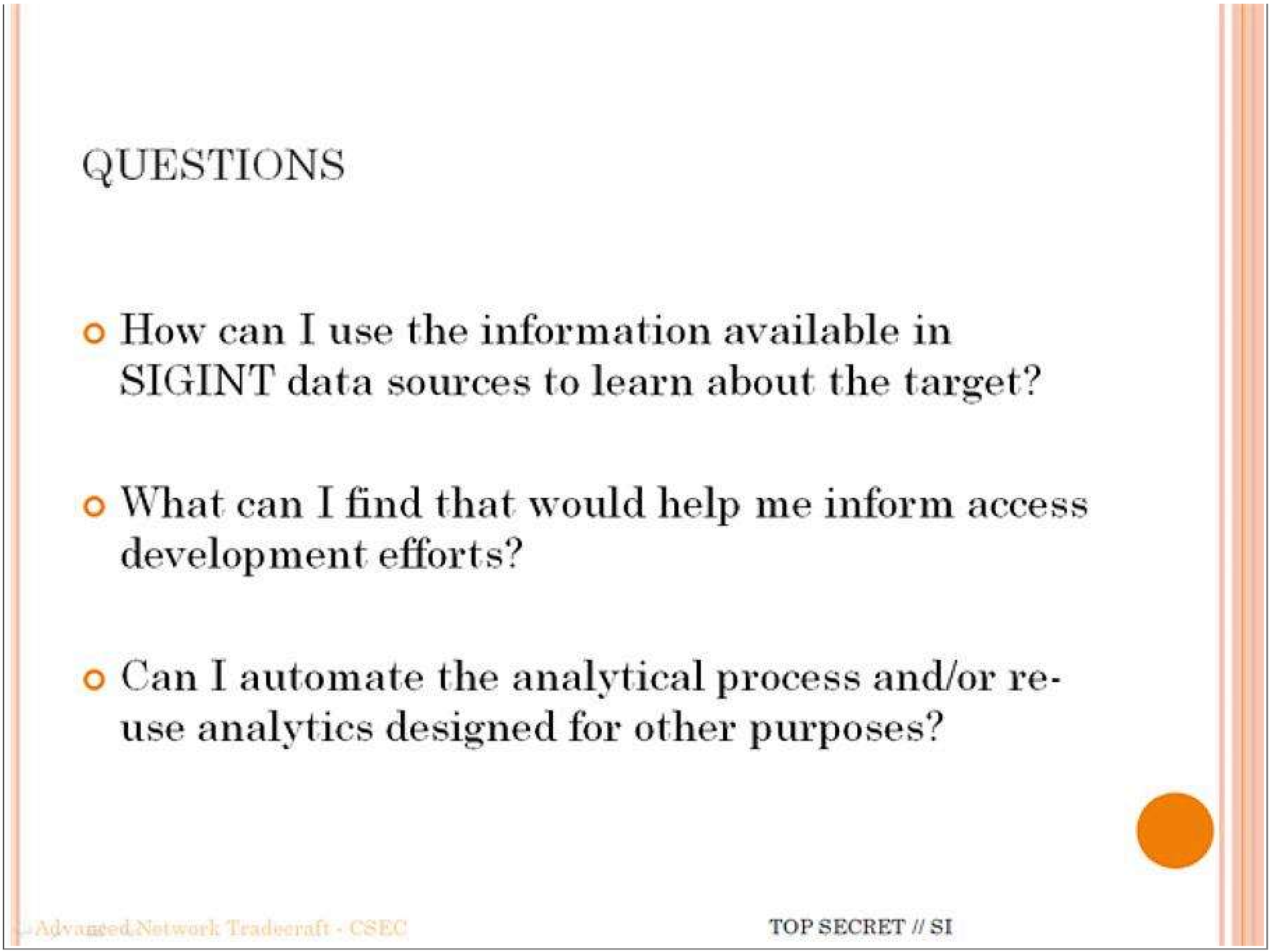
The questions that the presentation seeks to answer:

"How can I use the information available in data sources signals intelligence to learn about the target?"

"What can I find to help me inform efforts to develop access?"

"Can I automate the analytical process and / or reuse analyzes created for other purposes?"

The acronym SIGINT is literally Signal Intelligence, a way of designating eavesdropping.



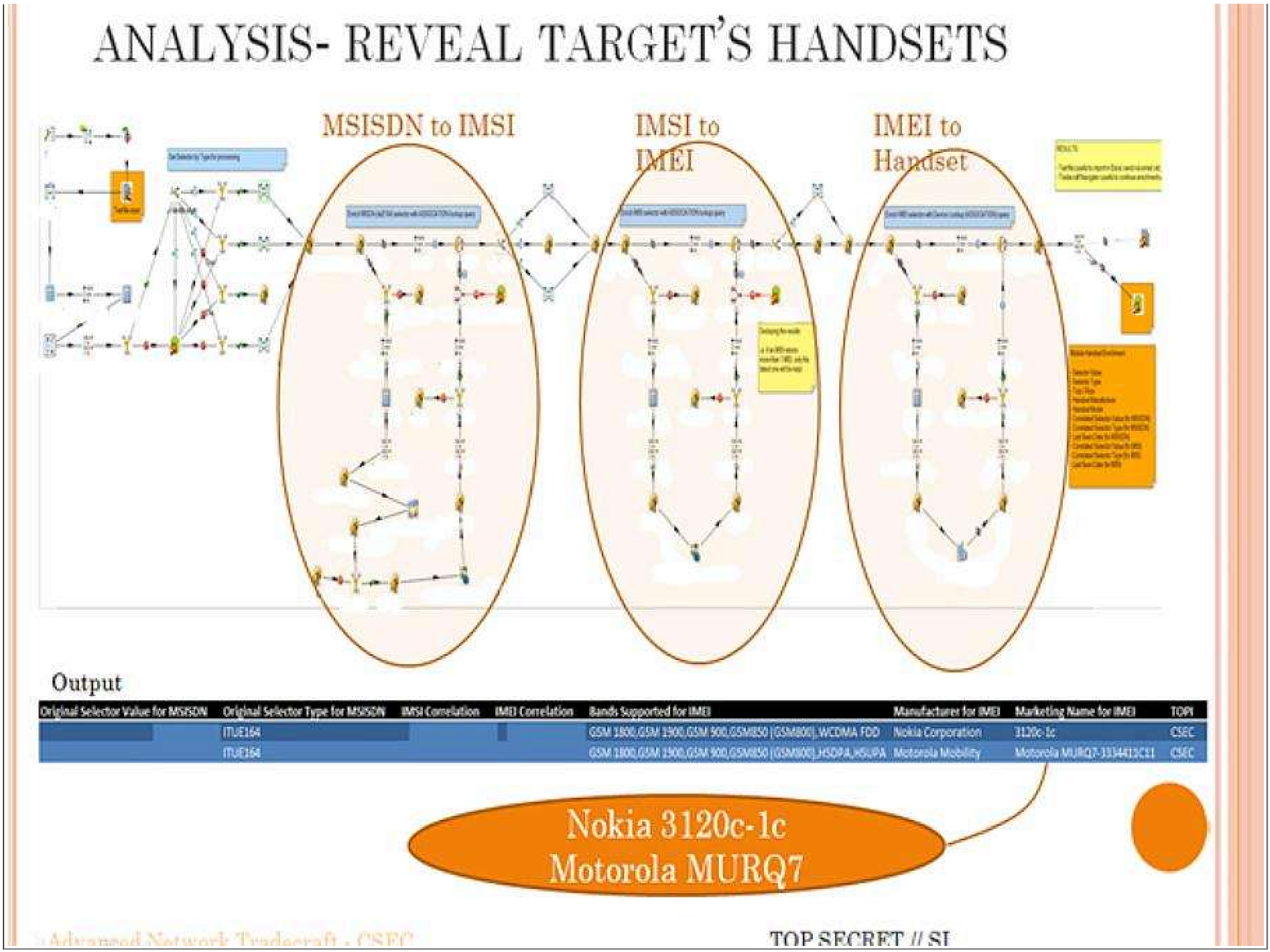
QUESTIONS

- How can I use the information available in SIGINT data sources to learn about the target?
- What can I find that would help me inform access development efforts?
- Can I automate the analytical process and/or re-use analytics designed for other purposes?

Advanced Network Tradecraft - CSEC

TOP SECRET // SI

Here diagrams show how to identify the "target cell". At the foot of the slide, there are two numbers Brasilia and the numbering of their chips.



ANALYSIS- REVEAL TARGET'S HANDSETS

Output

Original Selector Value for MSISDN	Original Selector Type for MSISDN	IMSI Correlation	IMEI Correlation	Bands Supported for IMEI	Manufacturer for IMEI	Marketing Name for IMEI	TOPI
[redacted]	ITUE164	[redacted]	[redacted]	GSM 1800,GSM 1900,GSM 900,GSM850 (GSM800),WCDMA FDD	Nokia Corporation	3120c-1c	CSEC
	ITUE164			GSM 1800,GSM 1900,GSM 900,GSM850 (GSM800),HSDPA,HSUPA	Motorola Mobility	Motorola MURQ7-3334413C11	CSEC

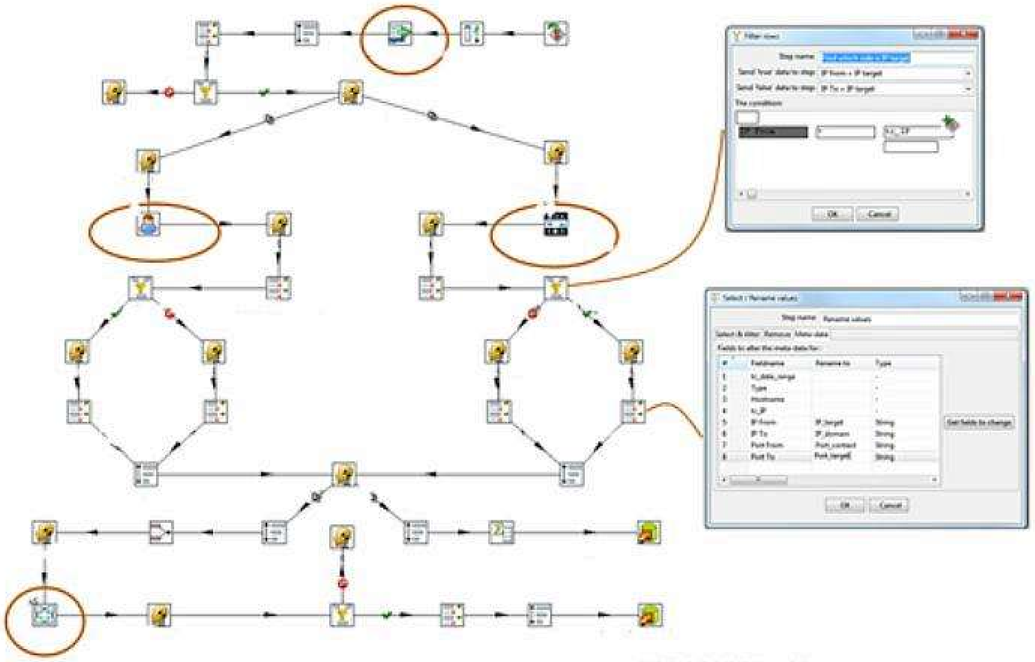
Nokia 3120c-1c
Motorola MURQ7

Advanced Network Tradecraft - CSEC

TOP SECRET // SI

In this slide, the flow that gives the process that determines "the IPs with which it communicates my aim."

ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH



Filter rows

Step name: [illegible]

Send 'true' data to step: IP From = IP target

Send 'false' data to step: IP To = IP target

The condition:

IP_From = tc_IP

Select / Rename values

Step name: Rename values

Select & Alter | Remove | Meta-data

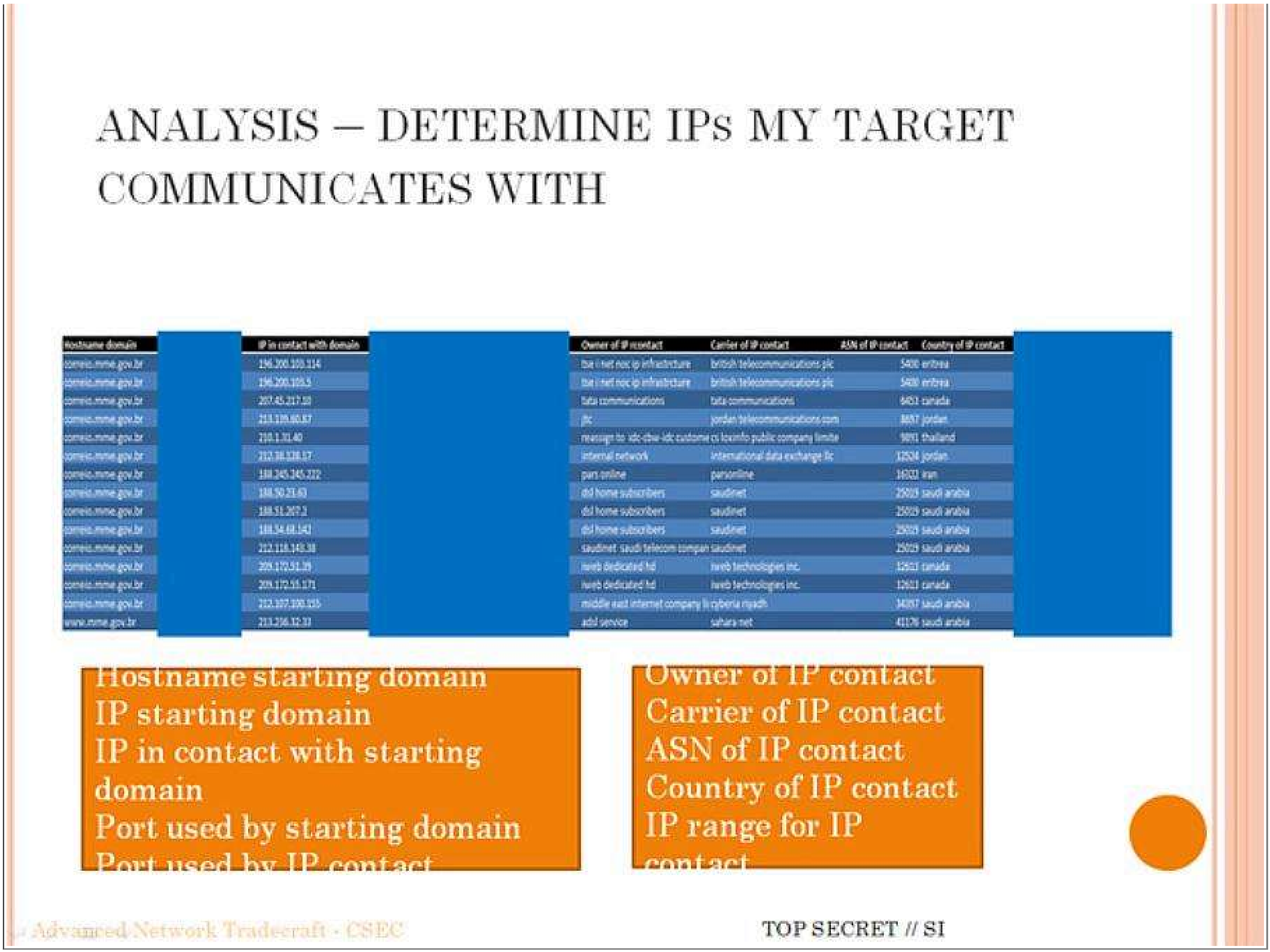
Fields to alter the meta-data for:

#	Fieldname	Rename to	Type
1	tc_date_range		-
2	Type		-
3	Hostname		-
4	tc_IP		-
5	IP From	IP_target	String
6	IP To	IP_domain	String
7	Port From	Port_contact	String
8	Port To	Port_target	String

Advanced Network Tradecraft - CSEC

TOP SECRET // SI

The next slide contains a table that shows the search result of IPs. Providers are countries like Thailand, Jordan, Iran, Saudi Arabia and Canada.



ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH

Hostname domain	[redacted]	IP in contact with domain	[redacted]	Owner of IP rcontact	Carrier of IP contact	ASN of IP contact	Country of IP contact	[redacted]
correio.mme.gov.br	[redacted]	196.200.103.114	[redacted]	tse i net noc ip infrastructure	british telecommunications plc	5400	eritrea	[redacted]
correio.mme.gov.br	[redacted]	196.200.103.5	[redacted]	tse i net noc ip infrastructure	british telecommunications plc	5400	eritrea	[redacted]
correio.mme.gov.br	[redacted]	207.45.217.10	[redacted]	tata communications	tata communications	6453	canada	[redacted]
correio.mme.gov.br	[redacted]	213.139.60.67	[redacted]	jtc	jordan telecommunications.com	8697	jordan	[redacted]
correio.mme.gov.br	[redacted]	210.1.31.40	[redacted]	reassign to: idc-cbw-idc custome	cs loxinfo public company limite	9891	thailand	[redacted]
correio.mme.gov.br	[redacted]	212.38.128.17	[redacted]	internal network	international data exchange llc	12524	jordan	[redacted]
correio.mme.gov.br	[redacted]	188.245.245.222	[redacted]	pars online	parsonline	16322	iran	[redacted]
correio.mme.gov.br	[redacted]	188.50.21.63	[redacted]	dsl home subscribers	saudinet	25019	saudi arabia	[redacted]
correio.mme.gov.br	[redacted]	188.51.207.1	[redacted]	dsl home subscribers	saudinet	25019	saudi arabia	[redacted]
correio.mme.gov.br	[redacted]	188.54.68.142	[redacted]	dsl home subscribers	saudinet	25019	saudi arabia	[redacted]
correio.mme.gov.br	[redacted]	212.118.143.38	[redacted]	saudinet saudi telecom compan	saudinet	25019	saudi arabia	[redacted]
correio.mme.gov.br	[redacted]	209.172.51.39	[redacted]	iweb dedicated hd	iweb technologies inc.	32613	canada	[redacted]
correio.mme.gov.br	[redacted]	209.172.55.171	[redacted]	iweb dedicated hd	iweb technologies inc.	32613	canada	[redacted]
correio.mme.gov.br	[redacted]	212.107.100.155	[redacted]	middle east internet company li	cyberia riyadh	34397	saudi arabia	[redacted]
www.mme.gov.br	[redacted]	213.236.32.33	[redacted]	adsl service	sahara net	41176	saudi arabia	[redacted]

Hostname starting domain
IP starting domain
IP in contact with starting domain
Port used by starting domain
Port used by IP contact

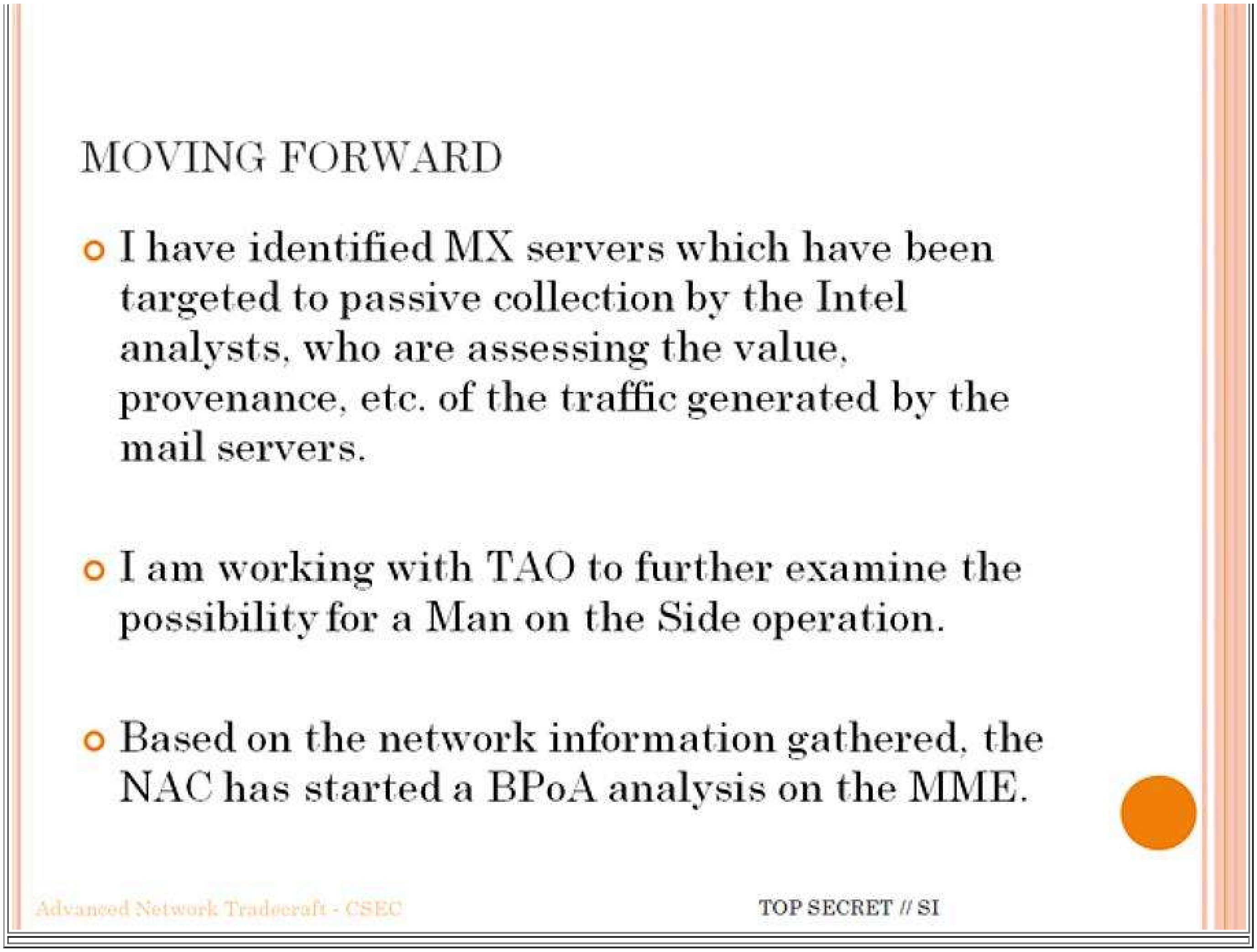
Owner of IP contact
Carrier of IP contact
ASN of IP contact
Country of IP contact
IP range for IP contact

Advanced Network Tradecraft - CSEC

TOP SECRET // SI

In conclusion, the responsibility for submitting claims: "I identified the mail servers that were targeted by passive collection of intelligence analysts who are evaluating the value, origin etc. Traffic generated by mail servers."

The remaining lines report that at the time (June 2012) the agency worked to evaluate a possible operation passive observation (Man on the Side operation), which suggests it is a watch without interference and to deepen the analyzes of Ministry based on the network information obtained.



MOVING FORWARD

- I have identified MX servers which have been targeted to passive collection by the Intel analysts, who are assessing the value, provenance, etc. of the traffic generated by the mail servers.
- I am working with TAO to further examine the possibility for a Man on the Side operation.
- Based on the network information gathered, the NAC has started a BPoA analysis on the MME.

Advanced Network Tradecraft - CSEC

TOP SECRET // SI