Zpráva centrále

Během vyšetřování bylo prokázáno, že Karel Weber komunikoval s centrálou pomocí šifrového spojení. Za tím účelem byl vybaven následující převodovou tabulkou a bločkem hesel. Tabulka i bloček byly přiloženy jako přílohy k vyšetřujícímu spisu.

	0	**1**	**2**	**4**	**6**	**7**	**8**	**9**		
-	D	E	I	N	S	T	A	R	Weber	57130 19
3	B	C	F	G	H	K	L	M	Heslo	34089 23
5	O	P	Q/J	U	V	W	X/Y	Z	šifra	81119 32

Obžalovaný Weber tvrdil, že žádnou zprávu nestačil odeslat. Zpravodajské službě se také žádný telegram, který by odpovídal této šifře, nepodařilo zachytit. Bloček s heslovým materiálem (http://soutez2009.crypto-world.info/pribeh/blocek.txt) byl neporušený. Vyšetřovatelům byl znám pokyn, že heslové skupiny, které byly použity k vytvoření šifrového textu, mají být ihned zničeny, a proto uvěřili, že Weber žádnou zprávu centrále neodeslal. I to byl jeden z důvodů, proč se předpokládalo, že informace o analyzovaném šifrátoru ŠD-2 / CM-1 nebyly předány cizí rozvědce.

Skutečnost však byla jiná. Weber centrále pravidelně zprávy zasílal. Informoval v nich o naverbování Václava Prokopce a zaslal do centrály vše, co se od něj dozvěděl. Z bločku však spotřebovaná hesla nevytrhával. Vždy si pouze zapamatoval, kde skončil a při přípravě nové zprávy začal s pětící na novém řádku. Tím si zajistil, že heslo nebylo nikdy použito dvakrát. Ze školení, kterým prošel, věděl, že v takovém případě nelze z šifrového textu zprávu vyluštit, a proto mu vytrhávání hesel připadalo nadbytečné. Heslový materiál mu zbýval ještě na několik zpráv.

Poslední zpráva, kterou odeslal, byla tato:

```
68576 77942 06114 43386 56023 74203 22741 66582 02226 13131 15890 66109
96557 20241 42904 12392 12984 70271 69657 78286 29296 00944 79991 19559
02306 94898 73939 34036 80892 35887 69559 31457 97026 13827 88962 80230
76938 94373 84895 78410 92618 94152 62805 91699 01170 62473 21551 37649
17124 18980 36924 89892 20370 25273 68133 02387 70637 66963 53819 88797
02705 51891 50361 67559 17921 14809 42001 68270 83314 91067 31520 82976
```

Před zatčením se mu podařilo uschovat rozbor a plán šifrátoru do mrtvé schránky, kde byly kurýrem cizí rozvědky vyzvednuty a odvezeny do centrály. Tajemství šifrátoru ŠD-2 / CM-1 tak bylo vyzrazeno a to umožnilo americké rozvědné službě postavit jeho funkční repliku. V následujících letech se pak rozvědce opakovaně podařilo získat klíčový materiál a dešifrovat řadu důležitých zpráv.