kloonscenario standhoudt indien het tot in detail onder de loep wordt genomen in het licht van de door mij in onderdeel 5 omschreven randvoorwaarden. Bovendien, het gaat er niet alleen om of het mogelijk is om van *een* simkaart een kloon te vervaardigen, maar of van de simkaart die in gebruik is bij een specifiek persoon onder de tap (i.c. Baybaşin) in de praktijk van 1997/1998 een kloon kon worden geconstrueerd.

Hieronder bespreek ik de argumenten van Van de Ven en de tegenwerpingen van Van den Heuvel. Pas op het eind bespreek ik de vraag of – zelfs aangenomen dat gsm-technologie en gsm-beveiligingsmechanismen sim-cloning toelaten – het kloonscenario een praktisch werkbaar scenario van manipulatie oplevert.

De argumenten van Van de Ven

Ik laat Van de Ven zelf aan het woord in z'n meest uitgebreide variant. Daarbij zou ik tevens zijn voetnoten hebben overgenomen, ware het niet dat die ontbreken. Ik citeer Van de Ven:

> *"Een bruikbare methode om gemanipuleerd audiomateriaal in een tapkamer-systeem te importeren is door gebruik te maken van een "gekloond" GSM-toestel.*
> *Middels dit "gekloonde" GSM-toestel is het mogelijk om vanuit Nederland een verbinding op te zetten die parallel loopt aan het "getapte" nummer en vervolgens kan er gemanipuleerd audiomateriaal in het Nederlandse tapkamersysteem (LEA domain) worden ingevoerd.*
>
> *Omdat binnen het GSM-netwerk maar één IMSI/IMEI paar per tijdseenheid wordt toegestaan, is het niet mogelijk dat zowel het originele GSM-toestel als het "gekloonde" GSM-toestel gelijktijdig in het GSM netwerk actief zijn. Het GSM-toestel dat in het GSM-netwerk actief is blokkeert automatisch het andere toestel.*
>
> *Bij deze vorm van manipulatie is het noodzakelijk om een "kloon" van een originele SIM-kaart te kunnen maken.*
> *Een SIM-kaart bevat standaard 29 files waarvan slechts de IMSI (International Mobile Subscriber Identity) en de Ki (geheime sleutel) nodig zijn voor het maken van een bruikbare "kloon".*