veiligheid van de staat
sûreté de l'état
VSSE

BISC : Cyber Security

What can the VSSE contribute?

VSSE

Overview

- Introduction
- Legal framework
- Dynamics of the threat
  - Nature of cyber attacks
  - Targeting
  - Paradigm shifts
  - Who's targeting what?
- Tools used – modus operandi
- VSSE at a glance
- VSSE understanding of Belgian Cyber Security policy

I. Legal Framework

- Law 30th November 1998
  → Duty to gather & analyse data related to 7 threats including espionage.
- Law 4th February 2010 – "BIM law"
  → Communications interception, IP identification.
- MoU with military intelligence

II. Dynamics of the cyber threat

- Intensified → sustained efforts must be dedicated to cyber-enabled espionage.
- Focused → victims of cyber espionage were carefully and repeatedly targeted.
- Is it cyber-enabled espionage only or the new dominant form of espionage on its own?

III. Nature of the threat

- Strong influence of three trends:
  - Rise of Big data
  - APTs
  - Web black market
- Who is attacking Belgium?
  - Nation states
  - Organized crime
  - Hacktivists
  - Terrorists

IV. Tools used & Modus Operandi: striking features

- Vast array of possible configurations
- Democratization of tools & services
- Stuxnet, Duqu, Flame and the like in Belgium?
  → Traces might be found but real issue is when such capacities will become available for others?

V. VSSE at a glance

- Modest technical and analysis capacity
- Cannot stand the comparison with foreign intelligence services
- National cyber security policy and associated processes still in their infancy

VI. VSSE & the new Belgian Cyber Security Strategy

- Acknowledgement of the threat
- Need for maximum cooperation
- Center for cyber security
- Duty to report

Thank you for your attention!