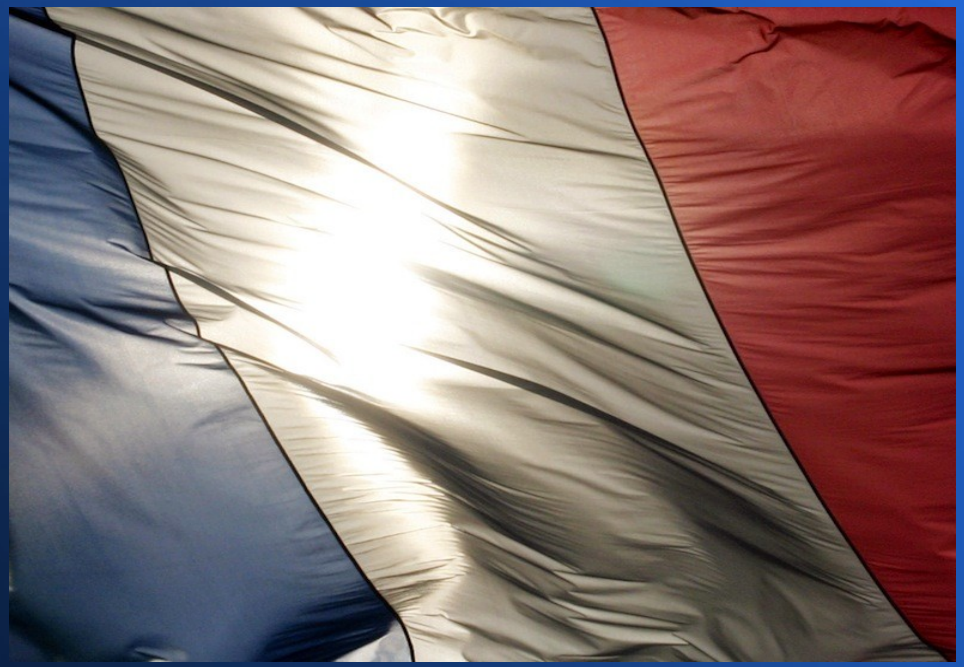
University of Florence: 5-6 May 2015

The new cyber defense policy of France: from late awareness to adapted response?

Overview



Thierry FORTIN
Sciences Po Lyon

British current Defence policy

Outline

- **Introduction:** the cyberspace: a new battlefield

  Part 1: late first steps in cyberdefense

  Part 2: threat awareness prompting response

  Part 3: the current organisation: momentum gained and enhanced cooperation between agencies

- **Conclusion: a** never-ending catchup to remain *a world power in cyberdefence*

  (France's Strategy, ANSSI, 2011)

Introduction

- Cyberspace = new battlefield requiring new technology, new staff (Cyber Reserve staff), new doctrines, new approaches
- Growing awareness BUT responsive moves not proactive ones
- e.g.: 2007 cyberattacks on Estonia

(NATO's article 5 challenged)

- Network centric structures = openness / information-sharing vs protection / need-to-know principle / defense postures

Introduction

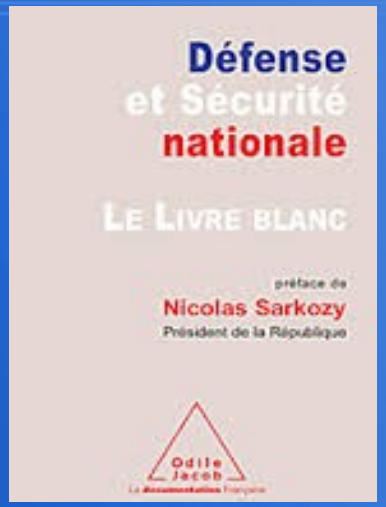
- Most of the initial literature in English (threat somehow overlooked by France until the 2000s)
- French Armed Forces bridging the digital gap through the 1990s and 2000s with little focus on defense = IT engineering schools not addressing the issue...
- Vulnerability growing with the parallel growth of the connected operators (energy production like nuclear plants / hospitals / transport networks / military assets and sites / telecom.)

"France must retain its areas of sovereignty, concentrated on the capability necessary for the maintenance of the strategic and political autonomy of the nation: nuclear deterrence; ballistic missiles; SSBNs and SSNs; and cyber-security are amongst the priorities."

French White Paper on Defence and National Security, p.306

Part 1

- Livre Blanc de la Défense 2008:
  (White Paper on Defence)



- Cyber = *the threat of the next 15 years*

- Threat taken into account (declaratory policy) but limited action

Part 1

- **Led to the creation of ANSSI (French Network and Information Security Agency)**
- Missions = higher national authority in ISS
- standardization / enforcement / watch-detection alert-response / information & awareness (firms) / support

  Budget = 75mn EUR / Staff = 360 (2013) 500 pers (end 2015)
- Patrick PAILLOUX (first DGANSSI)
- Current director = Guillaume POUPARD (nom. March 2014) (cryptography and cyberdefense specialist)
- **Governance = Strategic Committee (SGDSN / EMA / DGA / DGSE / DGSI + other members)**

ANSSI
(French Network and Information Security Agency)

Part 1

- International situation accelerating the awareness-growing process in highly connected nations:

  2010 *Stuxnet* attack on Iran's uranium enrichment facilities (US and Israel?)

- Standoff capability to deliver strikes on a nation's vital interests without resorting to "conventional" weaponry

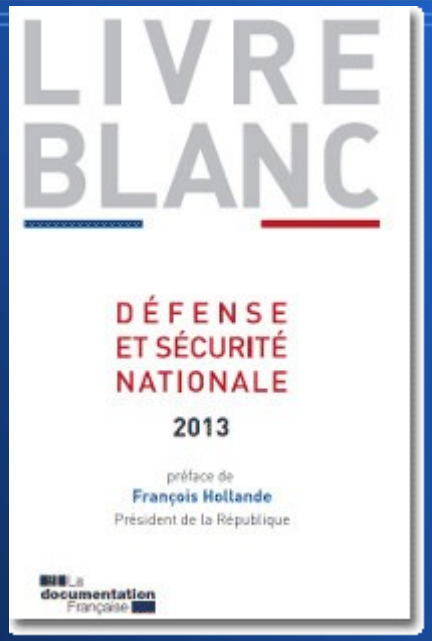
Part 2

- 2011: release of *France's Strategy = national sovereignty (decision-making) / protection of vital infrastructures / first-ranking nation (France's grandeur?)*
- French Senator Jean-Marie Bockel's quote in 2012

  "France still late on schedule in comparison with the UK and Germany..."
- Increasing number of attacks on all types of institutions (public-private / civilian-military) prompted a reinforced defensive stance

Part 2

- Livre Blanc 2013:



- LPM 2014-19:

Part 3

- Current trends = intense cooperation between services
- Addressing the full spectrum of threats with the widest range of measures
- Prevention (through awareness, education and training)
- Support
- Defense
- Attack

Part 3

- ANSSI: enhancing scope of action / building closer cooperation with other CD components

  relocation with CALID (cyber defense unit) in the same building in Paris 7

Part 3

- Military Component of Cyberdefense
- Cyberdefense Centre (detect – defend – locate & ID)
- DGA – MI (Maîtrise de l'Information) at Bruz
- Creation of CALID (current staff = 60 / next 5 yrs several hundred) [same site as ANSSI]

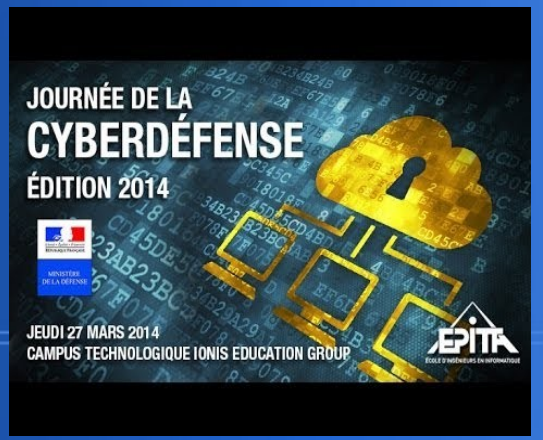
CA Arnaud Coustilière

Part 3

- Military Component of Cyberdefense

- Cyberdefense integrated into training like CRBN or First aid (ESCC = Cyber Dpt)

- Cyber Reserve (ca. 150 personnel)



Part 3

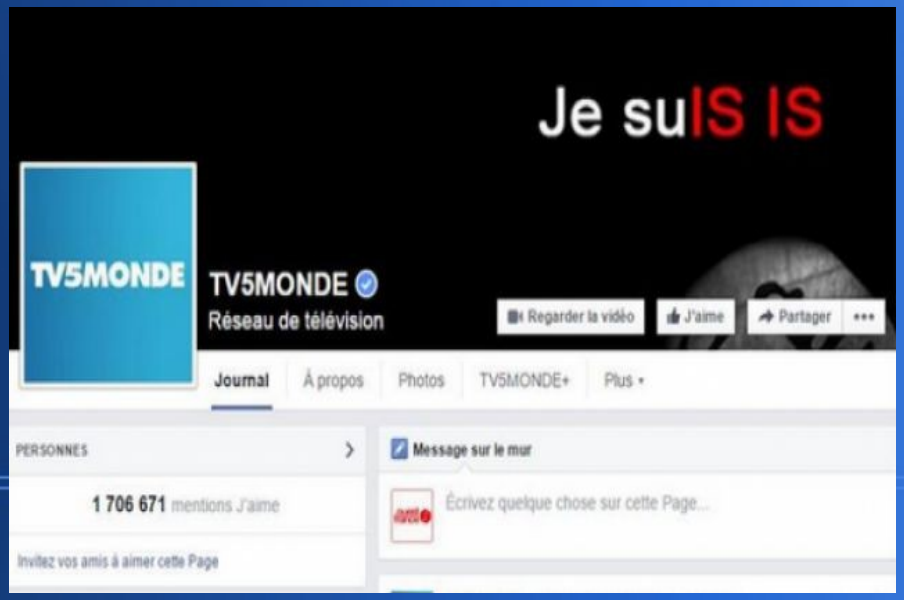
- Civilian sphere:
- Creation of Cyberdefense Engineering School in Vannes
- first class of 26 engineers trained
- Hundreds needed

Conclusion

- Permanent beefing-up to catch up with the increasing challenges and the omnipresent threat (ANSSI projected staff 500+ (end 2015) + budget = 80mn EUR (2014)
- Cyber = standoff / limited number of operators / high payoff attacks / locating difficult / maximum number of victims

Conclusion

- Peak of attacks in the aftermath of the 7 January terrorist attacks in France (hundreds of sites with impact but no significant damage)
- Jan 2015: *Le Monde* (Syrian Electronic Army)
- April 2015: TV5 Monde



Thank you for your attention !