

# Backup network for incident response

## *How do face network breakdown ?*

Gilles ANDRÉ

gilles.andre@certa.ssi.gouv.fr

CERTA

1	Purpose of a CERT . . . . .	2	8	Candidate solutions . . . . .	9
2	How do we work ? . . . . .	3	9	A Radio network for European CSIRTs . . . . .	10
3	Sample of contact information . . . . .	4	10	Are we radio hobbyists ? . . . . .	11
4	Single point of failure . . . . .	5	11	A network dedicated to CSIRTs . . . . .	12
5	Probability of such an attack . . . . .	6	12	Constraints . . . . .	13
6	Need for a backup network . . . . .	7	13	Your opinion is welcome . . . . .	14
7	Requirements for a backup network . . . . .	8			

## Purpose of a CERT

---

Backup network for incident response

- Coordination of incident response
- Vulnerability advisories

## How do we work ?

---

Backup network for incident response

- our job is to respond to incidents involving our constituency ;
- if an incident involves other constituencies then :
  - we have to warn these CERTs
  - by mail
  - or fax
  - by phone

# Sample of contact information

Backup network for incident response

## Constituency

Type of constituency	Government related
Description of constituency	French administration community; All french public offices and services as well as local territorial offices.
Internet domains and/or IP address ranges	* .gouv.fr (kernel constituency), * .fr
Country of constituency	France

## Team Contact Information

Public WWW server	<a href="http://www.certa.ssi.gouv.fr">http://www.certa.ssi.gouv.fr</a> (french only)
Email address	<a href="mailto:certa-svp@certa.ssi.gouv.fr">certa-svp@certa.ssi.gouv.fr</a>
Regular telephone number	+33 1 41 46 25 23
Emergency telephone number	+33 1 71 75 83 00 (french speaking)
Facsimile number	+33 1 41 46 37 01
Other telecommunication facilities	
Postal address	SGDN/DCSSI/CERTA 51, boulevard de Latour-Maubourg 75700 Paris 07 SP France

## Business Hours

08:30 to 18:30 Monday to Friday (GMT+1, GMT+2 with DST)

## Single point of failure

---

Backup network for incident response

- *trend* : convergence of data and voice networks ;
- the same network will be used for everything ;
- thus, if the network suffers a successful attack, we can't solve the incident because we can neither talk nor send mail to each other.

## Probability of such an attack

Backup network for incident response

- Prophets has been announcing such an attack for years, but ...
  - ... we have never seen such attacks
  - is such an attack possible ?  
there is much debate about it.
  - your opinion is welcome.
- If we believe that such an attack could happen, we have to anticipate to minimize its outcome.
- In the following slides, I have made the assumption that one believes in such an attack.

## Need for a backup network

---

Backup network for incident response

- whatever happen we need to be able to keep in touch
- the network we use to keep in touch could collapse
- thus we need another (backup) network

## Requirements for a backup network

---

Backup network for incident response

**mandatory** these requirements **MUST** be fulfilled

- we need a *physically* different network (to get rid of the convergence effect)
- we need a network that covers our groups (*i.e.* Europe with a rather loose definition of what Europe is)

**important** these requirements are not strictly necessary but brings common sense :

- the network should be cheap ;
- the network should be based on proven technology (we do not want to fund a big study on emergent technologies)

## Candidate solutions

---

Backup network for incident response

- CSIRT team members physically meeting (how do we know where and when to meet ?)
- RFC 1149 : IP datagrams on Avian Carriers :-)
- snail mail : efficient, known, cheap but slow
- satellite telephone (will CSIRT activities be a priority when satellite resources become scarce ?)
- radio network

I will now emphasize on *radio network*

## A Radio network for European CSIRTs

---

Backup network for incident response

- members of the network on a voluntary basis
- based on packet radio (amateur radio or HAM had been using this technology for years)
- HF is necessary because of distances

## Are we radio hobbyists ?

---

Backup network for incident response

- amateur radio is *very* strictly reglemented :
  - it is meant as a hobby designed to improve technology
  - exchange should be limited to technical (radio) topics
  - *exchanges should be clear*
  - amateur radio is done between identified people who acquired a license
- We obviously cannot use radio for CSIRT purpose as hobbyists.

## A network dedicated to CSIRTs

---

Backup network for incident response

- most countries have some kind of “National Agency for Frequencies” to allocate frequencies for those who need one
- license seems not to be mandatory when radio is done between organisation and not people
- It is easier to ask for a frequency when you are an already build organisation
- Is TF-CSIRT the right body to do it ?

## Constraints

---

Backup network for incident response

- it is easy to “sniff” a radio network, cyphering will be mandatory for any exchange
- we need to ensure that cyphering is allowed in every participating CERT countries
- bandwidth of radio networks is rather low (we can't expect more than 300 Bytes/s, better rates cannot be guaranteed), this limits the use of the network to mere mail exchange
- radio network depends on propagation (i.e. some moments are better for communication than others)
- is there still any free frequency available in each involved countries that covers all Europe ?

## Your opinion is welcome

---

Backup network for incident response

- Is the threat of network breakdown probable in a foreseeable future ?
- Is a radio network the appropriate answer ?
- Is there a better answer ?
- Who should be part of such a network ?
- Who should lead (in the radio meaning) the network ?
- Who pays ?

*Proposal* : creation of a working group within TF-CSIRT dedicated to define and experiment an appropriate backup network for European CSIRTs.