CERT Emergency Network

Students:
G.A. van Malenstein, B ICT
R.P. Vloothuis, B ICT

Supervisor:
Jan Meijer, SURFnet

Research Project 1
System and Network Engineering

University of Amsterdam

SURFnet

February 4, 2007

Abstract

This report describes alternative ways for Computer Emergency Response Teams (CERTs) to communicate with each other in case all regular communication methods (Internet, GSM) fail. First, the function of CERTs is described. An overview of techniques for this problem is presented: a TETRA network, KPN Emergency Network, (packet)radio, WiMAX and satellite communications. Also organizational problems are described. A possible solution direction is described along with recommendations and future work.

Contents

Chapter 1

Introduction

On the 18th of January 2007 a big storm hit the Netherlands. Many services like the railroad became unavailable and many people were stranded on railroad stations like Utrecht Centraal. In the SURFnet office at Utrecht there was a power outage in the server room. The servers should have a backup UPS, but these failed to provide the necessary power. An independent power supply was not present. This resulted in a network failure which disconnected the office from the internet. In addition to this, the phones stopped working because they relied on a voice-over-ip network which is based on the same affected network. Communication by phone and the internet became impossible. As backup, CERT members (and also other SURFnet employees) use a cellular phone. Since there were so many people stranded on Utrecht Centraal as a result of the storm, the GSM network overloaded and communicating through this network became impossible. Because of these problems, no one was able to communicate outside of the office making solving this problem very difficult. No one could contact the power company to try to restore the power.

This month, January 2007, a security problem in the Cisco IOS software emerged. Cisco is a big supplier of network equipment and is the major brand for internet routers. A lot of internet nodal points consist of Cisco routers. If there happens to be a flaw in Ciscos TCP/IP implementation it is possible all routers are vulnerable.

Quotation from the Cisco bug report:

> The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.[1]

This affects most Cisco products which uses IOS software. Luckily, Cisco distributed a patch quickly and it didnt have big consequences, but it could have been disastrous if this vulnerability was exploited on a large scale. It could have made all IP traffic impossible including voice over IP networks.

The internet in the SURFnet office was unavailable, which made all land line communication impossible, and the GSM service was overloaded which was supposed to be the backup line for the CERTs. If they had access to an emergency communication network like satellite phone, this wouldnt be a problem. Of course the absence of an independent power supply and the failure of several UPS devices was also part of the problem, but this does not give 100% guarantee it will not occur.

With these incidents it became clear research about this problem is very important. Because we rely so much on the internet we should have some level of certainty it will keep functioning or keep downtime as short as possible. This requires a reliable backup voice communication channel which is always available.

The Internet is a worldwide network of networks. Everywhere in the world, people rely on the Internet. At the same time, people depend on this network. Most Universities, companies, Internet Service Providers and governments have a Computer Emergency Response Team (CERT). A CERT supports these organizations when serious IT-related incidents occur, such as security incidents, 24 hours a day, 7 days a week. We also encounter the term CSIRT (Computer Security Incident Response Team) which in practice means the same.

In this report we describe a solution direction for the situation in which the regular communication channels – Internet, GSM, and PSTN (Public Switched Telephone Network) – are not available. We describe organizational problems and technical solutions. We did not research in which ways the communication between CERTs can be secured; this research focuses on possible solutions. Implementing directives have to be worked out in future work, see chapter Future Work.

1.1 Key problem

For a couple of years, CERT members are concerned how the teams may communicate when the regular communication methods are unavailable because of a (partial) network failure. When a security incident this serious occurs, the CERT-community investigates the cause of the problem and works towards a solution or a direction of a solution for the arisen problem.

During a serious emergency, communication has to be possible via an Emergency Network. The de facto Emergency Network nowadays is the regular Public Switched Telephone Network. However, after British Telecom, KPN Telecom also plans to deploy an All-IP network. This involves a great threat for Internet technology, as the traditional Emergency Network for Computer Security Incident Response Teams may become unavailable in case of a security incident or a network failure.

Because the technical structure of the PSTN network will be changed to IP-technology, Internet IP security incidents can have effect on this telephone network; so communication by telephone can become impossible in case of an emergency.

1.2 Main research question

Which ways of communication can be used for the CERTs for mutual communication when the regular communications network (Internet) fails?

In order to answer this question, we first have to establish what CERTs are, and how they communicate with each other. This is described in section CERTs. We also have to know if there are any organizational obstructions for implementing the possible solution. This solution must fit the need of the CERTs, so technical requirements must be identified.

Because the problem is too wide to address given the time, we have to specify certain pa-

rameters for this project.

1.3 Scope

- The problem focuses on the communication between CERTs at different geographical locations, which may have influence on the functioning of the Internet or are responsible for it. However other persons or departments which have influence on the functioning of the Internet may be described in this report.
- In this research, only the communication between European CERTs – and Dutch CERTs specifically – will be examined. The intention is to create a solution or a direction to a solution, which has to be scalable to European or even to a worldwide level. However, we focus our view on SURFnet-CERT and its surrounding contacts.
- Possible technical solutions will only be examined when they are realistic. One communication node may cost approximately a couple of hundreds of Euros. When an appropriate solution is found, we will try to produce a Proof of Concept (PoC) if possible. Because there is no realistic budget available for this project, this will be very difficult.
- Solutions are being examined on the basis of feasibility and the time available for this Research Project.
- In this Research Project, the emphasis is set onto the use of techniques available at the moment of publishing.
- In the review of the technical solutions, we analyze the feasibility of possible solutions, however we will not cover the security aspect. We cannot establish the requirements of the security aspect, because we do not have a communication plan.

1.4 Research methods

At the start of this project, we did not know which CERTs exist and what their exact functions were. This was the first information we needed. We obtained the necessary information by interviewing Jan Meijer and Xander Jansen of SURFnet-CERT[2]. Jan and Xander are employees of SURFnet and members of SURFnet-CERT. Because they are active for many years within SURFnet-CERT, their knowledge of CERTs is valuable to us. The results of these interviews are described in the section CERTs.

Next, we analyzed what information in which way has to be communicated in case of an emergency. We decided to do basic research on the organizational problems (see section Organizational problems). This information is also obtained by interviewing Xander Jansen.

To create a solution, or a direction towards a solution, a technical communication infrastructure is needed. To focus on usable technologies, we stated a list of requirements, see section Requirements. Only technical solutions which initially came near our requirements are further examined.

The possible technical solutions are described. We organized a brainstorm session and concluded there were five possible suitable technical solutions. Per solution, we checked it against the requirements and did research, by interviewing involved persons and by browsing the Internet for information.

For the first possible solution, a TETRA network, we did research on the Internet and had contact with Teus van Houwelingen of the C2000 Emergency Network. We also had contact by email with the Ministry of Interior and Kingdom Relations (MinBZK[3]).

The information for the second technical solution, is obtained by an interview with Marcel van Apeldoorn, employee of the KPN Emergency Network[4] department.

For information on the third possible technical solution, we did research on the website of the VRZA (the Dutch Association of Radio Amateurs[5]) and the website of DARES (Dutch Amateur Radio Emergency Service[6]).

Information on WiMAX is obtained by browsing the Internetsite of the WiMAX forum[7].

For obtaining information on satellite communication, we arranged an interview with two employees of K.S.C.[8]. This company is a supplier of satellite phones in The Netherlands, Germany and Belgium.

After researching organizational problems and possible technical solutions, a solution direction had to be described. We combined information from interviews with the technical solution which fitted our requirements best. This resulted in the recommendation of creating agreements between CERTs and the recommendation to set up a communication plan.

Due to the short time available for this research, we had no possibility to develop a communication plan. All problems which we did not research are described in the section Future Work.

1.5 Literature

Literature study is done by searching for existing articles and research on different libraries:

- Citeseer
- CiteULike
- Gigablast
- Google scholar
- Science Direct

Chapter 2

CERTs

With the expansion of the Internet to a worldwide network, security of this network became a real problem. Security incidents on one node may affect other nodes, which may be on a different geographically location. The Internet is not geographical bound, but the availability of this global network depends on different organizations of different nations working together. This situation is difficult as everyone has to use the same technology and has to agree on some rules how to operate the network. This structure works surprisingly well and there is not even an official hierarchy present to govern this. Organizations which are responsible for different nodes in the network are in frequent contact with each other about e.g. security incidents. From these organizations, groups of employees formed a team which responds to security threats and incidents. They also have contact with other similar groups from other organizations to exchange information about these security threats. These organizations were not asked or dictated to from those groups, but they were created by self organization.

These organizations are called CERTs (Computer Emergency Response Team) or CSIRTs (Computer Security Incident Response Team). From now on we only use the term CERT. CERTs originate from around 1988 when the DoD (U.S. Department of Defense) network was attacked by a worm. In response to this incident, the DoD collaborated with other communities connected to this network to solve the problem. After this incident, The DARPA established a CERT in order to address these problems. Since then, other CERTs have risen.

CERTs consist of a group of people from one or more organization(s), which work together to manage the security incidents occurring on the network they control. The employees are often not dedicated to this task, but work in a rotating shift apart from their daily work. A well trained CERT member is an expert on his task, understands incoming reports and has connections to other organizations which can solve the problems on the node the CERT is responsible for.

For this research project we only identify some organizations which are known to SURFnet-CERT. We interviewed Xander Jansen, member of SURFnet-CERT to identify the tasks of this particular CERT and a possible existence of a hierarchy. According to Xander Jansen there is no official hierarchy between other CERTs but maybe future research proves otherwise. The structure can be identified as informal, which makes it hard for outsiders to understand its structure.

For example, the Dutch GOV-CERT monitors security incidents in The Netherlands. They are not responsible for the Dutch IP-range, but monitor security risks. We assume they are not directly involved with other CERTs, but information is exchanged on a voluntary basis. In

some situations, a formal structure is present. SURFnet-CERT is a organization which only monitors its own IP-range. The University of Amsterdam (UvA) is connected to the internet by SURFnet. Below this we find organizations as OS3 (our educational unit) which are responsible for their own IP-range. For example, if there is a problem with a node which belongs to OS3 and it is reported to SURFnet-CERT, this report is forwarded to UVA-Cert which forwards it to OS3. Because OS3 and UvA-CERT have a contract with SURFnet, they are responsible for their own IP-range and must act accordingly. In this situation we identify a structure between SURFnet, UvA and OS3 which is not informal but dictated.

Not all CERTs are capable of solving an incident directly. A CERT can also be a coordinating point like SURFnet-CERT. It does not take direct action on incidents but contacts the person(s) or organization(s) which can solve the problem. Such a CERT does not correct problems, it manages them. For instance, SURFnet-CERT has connections with Network Operation Control (NOC) which controls the physical network of SURFnet. Network Operation Control is also part of the SURFnet organization; however they work separated from the SURFnet-CERT group.

CERTs are also a source of information for each other. Knowledge about possible threats or other relevant information is distributed across the CERTs through mailing lists or by personal informal contacts. By distributing this knowledge, security incidents and other problems may be prevented.

An example of an organization which distributed knowledge is FIRST (Forum for Incident Response and Security Teams). FIRST was launched only a year after the establishment of the first CERT. FIRST is a platform on which different CERTs - which are members of FIRST - exchange information about security-related vulnerabilities; FIRST itself is not a CERT. SURFnet-CERT and GOVCERT for example are members of FIRST. Members are added by a procedure called Trusted Introducer; this means CERTs which are already a member of CERT introduce other CERTs to this FIRST network. The new CERT is trusted by the already trusted CERT and can contribute to exchange information about security related problems. The members of FIRST are sharing this information via mailing lists and organized events. With this information, CERTs can react to incidents.

An everyday problem for example might be a computer sending spam attached to the node which a CERT monitors. If the CERT receives a report about this specific computer, the CERT or person responsible for this node can be contacted to solve the problem. Each problem reported to SURFnet is stored in a ticket system called AIRT[9]. Tickets can be forwarded to NOC, other CERT members or CERTs like UVA-CERT. These problems are mostly not critical for the functioning of the network so they can be managed by email or the AIRT ticket system.

In case of a severe security incident, CERT members may have to communicate with each other to address the problem. If this incident affects the availability of the network (Internet), an emergency communications channel has to be used to be able to communicate. At SURFnet-CERT this is currently done by using mobile telephone and pagers. Other CERTs also communicate with each other by telephone (point-to-point communication). Every SURFnet-CERT member has his own mobile phone and pager and is twenty-four hours a day reachable during duty.

Chapter 3

Organizational problems

An incident like the total failure of the Internet has never occurred, because the infrastructure is robust. But the possibility still exists, as stated in the section Key problem. If this scenario occurs in the current situation, no communication will be possible between the CERTs. This problem must be tackled by implementing an independent Emergency Network. Implementing such a network, can cause organizational problems.

As most CERTs communicate informally, there is no official hierarchy present between most CERT organizations. Also, there is no overall chart about which CERT is important or responsible for which part of the internet. As a result, who has to communicate with whom, what information should be exchanged and how this should be done is not clear; a communication plan is absent. Total chaos might occur when the worst scenario happens.

In the section Technical solution we describe a point-to-point communication network is needed. By absence of a clear communication structure, it is not possible to set up a point-to-point Emergency Network – it is not clear who should communicate with whom in case of emergency.

Chapter 4

Technical solutions

In this chapter, possible technical solutions or directions to a possible solution to our research question will be covered. The possible technical solutions mentioned in this section are described apart from the organizational problems. In order to distinguish a solution from a non-solution, we stated a list of requirements.

In the worst case scenario, the Internet, the telephone network and the power network are all down. In many emergencies, cascading failures are seen. This is the effect of one incident causing another. When a serious emergency occurs, people will try to use regular telephone communication networks, which causes these networks to fail due to their limited maximum capacity. When telephone networks reached their maximum capacity and the Internet is not available, it is possible regular power is also not available. Even in this case, the Emergency Network has to work which can be done by implementing a backup power supply. Also the network has to be completely independent of the Internet and its underlying technology.

The requirements are stated to ensure a possible solution does not fail in case the worst case scenario strikes. When a technical solution matches all items from this list, its possible this solution can be used for an Emergency Network.

Requirements

To make sure a solution is a possible answer to our research question, all solutions found will be checked against the following requirements. The technical solution has to be:

Scalable
The solution may intentionally be realized to serve a small geographical area, however, when this area is expanded, the solution must be scalable; it has to be possible to create new connections to the Emergency Network.

Flexible
Because CERT members tend to be mobile, the solution should also be portable and easy to deploy. A battery unit should be provided because it must be independent from regular AC power.

Affordable
Describing the term affordable for multiple CERTs is not possible; each CERT has an amount of money and time, which they may invest in the Emergency Network. We assume the Emergency Network will be used very rarely. Expensive systems are for this reason not possible to install

for the CERTs. The costs of the Emergency Network have to be reasonable and justifiable towards the organization of which the CERT forms a department.

Physically separated from the Internet
When large problems cause the Internet infrastructure to fail, the Emergency Network has to be independent of it. In case of a serious bug in the IP protocol for example, all IP devices are affected. In this situation, all parts of the Internet may experience problems. To ensure the Emergency Network is not affected by this kind of bugs, the network has to be independent of Internet. We also recommend not to use the regular Internet protocols for the Emergency Network.

Available
When all regular communications lines – PSTN, GSM and the Internet – are unavailable, the solution must be available to its users. Even in case of total power loss.

Communication can take place in various ways. Point-to-point, point-to-all, all-to-all and by speech or data (text). In emergencies it is sufficient to only have a point-to-point voice connection, because this is currently done in the same way – using (mobile) telephone networks – and because of the self organizing structure of the CERTs. If one CERT member communicates with another CERT member, this CERT member can forward the information to another CERT member. The flow of information will stream naturally trough all CERTs. Point-to-all or all-to-all communication like a conference call is convenient but is in an emergency situation not necessary. Thus we only need a point-to-point communication solution

4.1 Solution 1 – TETRA Network

Introduction to TETRA

Terrestrial Trunked Radio (TETRA) is a digital trunked mobile radio standard developed by the European Telecommunications Standards Institute (ETSI[10]). The air interfaces, network interfaces as well as the services and facilities are specified in sufficient detail to enable independent manufacturers develop infrastructure and radio terminal products that would fully interoperate with each other. For example, radio terminals from different manufacturers can operate on infrastructures from other manufacturers[11].

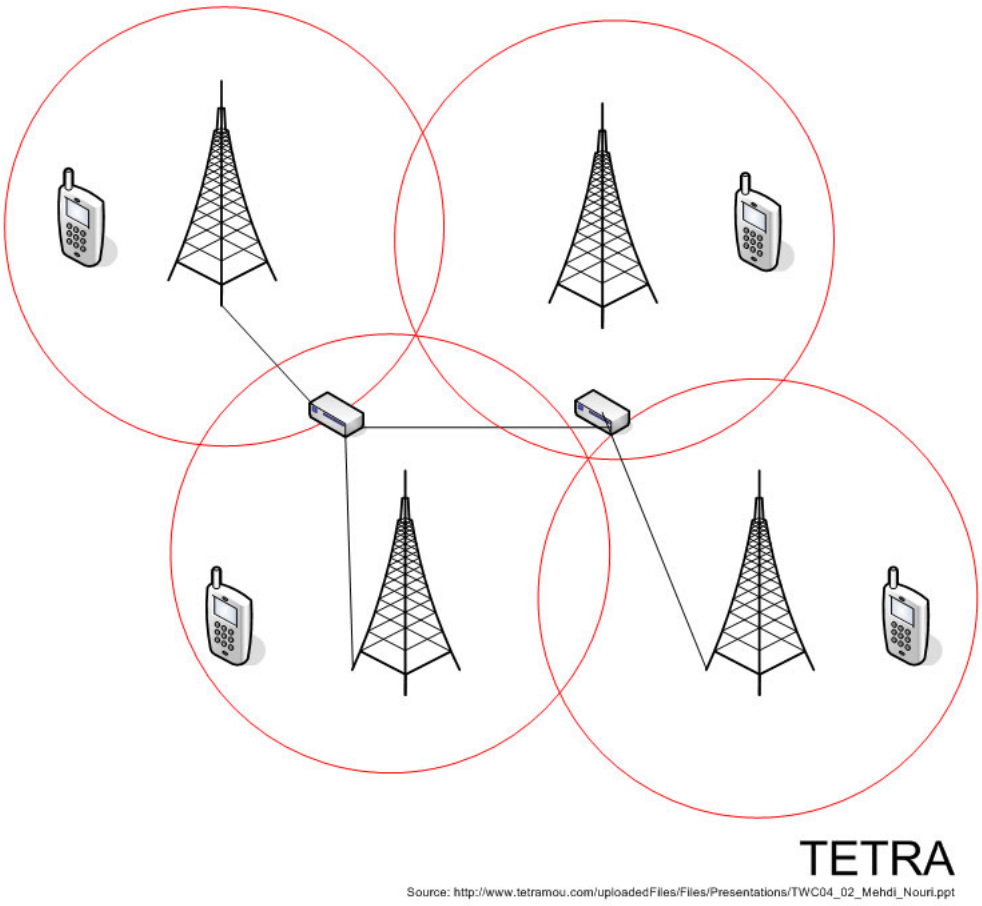

Figure 4.1: Example of a TETRA network setup. The network is based on masts – connected with cables – and mobile communication units.

C2000

The C2000 Emergency Network is a Dutch network, which is being used in case of an emergency by police departments, fire departments and medical departments. On 26 October 2005, the Dutch C2000 and the Belgian ASTRID networks have been connected for an international operation between the Dutch and Belgian police departments[**?**].

We contacted the police department in Driebergen, where the C2000-management is located.

The spokesman told us it would be nearly impossible to connect (Dutch) CERTs to this network. We have been redirected to the Ministry of Interior and Kingdom Relations (MinBZK[3]), however within the remaining time for this research we could not make an appointment. See section Future Work.

MCCN

The Dutch TETRA-operator Mission Critical Communications Network (MCCN) uses the same technique as the C2000 network. However, the MCCN-infrastructure is accessible for public and uses the frequencies meant for commercial trunking (410 – 430 MHz)[14].

TETRA and our requirements

Scalable
The TETRA network is easily scalable – apart from the necessary investment – by placing new radio masts. For intercontinental communication, a satellite connection has to be established between two TETRA ground stations. Placing new devices in a TETRA network is as easy as connect a new cell phone into an existing network. On a commercial perspective it is much more difficult to scale this international. Serving a bigger area costs a lot more and placing masts in other nations requires permission from the governments. This might be difficult to accomplish. Building your own network only for this purpose is not feasible as it is to expensive to set up.

Flexible
TETRA is a network which is intended for mobile use. As long the user is in the service area, communication can take place.

Affordable
Currently there is no pricing known. The only operator of such an open TETRA network is currently not providing this information. Building an own TETRA infrastructure is not affordable according to Marcel van Apeldoorn of KPN.

Physically separated from the Internet
The TETRA infrastructure is set up as an independent network. Within this network, all devices can communicate with each other, as long as the network covers each device. The network does not need an Internet connection – however it is possible to connect the TETRA network to the Internet.

Available
A commercial tetra network is not widely available. In time this may change and research on this option should be done.

4.2 Solution 2 – KPN National Emergency Network

In The Netherlands, commercial telecom operator KPN has deployed a private Emergency Network. This network connects 6000 locations throughout The Netherlands, for example police stations, hospitals and departments of the Dutch government. Each connection to this network has been approved by the Ministry of Interior and Kingdom Relations (MinBZK). The network is tested each 6 weeks by KPN. Many customers are using the network daily. Figure 4.2 describes the infrastructure of the KPN Emergency Network, but in a simplified version.

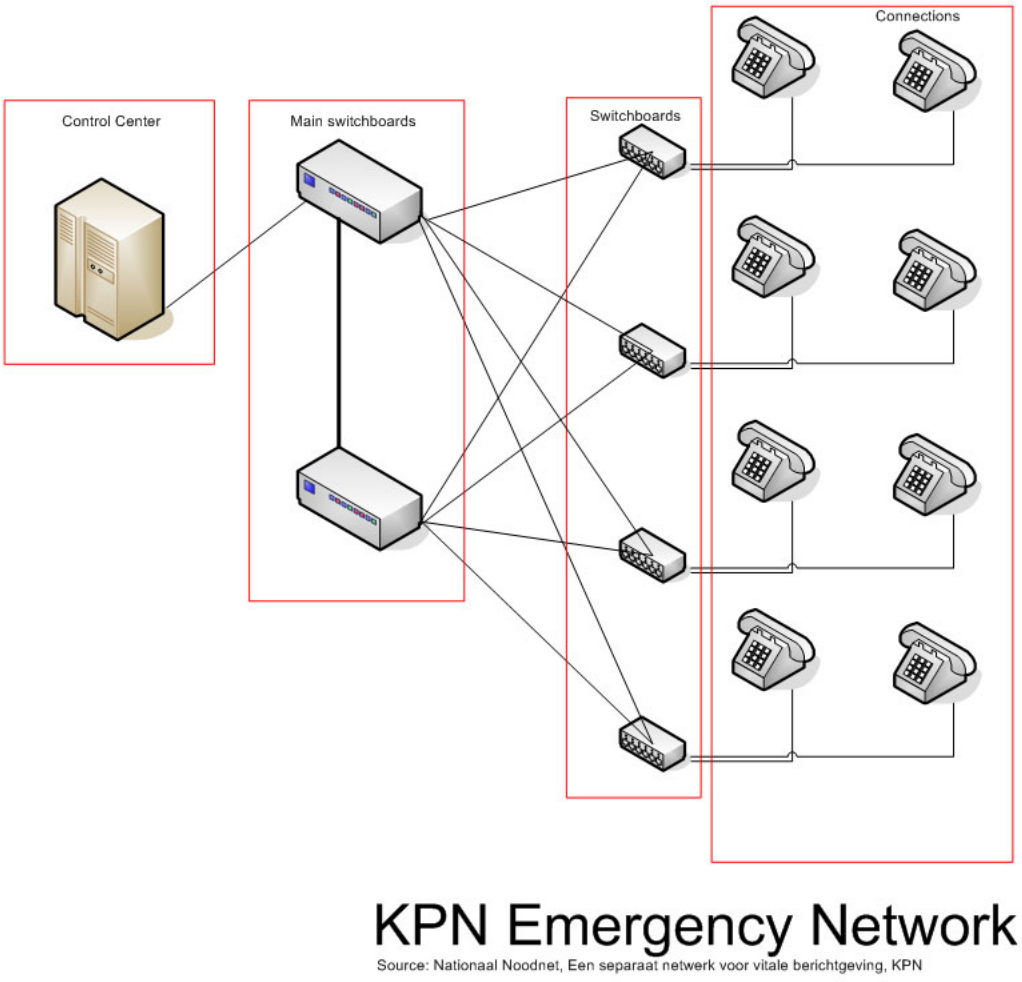

Figure 4.2: Infrastructure of the KPN Emergency Network, a simplified version.

Scalable

The KPN Emergency Network may be connected to other Emergency Networks, however some countries around The Netherlands such as Germany do not have completely separated infrastructures for communication in case of emergency. The network is not easily scalable, as all decisions have to be approved at the Ministry of Interior and Kingdom Relations. It is not easily possible to connect more than one or two countries within years with this kind of network. A request for a new number and phone on KPNs Emergency Network will take around four weeks. Once installed, the equipment is ready for use 24/7.

Flexible
In the past, mobile units have been placed in the network; when the millennium-bug should cause all systems to go down. This option was disabled after the year 2000. All locations in the network are fixed points. This network is not suitable for mobile users; a strong disadvantage for using it as an Emergency Network.

Affordable
A connection to the KPN Emergency Network costs EUR 643,89 once, plus around EUR 80 per month. However, making or receiving a call is free within the whole network.

Physically separated from the Internet
The KPN Emergency Network is completely separated from the rest of the Dutch infrastructure. The network can be used by dialing 5 numbers on any phone in the network. Each location may call all other locations. There is even a phonebook available for only the numbers on this separated network. At this moment, the KPN Emergency Network consists of 2 main exchange locations and 600 switchboards throughout the country. The network is built on the analogue PSTN-technique. At the end of 2007, contracts between KPN and the Ministry of Interior and Kingdom Relations are ending. Around this time, KPN will probably introduce the all-IP infrastructure. The KPN Emergency Network will also be converted to an all-IP network, however, completely separated from the main network.

Available
When connected, the network can handle all possible connections; it is designed especially to do so. The network will always be available when people need it. To ensure the availability, all switchboard connections in the network have alternative power sources nearby, which will switch on when the electricity network fails. These alternative power sources run on diesel.

4.3 Solution 3 – Radio

Radio frequencies can be used for various applications. The advantage of radio transmission is its transmission medium: the air. Its not dependent on a wired network or other equipment and doesnt need maintenance. This meets the most important requirement; its completely independent of the current internet network and is not based on any internet protocol.

The most common application is FM radio for simplex communication. But other frequencies are also used for voice transmission. Most noticeable users are the radio amateurs. They use free frequencies for communicating with each other and can reach other countries several thousand kilometers away on lower bands.

FM radio on the other hand does not reach very far. And the equipment to reach distances as e.g. Radio 538 is expensive and not usable without permission from the government. In fact, it may not be possible at all to get access to such a big radio mast. Solutions have to be found at a smaller scale or at the long wave band. The low wave band reaches much farther than FM and AM but the sound quality is also lower. It might not be possible to send data through the air on this band or to slow to be usable. In our situation, radio can only be used for voice communication because data transmission on a large scale would not be possible.

Out of a radio amateurs society, the project DARES (Dutch Amateur Radio Emergency Service) was established to provide support in case of an emergency or major disaster. In such a case the regular phone lines and other communications channels may be unavailable. Licensed radio amateurs on voluntary basis work together to support emergency services on a national and international level. They have over 400 amateurs spread over the entire nation available.

It might be possible to use this network of volunteers to support the internet community in case of an emergency. However, if this option is reliable, remains to be seen. Volunteers dont get paid, so theres no guarantee the network is available when it is needed.

4.3.1 Packet radio

It is also possible to use radio for transmitting data. Digital signals can be modulated to analog signals and be transmitted through the air. TCP/IP is a packet based protocol thus the term Packet radio is created. A half-duplex connection can be established by using a computer connected to a transceiver.

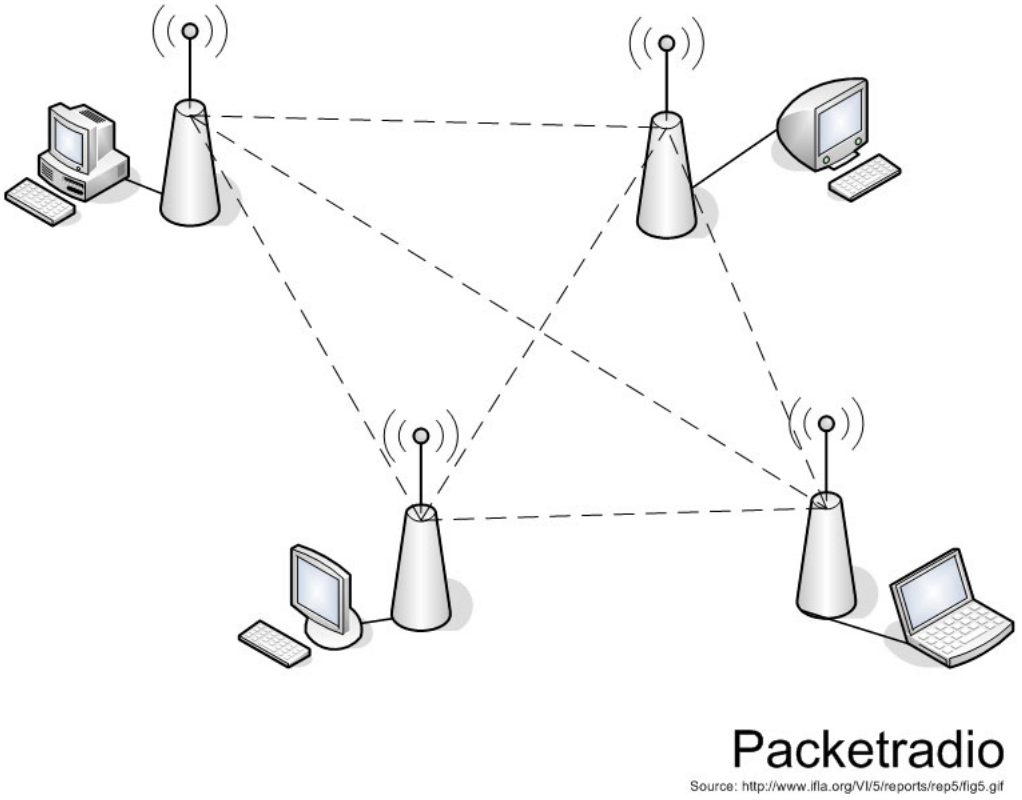

Figure 4.3: Example of an implementation of packet radio for an Emergency Network.

One downfall is the limited amount of free frequencies available. Only a few FM frequencies are free to use and it is not allowed to use strong transmitters on these frequencies. A higher sound quality translates to a higher bit rate which is necessary for transmitting large amounts of data. This bit rate is mostly limited to 9200bps which is not very fast. For text messages and maybe some text log files it should be sufficient. CERT members could communicate through e.g. a chat program and transmit data along with it.
Radio and the stated requirements:

Scalable
Radio can carry very far, but only on lower bands or with very strong transmitters. It is scalable if other countries and radio amateurs cooperate in this network. DARES might be able to set this up. Radio is not location limited.

Flexible
Portable transmitting equipment is available and easy to use. It can be used by anyone.

Affordable
Big transmitting masts are too expensive and clearance to use this kind of equipment is not easy to get. However, equipment which uses the lower band is affordable. Also radio amateurs are already equipped with these devices.

Available
The Emergency Network must always be available in case of an emergency. If the functioning of the network depends on volunteers, it might not be reliable. Also, volunteers might not be alerted fast enough to respond to a problem. This should be consulted with the radio amateurs.

Physically separated from the internet
Radio has absolutely nothing to do with the internet or internet technology if it is not used. Radio can support protocols like IP, but this can also be avoided by using other protocols.

4.4 Solution 4 – WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is not a technology, but a certification mark to equipment that meets the 802.16 standard specified by the WiMAX Forum. Its purpose is to establish a wireless link over a long distance. It is similar to Wi-Fi, but has a wider range. Like Wi-Fi, it uses free frequencies of the RF spectrum e.g. around 2.5 GHz, but this depends on the permission the nation has given. The RF spectrum is protected by the government and they have to give permission to use certain frequencies. This interferes with the adaptation of this technology.

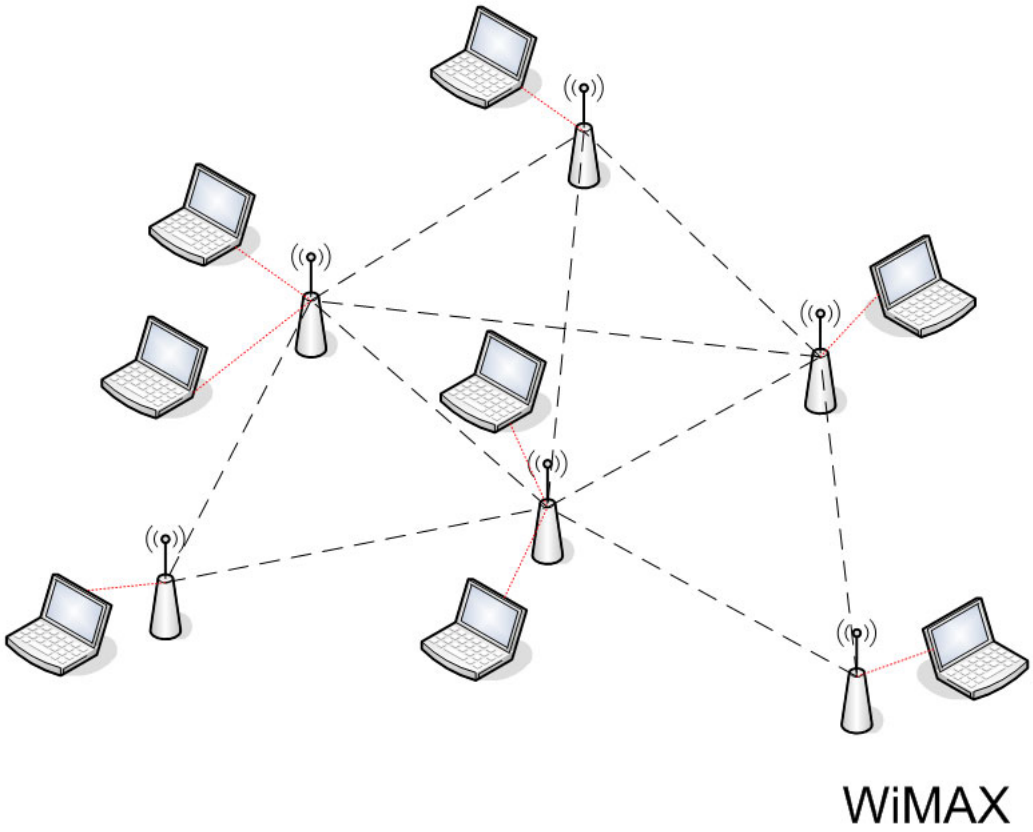

Figure 4.4: Example of a WiMAX network infrastructure, based on masts and (mobile) computers

An international and even a national covering network are not yet available. This upcoming technology looks very promising because of its range and connection speed. 10-70Mbps is possible, but 70Mbps is only achieved at very short ranges. Still, it is far more superior to GSM services, for example. Commercial companies are currently conducting tests on how this technology can be used and how it is applicable to a large geographical area. For instance, the Dutch company isence is already building a WiMAX network, but its a long way from becoming nation covered. If WiMAX comes widely available to the public, it should be a very interesting solution for our problem. Of course we cant say how dependent this network will be on the Internet because that is the responsibility of the network operators. WiMAX and the stated requirements:

Scalable

WiMAX masts can be placed everywhere so it should be technically possible to limitlessly extend this network. It is possible to use WiMAX geographically independent if there are enough masts.

Flexible
For mobile CERT members, it should be possible to access the network like the GSM network today.

Affordable
Building your own WiMAX network is too expensive for our problem. If a commercial network comes available, it is more likely affordable.

Available
WiMAX masts should always have a backup power generator. This way, the network will never go down. If a WiMAX network is tied to the internet, it might also become unavailable in case of an incident. It is extremely important the network still functions if the internet becomes unavailable.

Physically separated from the internet
WiMAX can be separated from the internet, but likely it will be connected in such a way it will also fail in case of an incident. A WiMAX network without an IP protocol might not be cost-effective to setup[7].

4.5 Solution 5 – Satellite communications

Communication via satellites is possible since around the 1960s. Nowadays, two types of networks can be distinguished: LEO and GEO satellites.

Low Earth Orbit (LEO) satellites are up to 1,500 kilometers from the earth surface. These satellites are moving constantly around the earth. Geosynchronous satellites (GEO) are stationed at around 35,000 kilometers from the earth surface. Due to this altitude, the satellites are moving synchronously with the earth; the satellites never change location relatively to the earth.

GEO systems require antennas to be pointed directly towards a satellite, and are less effective in mobile use than LEO systems. Omni antennas are used at LEO systems. This type of antenna requires an 80% clear view of the sky. Globalstar and Iridium are LEO satellite networks. At this moment, the Globalstar network counts 68 satellites. In March 2007, 8 satellites will be added. Thuraya is a GEO satellite operator, which uses only one geosynchronous satellite[15].

Because of the coverage of the described networks, we will focus on the Globalstar network as a solution for an Emergency Network. The network is connected to the PSTN infrastructure, however it is independent of it.

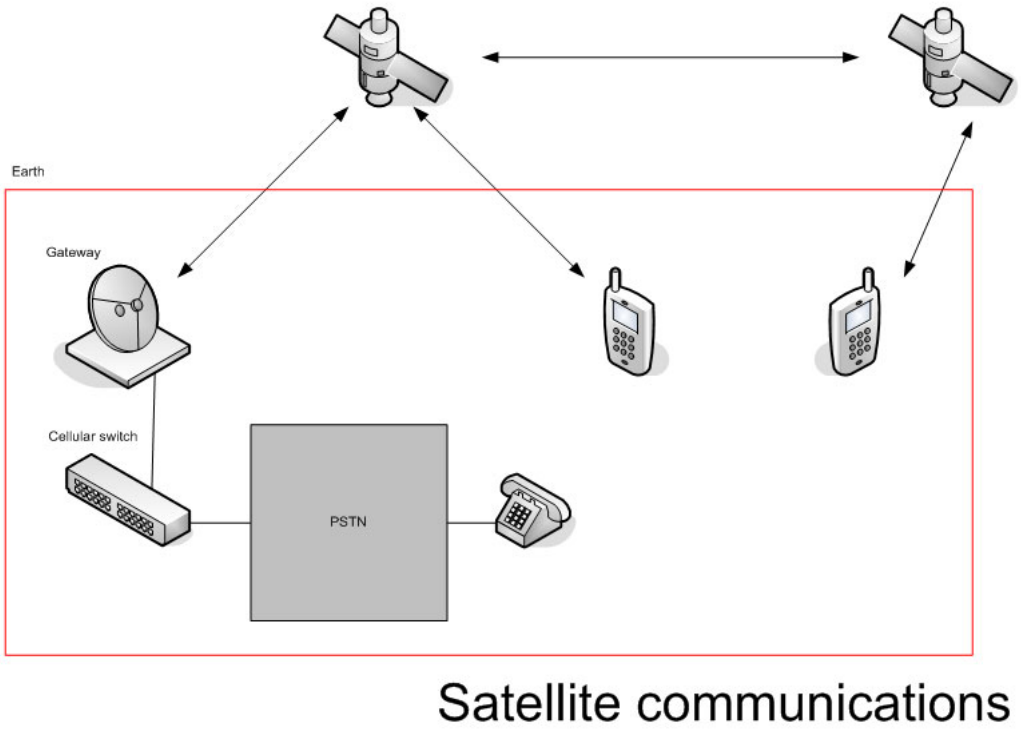

Figure 4.5: Example of communication by satellite.

Scalable
The Globalstar network is the only satellite network with worldwide coverage. Thuraya only offers satellite telephony in Europe and the Middle East. It is not possible to use Globalstar phones on the Thuraya network, or vice versa. Because of the small coverage of the Thuraya network, the Globalstar network is the best choice.

Flexible
With a satellite phone, it is possible to call from nearly all places on earth, as long as the phone has a clear view to the sky. For mobile CERT members, mobile satellite phones may be purchased.

Affordable
On the Globalstar network, the costs for a mobile satellite phone are EUR 1500 once. Per month a subscription fee of EUR 20 per connection will be charged by the operator. If the phone is not used, there are no additional costs. When calling, a fee of EUR 1 per minute will be charged.

Physically separated from the Internet
The satellite communications network is not depending on the Internet, however via some satellite devices – such as the Nera WorldPro 1000 – it is possible to access the internet. When the Internet (partially) fails, the satellite network stays available.

Available The satellite communications network is always available. However, in times of war, an enemy may interfere with the satellites, making communications impossible. Satellite communications also can be shut down by the operator. When using satellite telephones as devices for a CERT Emergency Network, alternative power sources must always be available in case of total power loss.

Chapter 5

Solution direction

By listing all requirements per solution, the best solution can be chosen from all described technical solutions.

5.1 TETRA

The TETRA network infrastructure is very flexible. The network is completely suitable for mobile units. However, the flexibility is based on the network coverage. This coverage needs a large number of masts. Building an own TETRA network is too expensive. The current pricing of units and subscription fees are unknown. The scalability of this network type is very poor, as agreements have to be made with other countries to place the necessary extra ground masts.

5.2 KPN National Emergency Network

The KPN National Emergency network is cost-effective, easy to install - as it is like a normal PSTN phone line - but not very scalable. Other countries do not have a separated network like this one. The KPN Emergency Network is also not flexible; there is no possibility to connect mobile units to this network. Furthermore, the Emergency Network moves to IP technology, which is as vulnerable to a security incident as the All-IP PSTN network. This option might be a good solution at the present time, but as KPN has stated it moves to an all IP network by end 2007.

5.3 Radio

Radio can in theory be very scalable, but this is limited to the number of volunteers that can manage a node in the network. This is not easily done, especially international. Therefore the scalability is not very good. However, it is always available and is a completely separated network. The drawback of being not very scalable is too big to choose this method. Radio networks are depending on the effort amateurs put in it. However, for an Emergency Network, it is not the intention to rely completely on professional amateurs; the availability is not guaranteed by this people.

Packet radio might be too slow to be usable because of its low data rate (9600bps max with a good FM signal) and it is not usable for point-to-point voice transmission. However, if all the requirements were met, it might have been a good alternative even if you only can use text messages.

5.4 WiMAX

WiMAX is an upcoming technology and not widely implemented. Therefore it is not useable at the present time. You can set up your own network, but this is too expensive; the distance of the signal is limited, so you need a lot of masts to cover large areas. It is expected the commercial networks which will come available are based on IP technology as it will likely be used for internet access on mobile devices. WiMAX is for this reason not a separated network and thus not a viable option.

5.5 Satellite communications

Communication by satellites is very scalable; the satellites of the Globalstar network cover almost the complete earth. Also, this way of communication is very flexible. Mobile units can access the satellites, and new connections to the network can be made quickly. The price of satellite (mobile) phones and their subscription fees for accessing the network are reasonable, see chapter Satellite communications. The satellite operator is completely independent of the internet. There is a link between the satellite network and the Internet, however the satellites are not relying on the IP protocol themselves. The satellites network is always available; only during war, satellites might be disabled.

The following table represents the final score per solution of all stated requirements.

	Scalable	Flexible	Affordable	Separated network	Available
TETRA	+	0	--	+	+
KPN Emergency Network	--	-	0	-	0
Radio	-	+	++	++	+
WiMAX	+	0	-	-	-
Satellite	++	++	+	+	++

Figure 5.1: Final scores per solution per requirement. Scale from – to ++, where 0 is neutral.

Because communication by satellites matches all of our requirements, this is the best technical solution available at this time. In order to use this solution, every one who has to communicate in case of an emergency has to have a satellite phone unit either mobile or a ground unit. In a future communication plan, all phone numbers are listed and this is updated frequently. This plan also contains procedures, which have to be executed during an emergency. This way a CERT member can always contact a member of another CERT who also has a connection to the Emergency Network.

5.6 Example of satellite communications as an Emergency Network

An Emergency Network can be established using satellite communications. Via satellites, point-to-point communication is possible. Additionally, the network meets all of our requirements. In the section Organizational problems, we described the absence of a communication structure between CERTs in case of an emergency.

For this example, the communication between SURFnet-CERT and SURFnet NOC in case of an emergency will be described. In case of a serious network failure, a SURFnet-CERT member can use his mobile satellite phone unit to call a NOC employee who also has a unit. If necessary, both parties can contact other CERTs connected to the Emergency Network to solve the problem, see figure 5.2; the figure is simplified, not all CERTs are represented. The procedure of contacting and the phone numbers are stored in a communication plan.

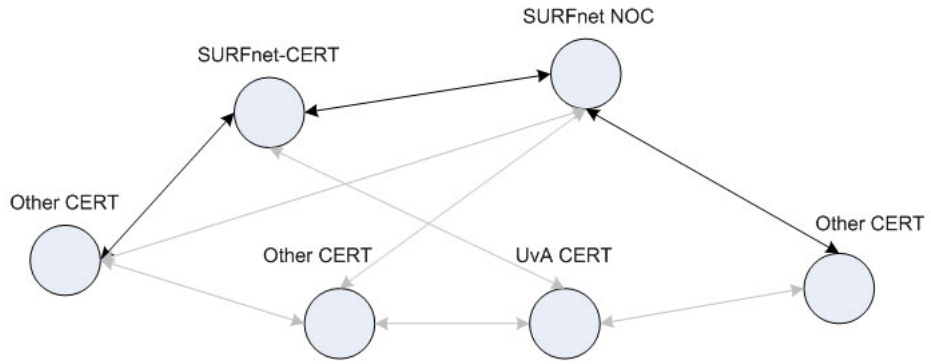

Figure 5.2: Communication in an Emergency Network, simplified. Black arrows represent real communication, grey arrows represent possibilities to communicate

For every arrow in figure 5.2, an entry in the communication plan is needed. This clarifies who to call (procedure) and which number is linked to which CERT.

Next, we describe the costs of an implementation of satellite communication for 6 mobile units. EUR 1.500 per CERT makes a total EUR 9.000 total non-recurring costs. Per month, EUR 20 per CERT is charged. This makes a total of EUR 1.440 per year. In case the Emergency Network is used, the costs of calling by satellites phone are EUR 1 per minute.

5.7 Proof of Concept

Setting up satellite a Proof of Concept (PoC) of satellite communication is too expensive for this limited project. However, we made some test calls with mobile satellite phones supplied by K.S.C. The quality of the conversations turned out to be good and the delay of calling by satellite was negligible in comparison to GSM telephony.

5.8 Implementing a satellite Emergency Network

To deploy an Emergency Network, the following steps have to be taken:
1. Organize a meeting with at least 2 CERTs
2. Create agreements on how the network is set up
3. Describe these agreements in a communication plan
4. Connect all participating CERTs to the satellite network
5. Add all CERT names and numbers to the communication plan
6. Update and distribute the communication plan on a frequent basis
7. Get more CERTs interested to participate in the arisen Emergency Network; start again at step 1

Chapter 6

Conclusion

Which ways of communication can be used for the CERTs for mutual communication when the regular communications network (Internet) fails?

After examining all possible solutions for an Emergency Network, our conclusions are the following. Communication can be done best with satellite communication, which is a completely separated network and the network is always worldwide available. Because there is no communication structure agreed between CERTs in case of (partial) failure of the Internet, a communication plan is needed. This plan must contain all procedures and (mobile) satellites phone numbers of the participating CERTs.

6.1 Recommendations

In order to successfully deploy the solution, first a few CERTs have to implement this technology. Hence, if one sheep leaps over the ditch, all the rest will follow. Other CERTs will notice the existence of the Emergency Network and may join it

Chapter 7

Future Work

During this project we researched different technical solutions which may or may not be usable for an Emergency Network.

Implementing an Emergency Network requires a communication plan which is agreed on by all CERTs who participate in this network. This requires more research which was not part of this project. CERTs should also address this problem as it is not a priority at this moment; this requires arrangements with other CERTs.

Other technical solutions like WiMAX should also be further researched on their potential. It is possible this proves to be a better and cheaper solution in the future when it becomes widely available. In the case of building an Emergency Network on WiMAX technology, CERTs should realize this is an IP network, with the danger the network is probably not completely separated from the internet.

Another possibility is opening a dialog with amateur radio societies on how they can help establish communications if the regular methods are unavailable. However, amateurs may not be a good alternative for an always-available satellite network. Notice that crossing the oceans may need satellite communications in the end, when using packet radio technology.

The security of the solution has to be researched. This is part of the implementation of the solution, which is not part of this research. CERTs should evaluate if the Emergency Network must be secured and which requirements are needed.

Bibliography

[1] CISCO, *Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service*, http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

[2] SURFnet, *Website*, http://cert.surfnet.nl/home-eng.html

[3] Ministry of Interior and Kingdom Relations (MinBZK), *Website*, http://www.minbzk.nl/bzk2006uk/

[4] KPN, *KPN Emergency Network*, http://www.minez.nl/content.jsp?objectid=150156&rid=149798

[5] Dutch Association of Radio Amateurs, *Website*, http://www.vrza.org/

[6] DARES (Dutch Amateur Radio Emergency Service), *Website*, http://www.dares.nl

[7] WiMAX Forum, *website*, http://www.wimaxforum.org

[8] K.S.C., *website*, http://www.kscehv.nl/

[9] Application for Incident Response Teams (AIRT), *Website*, http://www.surfnet.nl/info/diensten/beveiliging/airt.jsp

[10] European Telecommunications Standard Institute, *Website*, http://www.etsi.org/

[11] TETRA Memorandum of Understanding, *Website*, http://www.tetramou.com/

[12] TETRA Architecture and Interfaces, *Presentation*, http://www.tetramou.com/uploadedFiles/Files/Presentations/TWC04_02_Mehdi_Nouri.ppt

[13] TETRA Release 2.0 Overview, *Presentation*, http://www.tetramou.com/uploadedFiles/Files/Archive/9_TWC03_TETRA2_Overview.ppt

[14] C2000, *Description*, http://nl.wikipedia.org/wiki/C2000

[15] LEO vs. GEO Satellites when used with Mobile Satellite Services, *Website*, http://www.globalcomsatphone.com/globalcom/leo_geo.html