2. CORS-Tr DATA COMMUNICATION

A GNSS network consists of several GNSS stations interconnected by reliable communications to enable real time computations and control. Each station has a cabinet which contains a receiver, an antenna, communication devices, small data storage, power supply, accumulator and so on. In most cases a computer is installed additionally for data transmission and control. It also contains a user interface which is required to configure and maintain the network. This may be realized remotely for example by radio communication, mobile phones or via internet connection.

In Turkey Turk Telekom Backbone for CORS-Tr data communication is available. CORS-Tr system has VPN tunel between reference station and control center as primary data communication and 3G APN tunnel as secondery. User connections are supported by APN tunnel by all three GSM Operators in Turkey. And all RTK correction send to user via an APN tunnel. Data communication structure is shown in section 3.3 Networks topic (Figure 3).

3. CORS-Tr SECURITY ISSUES

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cybersecurity. Elements of cybersecurity includes [2]:

- Application security
- Information security
- Network security
- Disaster recovery / business continuity planning
- End-user awareness and education.

3.1 Applications

In CORS-Tr system, we have Network RTK correction, networks DGPS correction, web online processing services and RINEX datas to provide our users. All applications are shown below.

Figure 1.a: TUSAGA-Aktif applications

CORS-Tr Main Applications			
RTO	Real Time Output	İScope	Realtime Visualization
TDC	Dynamic Control	TOP	Web Online Proces.
VRSNet	Corrections	TRI	Rover Integrity
TIC	Instrum. Config.	TED	Ephemeris Download.
TDS	Data Shop	TIM	Integrity Manager
TAC	Accounting	TSM	Streaming Manager
Atmo	Atmos. App.	TTG	Transformation Mang.

Figure 1.b: TUSAGA-Aktif applications

3.2 Information

CORS-Tr system works with 3 SQL databases which are ***TPPDB*** contains the history of the system, ***TPPAccounting*** contains the accounting information such as user, subscriptions, sessions, etc. and ***TPPDBRoverIntergrity*** is a separate database for the rover integrity results. Additionally we have RINEX datas, control center camera records and callcenter recorded voices.

No	Information Type	Resp. Unıt	Backup Period	Where	Keeping Duration	Time Deliver to Achieve
Y1	RINEX 1 Sec.	Geodesy	Weekly	Geodesy	3 Month	--------
Y2	RINEX 30 Sec.	Geodesy	Monthly	Geodesy	1 Year	End of the Year
Y3	Database Logs	Geodesy	Monthly	Geodesy	Endless	End of the Year
Y4	Control Center Camera Records	Geodesy	Monthly	Geodesy	6 Month	----------
Y5	Callcenter Recorded Voice	Data Mang.	Monthly	Geodesy	1 Year	----------

No	Information Type	Resp. Unıt	Achieving Period	Where	Keeping Duration	
A1	RINEX 30 Sec.	Data Mang.	Yearly	Data Mang.	10 Year	
A2	Database Logs	Data Mang.	Yearly	Data Mang.	Endless	

Figure 2-TUSAGA-Aktif Information to be backed up and to be archieved

3.3 Networks

We have two different networks in Geomatic Department. One of the network is CORS-Tr control center network, called

METRO. Other is General Directorate of Land Registry and Cadastre (GDLRC) wide area network, called TAKBIS. TAKBIS network is under the responsibility of IT department of GDLRC. COSR-Tr network is an independent and special network. There is no connection or relation to TAKBIS network.

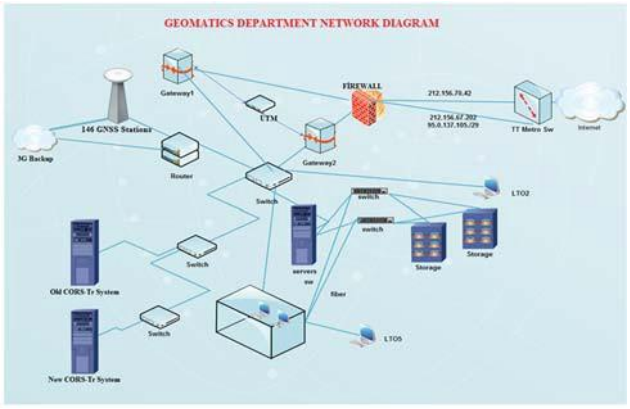

Figure 3- Geomatic Department Network Design

3.4 Our Experience and Business continuity planning

Of course CORS softwares including operating system and hardware, normally has their own firewall and some security issues with many applications. But we faced many problems since CORS-Tr established and these problems are briefly described below.

Lack of IT Personnel: Only Surveying Engineers and Surveying technicans were avaliable to operate CORS-Tr system, user membership and payment issues and to support users. There wasn't any IT staff to control system in case of a technical problem. Highly qualified geoinformatics personnel dealt with technical problems such as system freezing, communication bandwidth saturation or even exchange of broken hardisk.

DDOS Attacks: In summer season of year 2013 which mapping applications on the field by using CORS-Tr are very dense, we faced a very hard DDOS attack by an unknown source. DDOS attacks were continued for approximately 3 months, every day between 10 a.m. and 12 a.m.

Awareness of Internal Users: Internal system users who use computers that has virus, malware, trojan.etc. Internal users who used virus contaminated USB to connect system servers or unsafe remote desktop connection caused danger for the system. Unfortunately Institutional anti-virus system was unable to protect CORS-Tr system. Internal user's awareness on security issues should be increased.

Awareness of External Users: Some external users somehow adjusted their GNSS instrument settings to send more than five request in a second to connect CORS-Tr system. These requests interrupted other user connections and overloaded data communication bandwidth. Some external users shared their own password and user name with other users which cause conflict between the users. Another problem caused by external users is unnecessary attempts for connection. Although their term has finished many external users, try to connect to the system.

4. IMPROVEMENTS

Measures taken to establish trusted service in CORS-Tr system usage in terms of security requirements after experienced problems are:

- One specialised Computer Engineer and a specialised Electric and Electronic Engineer to operate COSR-Tr technical side were employed.
- UTM security device purchased for prevention from DDOS attacks. No DDOS attack detected since 2013.
- Directive about personal computer maintenance including software related security risks issued. Then data back-up and archiving directive with our employees in Geomatic Deparment issued.
- GNSS reference station data and information are stored in an SQL database. User information and activity log data are stored in another SQL database. These two databases and other related data have been started to be backed up ever day regularly according to department directive.
- Data comunication bandwidth enlarged from 20 GB to 50 GB after the realisation of unexpected external user dense connection activity.
- VPN tunnel established between reference station and control center as primary data communiciation and a 3G APN tunnel as secondary. Reference stations data storage capacity increased.
- Current software updated to latest version including required moduls such as Realtime Visualization, Atmosphere, Transformation Generator and Online Web Processing.
- New hardware provided according to updated software requirements.
- Main applications like Network RTK correction, networks DGPS correction and provision of RINEX data to the our users and SQL databases are protected by extra security software for cyber attacks.
- In CORS-Tr network, servers and end points are protected by a software from inside and outside cyber attacks.
- User awareness of CORS-Tr usage was increased by 444 call center, SMS message, Social Media and Local trainings. And also customer satisfaction are surveyed regularly.

5. CONCLUSION

At the beginning of TUSAGA-Aktif project we thought that project was considered geodesy related works only. Today we understood that TUSAGA-Aktif is not only a geodesic related work but also Information and Communication Technology work.

As a result today CORS-Tr have trusted data communication infrastructure, protected information and services by updated software and hardware including security devices and has more powerful user support.

REFERENCES

[1] URL1:http://www.sage.unsw.edu.au/currentstudents/ug/projects /Gowans/Thesis/What_is_it.html

[2] URL2: http://whatis.techtarget.com/definition/cybersecurity