SPARTA

5G network and elections

pros and cons

Prepared by	A. Meirāns, M. Švirksts, K. Makbets, K. Kalniņš, A. Mežciema, I. Toleika
Reference	SPARTA (Strategic programs for advanced research and technology in Europe) T-SHARK (Full spectrum Cybersecurity Situational Awareness)
Issue	1
Revision	Final
Date of iss/rev	18.01.2022
Classification	PUBLIC

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

Executive summary

A research paper addressing the needs for technical capacity mapping of those practitioners and decision makers working towards election process democratization. A particular focus is given for assessing the new generation – **5G mobile network enabled features for procedures associated with election digitalization.** Among new functionalities that 5G technology brings it may serve to society by improving election independent and GDPR inclusive monitoring. This feature allows to identify a potential meddling by third party as a mismatch of voters activity already at real time sequence hence reducing election process vulnerability to misinformation. False claims of stolen elections have soared within a last decade and requires a proper digital means to counterweight with factual indicators. Furthermore, from election resilience perspective the technology enables scalability for serverless user side/edge or distributed computing capacities and cross border integration for election cybersecurity.

Study was done as part of SPARTA T-SHARK program, challenging election processes and relation with hybrid cyber activities, in particular disinformation campaigns, fake news in combination with targeted cyber operations, varying in scope, scale, duration, intensity, complexity, sophistication and impact. T-SHARK program works under umbrella case that covers election process, starting with the announcement of candidates and ending with elections results.”. As a benchmark case the 2021 Latvia municipal election was selected for monitoring both network and election activity highlighting correlation and requirements for further capability extension and development from mobile network operator perspective in line with deployment of 5G. The case served to validate the hypothesis, that election activity can be monitored using mobile provider network activity data.

Overall, the main report has 34 pages complimented with three annexes on 24 pages. In the annexes the report is supplemented with answers from three expert interviews in which the experts answered five questions, four descriptions of real-life cyber security use cases – including Latvian Municipality Elections 2021 and overview of Estonian as only country in the world e-elections experience - and more in-depth elaboration of some specific 5G technical parameters. Also, the document has 28 figures.

Main part of the report consists of six chapters – introduction, use cases analyses, elections from MNO’s big data perspective, 5G added features and their impact for elections, identified elections improvement process use cases and 5G usability within the use cases and at the end conclusions are provided.

LMT study and the report provides a current snapshot of 5G feature capabilities, and it`s potential for resilience building against disinformation and election interference. Among those features are enablers for following capabilities:

1. Release 16 network slicing features, it becomes possible to prepare a **separate network slice** for devices and systems used in election process (e.g. counting votes, registering voters etc). This would guarantee a dedicated traffic to these devices, to protect from different Denial of Service attacks. This also protects devices, separating them from other, public networks, improving data integrity and confidentiality.
2. More and more elections are moving towards digitalization of some sort and using more electronical devices, to reduce manual labour. Depending on exact technical solutions used in election voting process, **Multi-Access Edge computing** can be leveraged, to improve resilience against to Denial of Service attacks, such as large scale internet outages etc. as part of national ATP actors. Using Mobile Edge computing and battery powered devices (mobile devices, laptops), election process can continue using electrical devices even without internet or electricity at their local “area” (within the range of Mobile Base Station).

3. As most people are carrying their mobile phones wherever they go, mobile technologies can be leveraged to identify, how many people have connected to base station, anonymously counting people in a specific area. Thus, providing approximate number (by combining numbers from all mobile operators) of voters in a given voting station. This can help to give more context to misinformation of election vote counting, e.g. showing, that counted total votes matches amount of people in the area (approximately, no large-scale deviations). 5G can provide precise location data using 5G positioning functionality, to gather statistical data even more precisely, like going to voting stations or even specific in-door locations, e.g., voting pools. Having such statistic data can help fighting misinformation of election process at level of each specific voting station.

Overall, 5G has unexplored advantages towards implementation in election process digitalisation, even though they are partly provided by other solutions already. It was noted that an alternative solutions broader deployment would requires much larger investments at each election voting location compared with enabling of certain features at national wide 5G deployment. No doubt that 5G deployment will start in centres of large cities, and furthermore extended to rural regions where it is more expensive to maintain the network. Mobile networks already cover most territories and national wide 5G are matter of time. This allows swift and easy implementation of certain solution for election process integrity in all regions of country with reduced costs, to protect devices against the cyber threats used in election process.

Table of Content

Executive summary 2
List of Figure and Tables 5
1 Introduction 6
1.1 Evaluation of main IT challenges in election process 6
1.2 Misinformation as part of cyber warfare 7
1.3 Election process parts 9
1.4 Implications of mistakes in election process 10
2 Use cases analyses 12
3 Elections from MNO`s big data perspective 13
3.1 Election data analysis method 15
3.2 Analysis of Latvia municipal elections on 5th of June 2021. 15
4 5G added features and their impact for elections 28
5 Identified election improvement process use cases and 5G usability within use cases 33
6 Conclusions 34
Annex Nr.1 - Technical capabilities 35
1.1 Higher speeds with 5G 35
1.2 Lower Latency 37
1.3 Longer reach, better coverage 37
1.4 Slicing 38
1.5 Positioning without GPS 39
1.5.1 5G positioning: What you need to know 39
1.5.2 5G positioning and use cases 40
1.6 Multi-Access Edge Computing 45
1.6.1 Ability to communicate locally 46
1.6.2 Improved integrity via separation 46
Annex Nr2 – Elections Cases Assessed 47
2.1 2019 European Parliament election 47
2.2. USA Presidential Elections in 2016 49
2.3. Latvian Municipal Elections in 2021 51
2.4. Estonian E-elections 54
Annex Nr3 – Interviews 56
List of Abbreviations 59
List of Definitions 60

List of Figure and Tables

Figures

Figure 1 Europarlament turnout by country (2019) 13
Figure 2 Locations of monitoring points of Latvia municipal election 5th of June 2021. 14
Figure 3 Example of data activity of base station for each sector ($30^0/150^0/240^0/270^0/300^0$) orientation towards horizon within a time section of a reference day. 16
Figure 4 Election Day versus reference day activity at 24th of April at Jelgava city monitoring point. ... 17
Figure 5 Election Day BS activity at Sigulda city monitoring point. 18
Figure 6 Election Day BS activity at Ikšķile monitoring point. 18
Figure 7 Election Day BS activity at Skrīveri monitoring point. 19
Figure 8 BS user activity at Jelgava election monitoring point – Election Day versus reference and AVE/MED patterns. 20
Figure 9 Election Day activities at Jelgava city pooling stations. 21
Figure 10 BS user activity at Sigulda election monitoring point – Election Day versus reference and AVE/MED patterns. 22
Figure 11 Election Day activities at Sigulda city and district pooling stations. 23
Figure 12 BS user activity at Ikšķile election monitoring point – Election Day versus reference and AVE/MED patterns. 24
Figure 13 Election Day activities at Ikšķile and Ogre district pooling stations. 25
Figure 14 BS user activity at Skrīveri election monitoring point – Election Day versus reference and AVE/MED patterns. 26
Figure 15 Election Day activities at Skrīveri and Aizkraukle district pooling stations. 27
Figure 16 Visualization of 5G network potential for serving the elections' IT systems 28
Figure 17 Evaluation of 5G sub-technologies' influence on the three scenarios 29
Figure 18 Spectrum bands for deployment of 5G 30
Figure 19 Qualcomm. Unlicensed Spectrum Bands in 3GPP 30
Figure 20 IoT growth estimate 36
Figure 21 Potential use cases of 5G location-based services 39
Figure 22 Requirements and specific solutions of 5G location-based use cases. 39
Figure 23 The features bring 5G particular releases an overview. 41
Figure 24 5G architecture supporting positioning - top: Location service 5G SA + 4G RAN network; bottom: Location service in 5G SA network. 42
Figure 25: Reference signals for positioning. Shown are one configuration each of DL-PRS and UL-SRS. 43
Figure 26 Reference signals for positioning. Shown are one configuration each of DL-PRS and UL-SRS. 44
Figure 27: LMT team in Jelgava 53
Figure 28: Outdoors polling station in Jelgava due to Covid-19 restrictions 54

1 Introduction

Along with technology development of information systems, the threats affecting these systems has grown as well, thus creating new and previously non-existent challenges for cybersecurity. Growing digital society requires continuous advancements in digitalization of processes for integrated interaction with governance, this includes the elections as a form of democratic expression of opinion. This poses a risk from external interested parties to falsify or manipulate these interactive processes using cyber-attacks in both civilian and governance sectors increasing exponentially in recent decade. Threats aimed on election process meddling have gained new perspectives, starting from the election administrative process manipulations, through to purposeful targeted misinformation spreading using social networks and attacks on political parties' domains and mail servers. This calls for the development of new or adaptation of existing technologies to ensure the security of the critical infrastructure and software solutions.

Exploring 5th generation of cellular networks or 5G as one of the potential solutions could provide basis for secure, accountable, and transparent election process management and organization. The technology of 5G can potentially provide solutions for cybersecurity threats, risk management, and provide statistical data by the precise positioning of anonymized device data in the voting polling stations, thus eliminating our drastically reducing the possibility of election falsification. For this purpose, existing election processes, known threats, potential future threats are evaluated within current research. Theoretical explorations are strengthened by a practical experiment, to determine the cellular network big-data opportunities of identifying the activity of given elections in given election polling office.

1.1 Evaluation of main IT challenges in election process

Firstly, each step of the election process, must be critically assessed to identify and evaluate possible threats and their impact on election process. Most countries, like Latvia, have not gone beyond in-person, traditional voter identification, and paper-based processes in critical aspects of elections. However, tasks, like ballot counting, vote counting, voter counting are repetitive, and the chance of human error is considerable, despite its relative reliability. Some aspects of process could be digitalized to reduce manual labour, to reduce human error and, to some degree, create new social involvement possibilities.

With digitalization, additional resource challenge within the IT landscape arises. For example, in municipality elections in Latvia, election process is for the large part planned by Central Election Commission, while it is executed by the local municipalities. Local municipalities must have technical and human resources to ensure election process as designed. Quality network connection is a must for all locations. However, still in some rural spots, the voting locations are chosen due to availability of network connection and electricity grid, compromising on people's needs for easy access.

When approaching online voting, one of the most important challenges are balance between integrity, confidentiality, and transparency. Online voting must be secure and there must be means for verification, also that results were not tampered with, including administrators and owners of system. Full transparency of the process must be ensured, making sure all votes are traceable, that they are counted towards the right party, while maintaining full voter confidentiality.

Even with increased complexity of election process, digitalization should be approached as an important step towards improving voter activity. During municipality elections, voter activity was low at 34.01%[1]. Out of those 34.01% of voters, 12.31% or 36% of voters gave their votes before the official voting day. This is an indication, that traditional style Saturday in-person voting is not convenient. Being in-person at specific place during specific timeframe is not customary habit for a

[1] Source: https://pv2021.cvk.lv/pub/aktivitate [Retrieved: June 26, 2021]

digital age voter. Online voting should be approached proactively to improve participation, by greatly improving usability and voter experience.

During budget planning in Latvia for 2022, Central Election Commission raises alert, that there might not be enough budget, to execute current plans of parliament elections[2]. In discussion with CERT.LV, risk of insufficient election financing was raised as well. Wanting to improve current election system using modern technologies can leave election process less secure as it is now, due to budget cuts, shortcuts, and other resource issues. Latvian Central Election Commission, currently, has as few as 2 IT specialists, while additional 4 vacancies, including information security manager, are required to satisfy current needs.

All aspects, and entry points towards election process must be validated to ensure security and transparency of democracy. Every data manipulation should be done in a secure and traceable way. For example, if there is an option to change a voting location some time before the election day, such process should be assessed against vulnerabilities, that can be abused to vote in multiple locations or create new options to vote. All “entry points” must be validated.

1.2 Misinformation as part of cyber warfare

Misinformation can be viewed as one of the tools of this age to alter the mindsets of public and potentially even the results of democratically executed processes, for example – elections. This is viewed as one of the greatest threats in the digital era of information exchange, since the information is more accessible as ever before. As general population capabilities to distinguish “fake news” from legitimate, truthful information is decreasing, the manipulation of the public becomes more common. As reviewed in the publications of the International Communications Association, in the 2016 Presidential elections of USA only 29% of the polled individuals were able to distinguish the difference between “fake news” like the “Pizzagate story”, where the Clinton campaign was allegedly linked to a pedophile ring[3].

Another study from the Massachusetts Institute of Technology (MIT) also found that fake news was more commonly re-tweeted by humans than bots and, as reported in the BBC[4] article, their findings, published in the journal Science[5], included:

- false news stories were 70% more likely to be re-tweeted than true stories
- It took true stories around six times longer to reach 1,500 people
- True stories were rarely shared beyond 1,000 people, but the most popular false news could reach up to 100,000.

By this we can assume that the potential of the spreading of “false news” outperforms the “actual news” in hundredfold. This tendency is genuinely dangerous trend as it affects the turnaround of voters critical for true democracy. As the statistics of 2019 European election results[6] in Latvia shows, that the turnout for the last two elections has been under 35%, accordingly – 30.24% in 2015 elections and 33.53% in 2019 elections. This shows that with only one third of the population participating in the elections, the potential impact of the election results could be non-representable by the general population, nevertheless, the impact of misinformation can be even higher, as it needs

[2] Source: https://www.lsm.lv/raksts/zinas/latvija/cvk-nepietiekama-finansejuma-del-apdraudeta-14-saeimas-velesanu-norise.a427874/ [Accessed: October 26, 2021]
[3] Source: https://www.tandfonline.com/doi/full/10.1080/23808985.2020.1759443 “Causes and consequences of mainstream media dissemination of fake news: literature review and synthesis“.
[4] Source: https://www.bbc.com/news/technology-43344256 “Fake news 'travels faster', study finds”.
[5] Source: https://www.science.org/doi/10.1126/science.aap9559 “The spread of true and false news online”.
[6] Source: https://www.europarl.europa.eu/election-results-2019/en/turnout/ “2019 European election results”.

to address less of the general population as the oversaturation of the “fake news” are dominating the legitimate and truthful public information.

There are several identified types of misinformation:

- Election Office Hoaxes (so called photo scams) - doctored photos to intimidate potential voters and discourage election participation.
- Promoting remote voting options when they do not exist or spreading wrong information on remote voting options to decrease election participation.
- Spreading fraudulent procedural information about voting (such as misinformation on changes in election office open hours, changes in document requirements, changes in eligibility to vote etc.) again to decrease election participation.
- Spreading rumours about irregularities at election offices to raise mistrust in election process and discourage voter participation.
- Manipulated (doctored or mislabelled) photos and videos (for example, with long lines at election offices etc.) to discourage voter participation.
- False Voter Fraud Allegations and claims of widespread voting fraud (in fact, it is rare) to undermine election integrity, to raise mistrust and discourage voter participation.
- Altering actual information by implementing deepfake technology.

This brings us to question about the potential dangers of 5G and deep-fake technologies if they are used against democratic processes. The genuine information alteration in a real time (commonly known as “real time deepfake technology”), that allows to alter the true information in a matter of milliseconds, thus, giving the potential to hijack live streaming news just by tampering with the data stream latency and altering the broadcasted information with no noticeable delays to the end users, is a risk that needs to be assessed with utmost care. Solutions like “Avatarify”, as reported by Samantha Cole in the “Vice”[7] in 2020, or “DeepFakeLive”, as reported by Mikael Thalen from the “Daily Dot”[8] in 2021, can already change the appearance and the sound of a person in live video. This becomes a dangerous scenario, where politically influential person is seemingly connecting to some meeting remotely, using practically any of the online meeting solutions known to this date.

The 5G technology can provide the necessary bandwidth and latency to either hijack a remote videocall, by replacing the actual speaker to another person, just altering expressions or simple answers like “Yes/No” or “Agree/Disagree” or replacing phrases that can create advantage or disadvantage for the representatives of political force or, in the worst-case scenarios, even on a country level. By no means this is simple to achieve, however, for the serious troll farms this is a new opportunity to weaponize not only social media, but traditional media as well.

[7] Source: https://www.vice.com/en/article/g5xagy/this-open-source-program-deepfakes-you-during-zoom-meetings-in-real-time “This Open-Source Program Deepfakes You During Zoom Meetings, in Real Time”
[8] Source: https://www.dailydot.com/debug/deepfacelive-deepfake-live-streaming/ “Real-time deepfakes could bring chaos to your next Zoom call”

1.3 Election process parts

In general, there are three existing voting systems – majority election system, proportional representation system and mixed system from both systems. In the Majority system - the person with most votes shall be selected to represent the constituency. In Proportional system - political parties play a key role in creating political solutions. A reasonable number of competing parties will create more and better ideas while two dominating forces tend to be at a deadlock with inflexible positions. Finally, there are mixed election systems of both previously mentioned.

However, from the election process standpoint the main parts in democratic elections are the same, overall. The election process can be viewed as a three-part cycle:

1. Pre-election phase.
2. Election phase.
3. Post-election phase.

Each of these parts plays significant role in the election system and can be influenced by potentially threatening interested parties, internal or even from outside the state borders to gain the manipulated election result. For example, by implementing cyber-attacks or hybrid type attacks using information technology solutions to influence of affect the voters.

Pre-election phase.

Pre-election phase is the longest in the timeframe, where all preparations for the election day are being defined and carried out and are as follows:

1. Defining of legal frameworks for elections.
2. Setting the electoral boundaries.
3. Defining and carrying out election management body process.
4. Creating election management body and administration structure.
5. Political party registration.
6. Ballot qualification and printing.
7. Security measure definition and processes of the election day.
8. Voter registration and information.
9. Political parties campaign financing.
10. Campaigning of the political parties.
11. Voter education and political debates.
12. Voter list creation.

Since the pre-election phase includes a wide variety of different subprocesses, any of these processes can be manipulated by outer entities, leading to a tainted election process. In the digital age this leads to new threats, as each innovative solution in the election process creates new threat opportunities for the process to be affected. As the pre-election phase usually starts about one year before the election day, giving ample time for different potential security attacks that can alter the election result.

From above mentioned 12 pre-election sub-processes the most vulnerable ones are those that involve public accessibility, since the influence of altering these are with the greatest impact on voters. These sub-processes are: campaigning of the political parties, voter education and political debates and political parties campaign financing. Each of these, if manipulated, can create a ripple effect in the eyes of voters and can sway the result of elections.

Election phase

The election process can be viewed as the election day; however, we have to take into account that there are “early voting” processes, most commonly a week before the election day in the households of voters and election offices for those who are unable to participate in the elections on the election day, as well as the voting by using postal services from different countries of the citizens living aboard.

This phase consists of given sub-processes:

1. Voting offices and officers.
2. Electronic voting (where applicable).
3. Election results.

This phase is considerably shorter in time, so the potential window of threats is narrower, however, the potential impact is critically high. By affecting information technology systems on the election day the whole elections can be rendered obsolete. This, of course, is the most severe potential scenario and there are several fallback solutions in each country. However, each year the potential impact is growing from the cyber and hybrid threats.

Post-election phase

The post-election phase can be viewed as the least-impactable part of the whole elections, as at this stage there are fewer potential threats that could impact the election results. That being said – post-election sub-process also investigates potential interference in the previous election subprocesses and can render the results of elections invalid. The post-election phase consists of:

1. Reviewing of complaints from all involved parties (voters, political forces, observers etc.).
2. Disputes of the complaints.
3. Resolutions of the disputes.

In the history of the world in 20th and 21st century there are 64[9] annulled election results to this date and 31 of these precedents have happened in the 21st century.

1.4 Implications of mistakes in election process

Rights to vote is pillar of any modern democracy and they are widely executed in election process. Overall, any mistake or flaw in election process, where someone cannot execute their right to vote, can be seen as obstacle to democracy. Any flaw can be turned against election process and results, as possible election interference.

During elections, any information system used for critical parts of election process must be made redundant and have close to 100% uptime. If systems are unavailable, due to error or attacks by malicious parties (e.g., DDoS attack), unavailability will be seen as obstacle to execute the right to vote. If system becomes too complicated, it can be seen as obstacle for people who are less familiar to modern technologies, as it reduces their ability to vote. If, for some reason, someone, or specific group of people (e.g., people who had their ID cards issued between date A and B), this group is discriminated, and objections are raised. Any flaw will be brought up against winning party, as these voters, who, for some reason, could not vote, would always 100% vote against losing party and that way change the results of elections. As described by CERT.LV expert (see Annex Nr3 – Interviews), it might be easier to influence people with fake content, than it would be to hack the systems and create backlash to elections.

Election process must be simple and understandable to public, so there is no confusion, and it is not used as aspect against trust of elections. Election process also includes observers, who make sure, that elections are fair, there is no data manipulation and public, as well as other countries, see these elections as legal execution of democracy. While digitalization of election systems can improve efficiency of them, it also makes them harder to understand, as a lot of processes happens digitally

[9] Azimi, Fakhreddin "Elections i. Under the Qajar and Pahlavi monarchies, 1906-79". In Yarshater, Ehsan (ed.). Encyclopædia Iranica. 4. VIII. New York City: Bibliotheca Persica Press. pp. 345–355.

and cannot be easily observed. Transparency becomes question of understanding. This is also raised as issue by CERT.LV expert. As we have observed with COVID-19 misinformation, people tend to trust posts on internet, that are easier to understand, compared to science behind vaccines. Same issues can come to digital elections, where people don't understand, how confidentiality and integrity is maintained, how they can know, that data were not manipulated in the system. Education campaigns should be used, and information made available to experts and influential representatives, who can verify that everything is one in a good manner and express their opinions to public.

2 Use cases analyses

Four election cases were assessed during particular study to examine indicators and markers for special aspects that are relevant within the context of election digitalization and different threats with links to cybersecurity domain (See Annex 2 Election Cases Assessed).

Two of the assessed cases were globally well-known elections with large numbers of voter participants over large number of states or countries. First, it is the European Parliament elections in May 2019. Second, The United States of America Presidential Elections in 2016 that are associated with spreading of misinformation and voter manipulation.

The other two assessed cases are of a smaller scale. The Latvian Municipal Elections in May/June 2021 is a special case within this study since it serves also as a basis of voter activity correlation with mobile network intensity indicators.

The Estonian E-elections are assessed from the perspective of “desirable future state scenario”. Estonian e-election system was analysed from the cybersecurity threats perspective in 2014 by well-known international cyber security researchers’ group.

3 Elections from MNO`s big data perspective

The legitimacy of power gained through free elections is based on society values and assumptions of social / state structure, which are difficult to verify separately for each involved person within the voting[1] process. The lack of a verification mechanism provides a fertile ground for manipulation of the information space, as well as ease spreading the fake and alternate news our opinions. More recently depiction of alternative reality has become a trend both in newer and older democracies. As a result, the key values of democratic society may disintegrate, spreading intolerance and misbeliefs. Which results in a tangible trend of dramatic reduction of voter activity as shown in Figure 1 where new democracy societies are more reluctant to voting process.

Country	1979	1984	1989	1994	1999	2004	2009	2014	2019
Belgium	91.36	92.09	90.73	90.66	91.05	90.81	90.39	89.64	88.47
Denmark	47.82	52.38	46.17	52.92	50.46	47.89	59.54	56.32	66.08
Germany	65.73	56.76	62.28	60.02	45.19	43	43.27	48.1	61.38
Ireland	63.61	47.56	68.28	43.98	50.21	58.58	58.64	52.44	49.7
France	60.71	56.72	48.8	52.71	46.76	42.76	40.63	42.43	50.12
Italy	85.65	82.47	81.07	73.6	69.76	71.72	66.47	57.22	54.5
Luxembourg	88.91	88.79	87.39	88.55	87.27	91.35	90.76	85.55	84.24
Netherlands	58.12	50.88	47.48	35.69	30.02	39.26	36.75	37.32	41.93
United Kingdom	32.35	32.57	36.37	36.43	24	38.52	34.7	35.6	37.18
Greece		80.59	80.03	73.18	70.25	63.22	52.54	59.97	58.69
Spain			54.71	59.14	63.05	45.14	44.87	43.81	60.73
Portugal			51.1	35.54	39.93	38.6	36.77	33.67	30.75
Sweden					38.84	37.85	45.53	51.07	55.27
Austria					49.4	42.43	45.97	45.39	59.8
Finland					30.14	39.43	38.6	39.1	40.8
Czechia						28.3	28.22	18.2	28.72
Estonia						26.83	43.9	36.52	37.6
Cyprus						72.5	59.4	43.97	44.99
Lithuania						48.38	20.98	47.35	53.48
Latvia						**41.34**	**53.7**	**30.24**	**33.53**
Hungary						38.5	36.31	28.97	43.36
Malta						82.39	78.79	74.8	72.7
Poland						20.87	24.53	23.83	45.68
Slovenia						28.35	28.37	24.55	28.89
Slovakia						16.97	19.64	13.05	22.74
Bulgaria							38.99	35.84	32.64
Romania							27.67	32.44	51.2
Croatia								25.24	29.85
Total EU	**61.99**	**58.98**	**58.41**	**56.67**	**49.51**	**45.47**	**42.97**	**42.61**	**50.66**

Figure 1 Europarlament turnout by country (2019)[10]

Continuously decreasing number of voters has a direct impact what alternative news left on an election process. As a result, achieved raising numbers of “drop off” voters increase the return on investment for political manipulation. Very fertile ground for internal and external ground of political technology which affect general perception that all elections are fixed, and democracy faked. Thus, by example external powers, increase they field of influence over the outcome of elections and processes in sovereign societies. Every stolen or compromised election undermines the credibility of this democratic process. Therefore, each election worldwide should not be considered a separate event, it has a spill over effect on society worldwide and should be examined more carefully.

One of options would be a technology driven voting reassurance mechanism integrated in a fabric of MNO`s daily mode of operandi. This could become an important public reassurance tool as it has potential of provision of open real time statistically reliable data that independent observers survey requires without the threat of invading privacy.

Hypothesis:

Alternatively, full-scale voter monitoring is needed to support a democratic and transparent electoral process. The essence of the voter monitoring tool is to correlate the daily activity in the network in comparison with the election day by identifying the activity of the society in a broader overview.

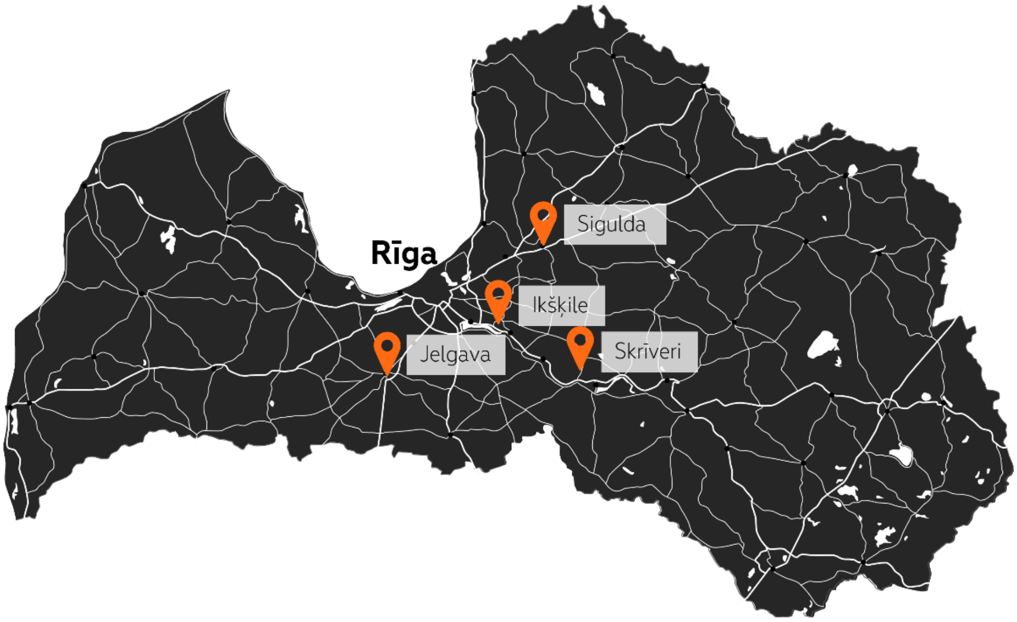


Figure 2 Locations of monitoring points of Latvia municipal election 5th of June 2021.

Important prerequisites:

The tool must not violate a person's right for privacy, nor by any means it should put in question a qualitative "hand counting" methods. The tool works as a quantitative method to serve as an assessment of relative electoral activity in the whole territory.

3.1 Election data analysis method

For technical reasons mobile network operator should monitor closely the performance of each base station and technology 24/7. A typical network contains of thousands of base stations and to keep up with the overall perspective it requires a simple performance indicator to monitor and to identify faults our to predict upcoming malfunctions. As technology evolves and fabric of mobile network is tailored from many different technology components and serving in various environments historical data are kept for learning from previous incidents. Aggregated periodic data containing 3G/4G/5G technology activity counts as well as total transferred data rates are those indicators describing the activity of each base station. Each base station has its own pattern of activity which taken as a reference for assessment and monitoring purposes. To generalise such aggregated data gives a overall perspective on surrounded territory – urban/sub-urban/rural as well as governing resident mobility patterns. These patterns could be set as a reference and activity compared to a “typical day at work” gives an estimate of peculiar resident activity. It is obvious that for residential territory working days and weekends clearly shows the change of habits. A bank holyday are those exceptional cases which does not fit the usual pattern. Similarly, as an election happens once in a long period of time the activity levels compared to a reference pattern should be distinguishable. This has been put to the test within SPARTA election monitoring task.

One of challenges to avoid bias is to set a reference for the election day. This is governed by several assumptions, however none of them are curved in stone as so far MNO`s in general do not explore big data with analysis perspective. Technically speaking as network evolves technology providing it evolves along. With newest 4G/5G technology introduced it enables new features for data collection. Therefore, the indicator - total incidents per period are summarised adding new elements to the equation, this equation over the time evolves and historical data becomes non-relevant to the newest release of technology. To account for this inconsistency for setting up a reference day base station patter a several tactics was considered:

- A reference day`s pattern is an average of particular weekday`s activity pattern within the period of a year our several years.
- A reference day`s pattern is an average of particular weekday`s activity pattern within the period of a previous month.
- A reference day`s pattern is preselected weekday with similar weather conditions. A particular expert judgement is requirement to assess particularities of election versus reference period indicators. As example pandemic induced lockdown activity pattern should not be set as a reference. Similarly, days with local large public gathering our social events should be avoided as referencing pattern.

To generalize a priority for setting up the reference day is cascading from data availability. In future the yearly pattern is a must, while short term activities could serve as a cross validation of election day activity. Obvious advantage of a yearly data is unrelated from weather conditions while monthly and a particular reference day selection is subjective and requires expert level data scientist.

3.2 Analysis of Latvia municipal elections on 5th of June 2021.

For Latvia municipal election day analysis four base stations within the vicinity of voting offices has been selected. Selection was based on similarities between residential density and expected activity in particular territory. As 2021 municipal elections did not include the capital city therefore selection of representative cities was selected based on the population and representation on national scale. A city of Jelgava represented top five by population city – population up to 60k. It should be noted that within Jelgava a residential/industrial district has been selected. Sigulda city represented next 15 city scale with population of approx. 15k inhabitants representing residential area with high influx of visitors during the weekends. Ikšķile city with population of 7.5k inhabitants representing suburban/residential area and finally Skrīveri with 2.5k population representing typical rural city and it`s centre of gravity.

It should be noted that mobile network base station consist of several sectors and identification of sectorial coverage of voting office is critical. As example a six sectorial base station data activity is shown in Figure 3. where vertical axes represent network activity per hour as a sum of data session requests and calls while horizontal axis separate each hour within 24-hour reference day. As one can observe a typical peak of activity is around the noon and declining afterwards. Furthermore, as base station antennas are spread around the azimuth no all of them are fully in-use and have no spikes in activity increase whatsoever. This low network activity depends on residential density within the sector. For further referencing these sectors should be categorised as example - mobile coverage or residential high activity sector. This was not initially done, nevertheless in the future analysis it may be necessary to do so. This data/residency activity indicator category would allow to filter locations where outlier events are most likely to happen which could compromise analysis sensitivity.

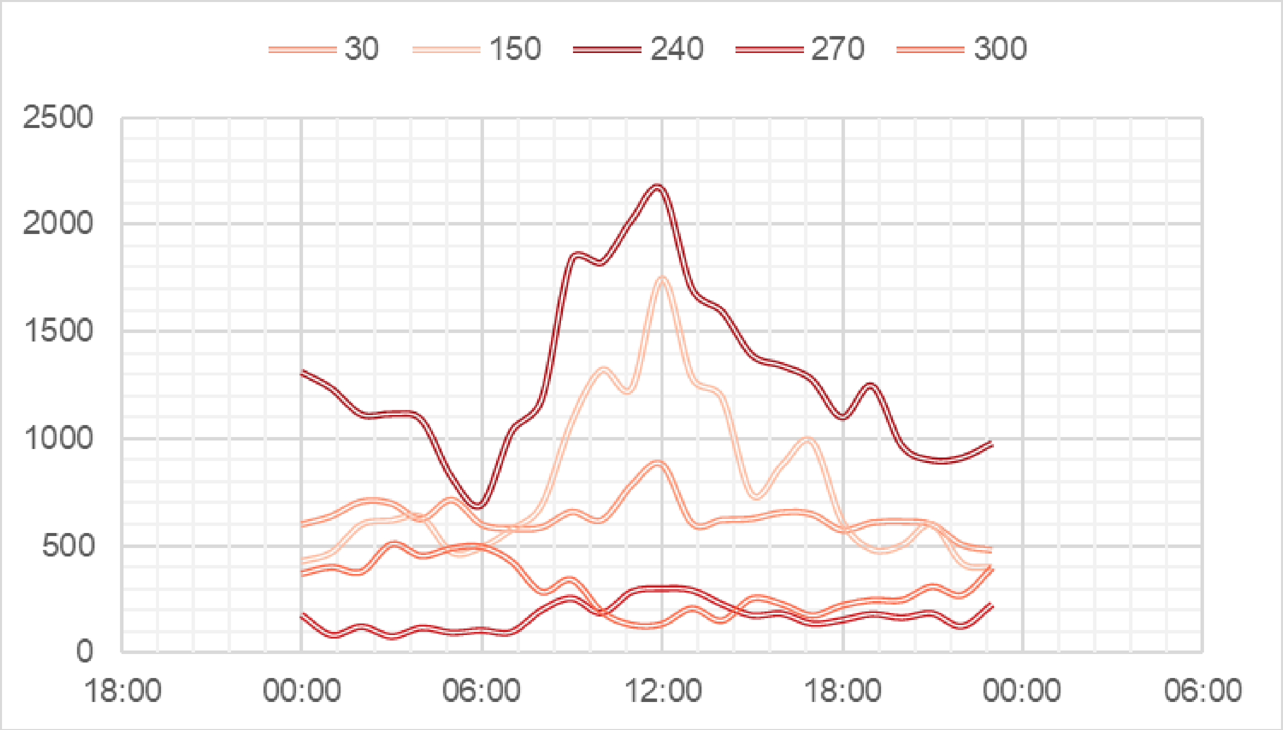


Figure 3 Example of data activity of base station for each sector ($30^0/150^0/240^0/270^0/300^0$) orientation towards horizon within a time section of a reference day.

Initial approach was based on assumption that minor amount of data would be used for verification of hypothesis only. Thus, LMT focus was to set up a reference day`s pattern as an average of weekday`s activity pattern within the period of a previous two month. It should be noted that within previous month Saturdays several national/bank holydays took place which would compromise a referencing them as a typical Saturday`s. Moreover, as spring is period of the time when residential activity is picking up the weather affects a lot of activities which is associated with urban mobility. Therefore, humidity - rain which affect the decision for family mobility during weekends was collected to filter conflicting Saturdays in the past. It was – pity that 5th of June was sunny day like most of Saturdays within April/May month of 2021. This for sure reduced the complexity for selection of reference day. Once the election day was over and verification study confirmed activity spike an authorization was given for more wider data collection within period of previous year. The annual average and median reference line were drawn for each of four points of interests. A figure 4 depict daily activity for each of four election monitoring points at Jelgava/Sigulda/Ikšķile/Skrīveri comparing with reference day of 24th April. Again, in figures 4 to 14 all vertical axes represent network activity per hour as a sum of data session requests and calls while horizontal axis separate each hour within 24-hour reference day

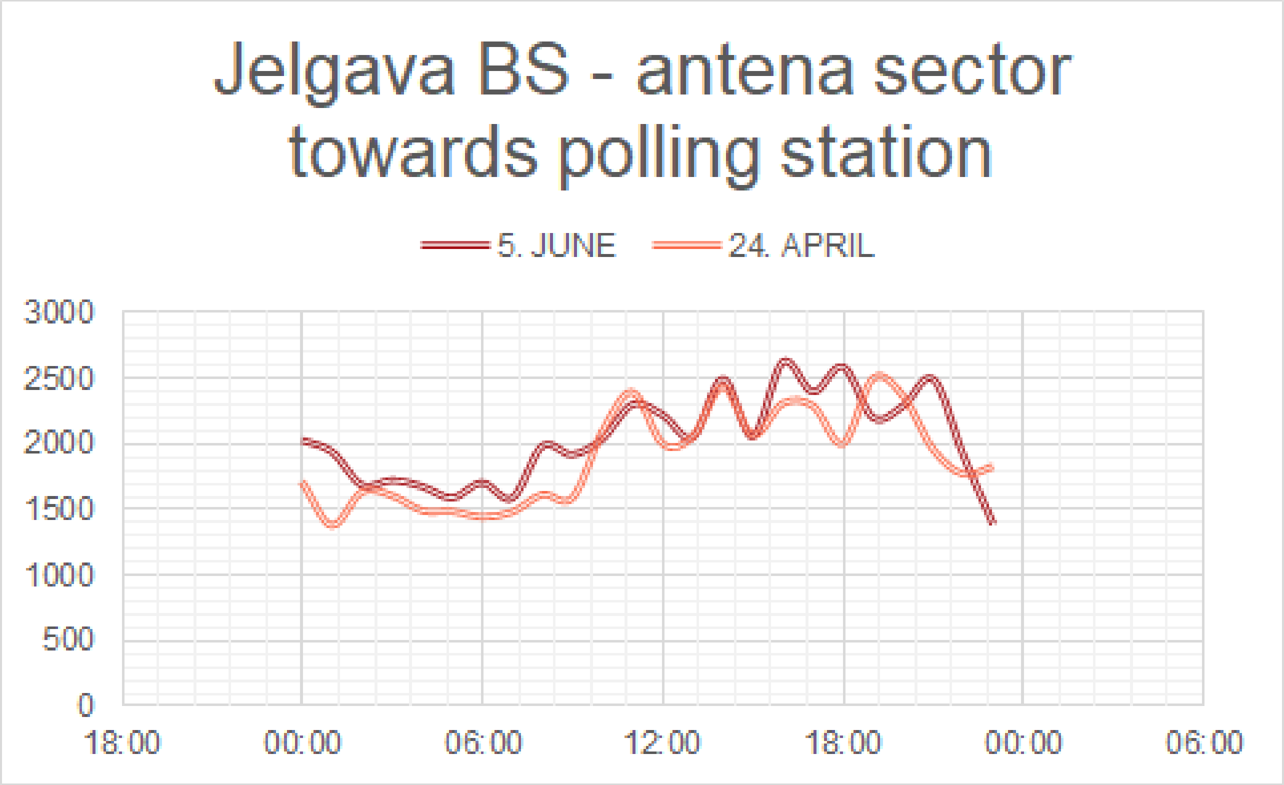


Figure 4 Election Day versus reference day activity at 24th of April at Jelgava city monitoring point.

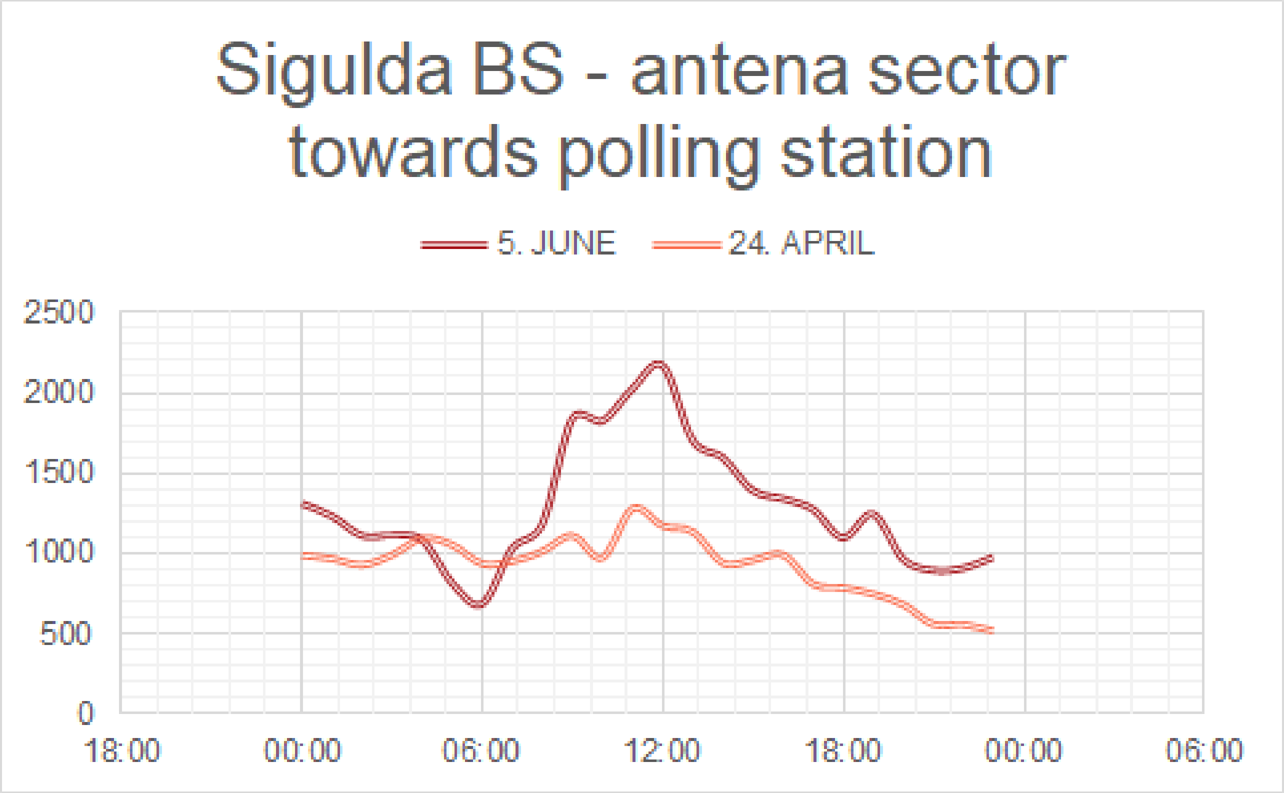


Figure 5 Election Day BS activity at Sigulda city monitoring point.

As one may see it in Figure 5. both Jelgava and Sigulda monitoring points are remotely located within the city therefore day`s average is marginal. For case of Jelgava it's no persistent spark of activities can be observed while for Sigulda monitoring point a constant increase in activity starting from the opening timing of election offices can be seen.

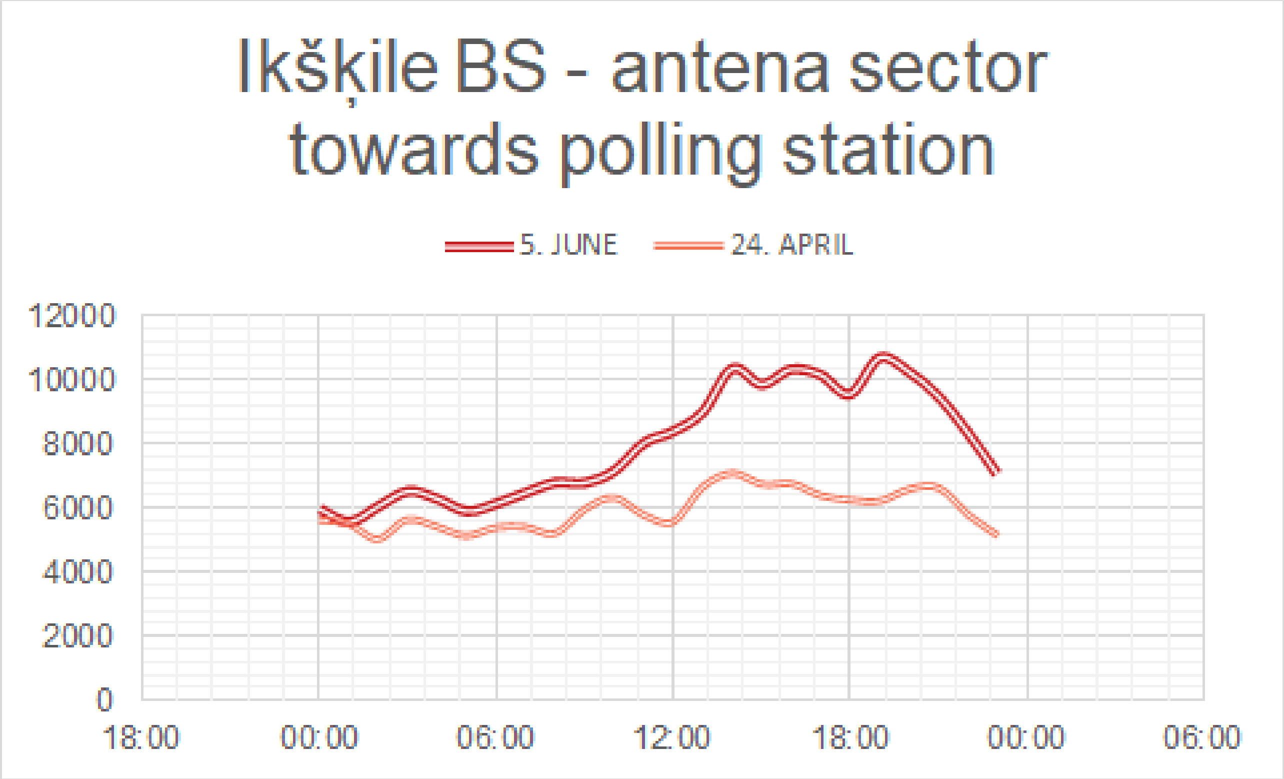


Figure 6 Election Day BS activity at Ikšķile monitoring point.

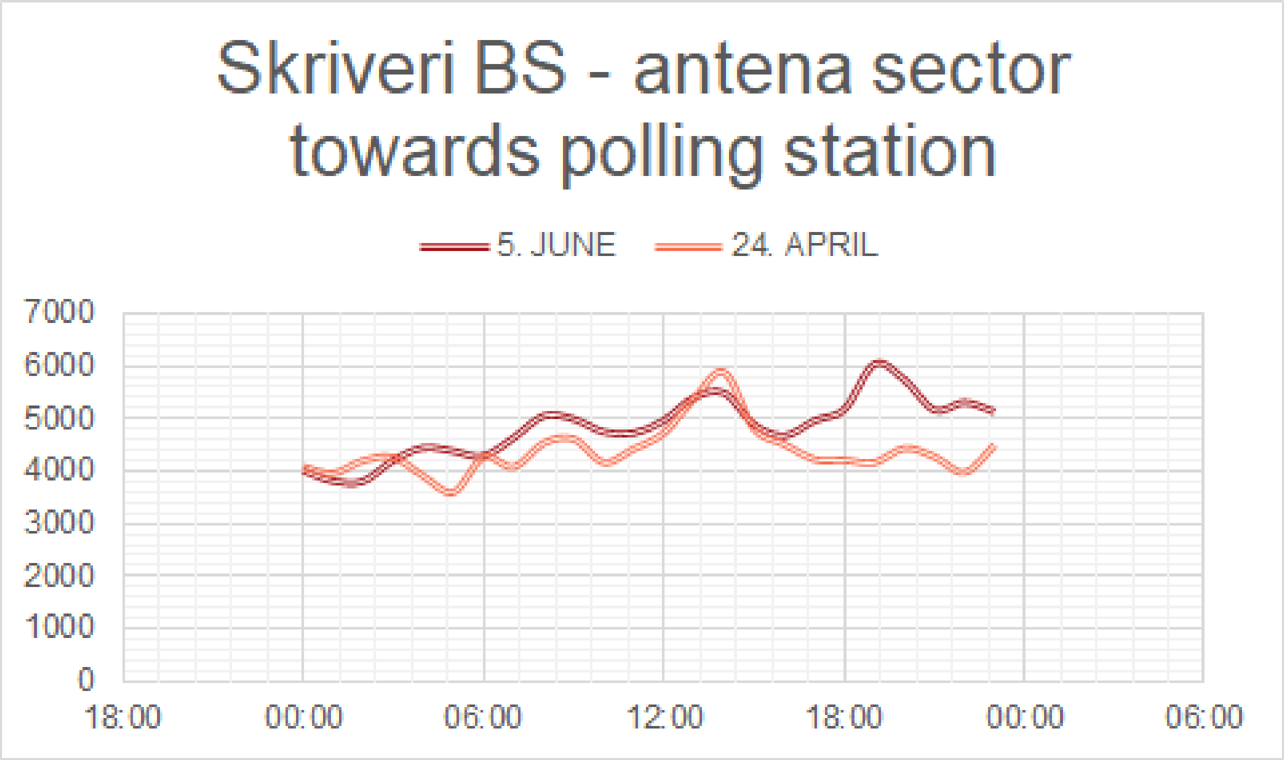


Figure 7 Election Day BS activity at Skrīveri monitoring point.

A counterintuitive observation is given in Figure 6 and 7 where suburban and rural base station in average is more activities populated than selected cities monitoring points. This phenomenon should be further investigated for categorization and attribution of base station type and its “potential” in election monitoring. From activity charts it is evident that Ikšķile monitoring point highlight consistent activity increment compared to the reference day, while Skrīveri show activity increment only in afternoon session. Such local spikes are reasons why annual average measurements should be used instead. As a next step monitoring point election day activity are compared with annual average and median histogram. All four monitoring point activities are compared in Figures 8 to 13.

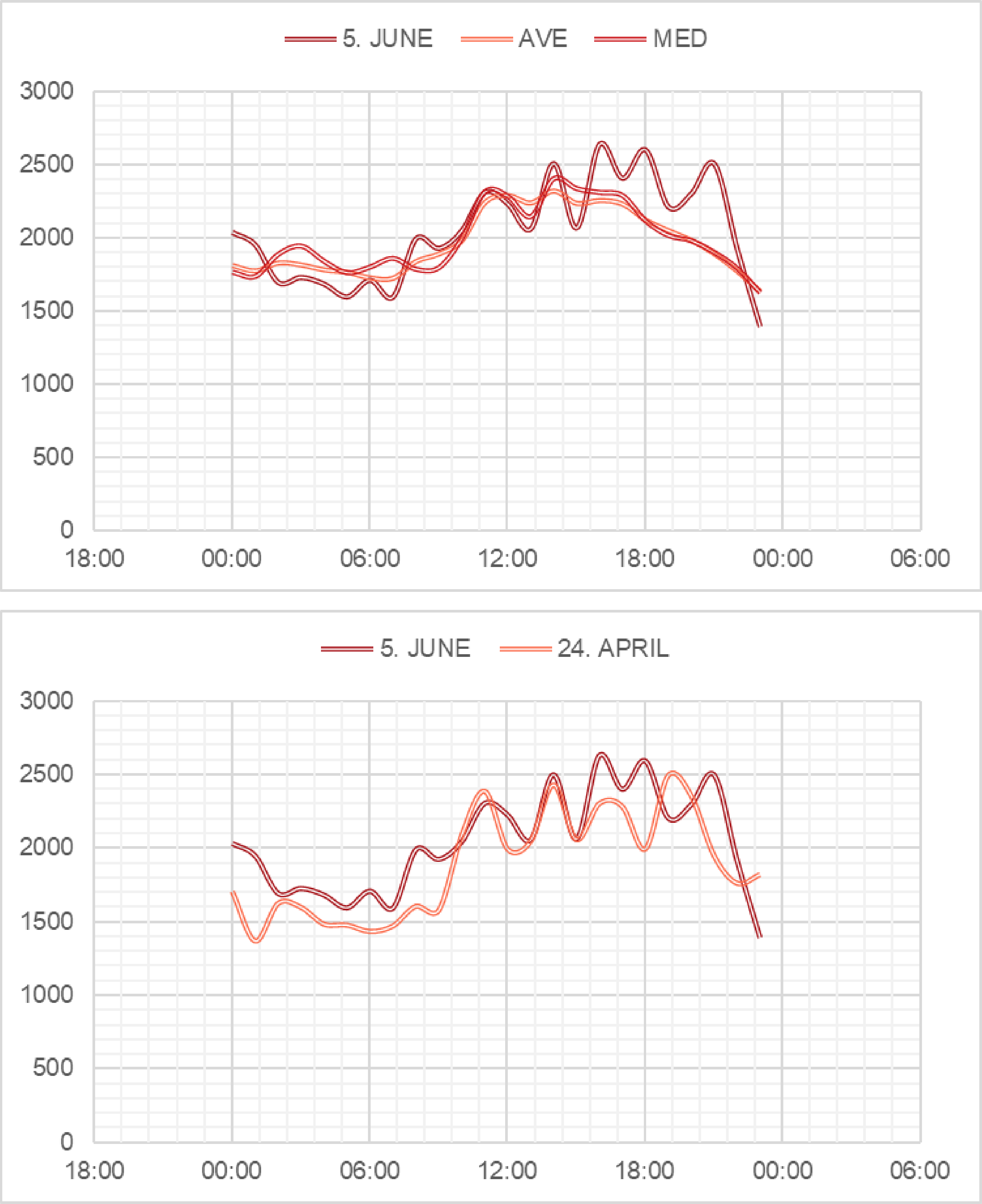


Figure 8 BS user activity at Jelgava election monitoring point – Election Day versus reference and AVE/MED patterns.

Jelgava monitoring point histograms shown in Figure 8 clearly identify that by averaging activity data on annual basis the corresponding activity spike becomes evident. Moreover, it shows that voting activity has started to pick up only in afternoon which is in line with polling station no. 196 “LLU Sports Hall” reported activity from Central Voting Commission of Latvia statistics. As shown in Figure 9 activity within polling station 196 was below average in perspective of Jelgava city, nevertheless by 16:00 majority of voters have casted the votes. This is very good indicator as each voter was surveying done by LMT at this pooling station and correlation could be drawn afterwards.

Nr.	Institution	7:00-8:00	7:00-12:00	7:00-16:00	7:00-20:00
189	JELGAVAS CENTRA PAMATSKOLA	11	200	387	613
190	IESTĀDE "KULTŪRA"	26	296	541	694
191	JELGAVAS MŪZIKAS VIDUSSKOLA	4	112	198	253
192	JELGAVAS 5. VIDUSSKOLA	23	283	535	737
193	JELGAVAS PILSĒTAS PAŠVALDĪBAS ADMINISTRĀCIJAS SABIEDRĪBAS INTEGRĀCIJAS PĀRVALDE	16	168	276	359
194	JELGAVAS PAULA BENDRUPA PAMATSKOLA	15	223	392	586
195	JELGAVAS VALSTS ĢIMNĀZIJA	19	293	530	725
196	**LLU SPORTA ZĀLE**	**6**	**149**	**288**	**383**

Figure 9 Election Day activities at Jelgava city pooling stations.

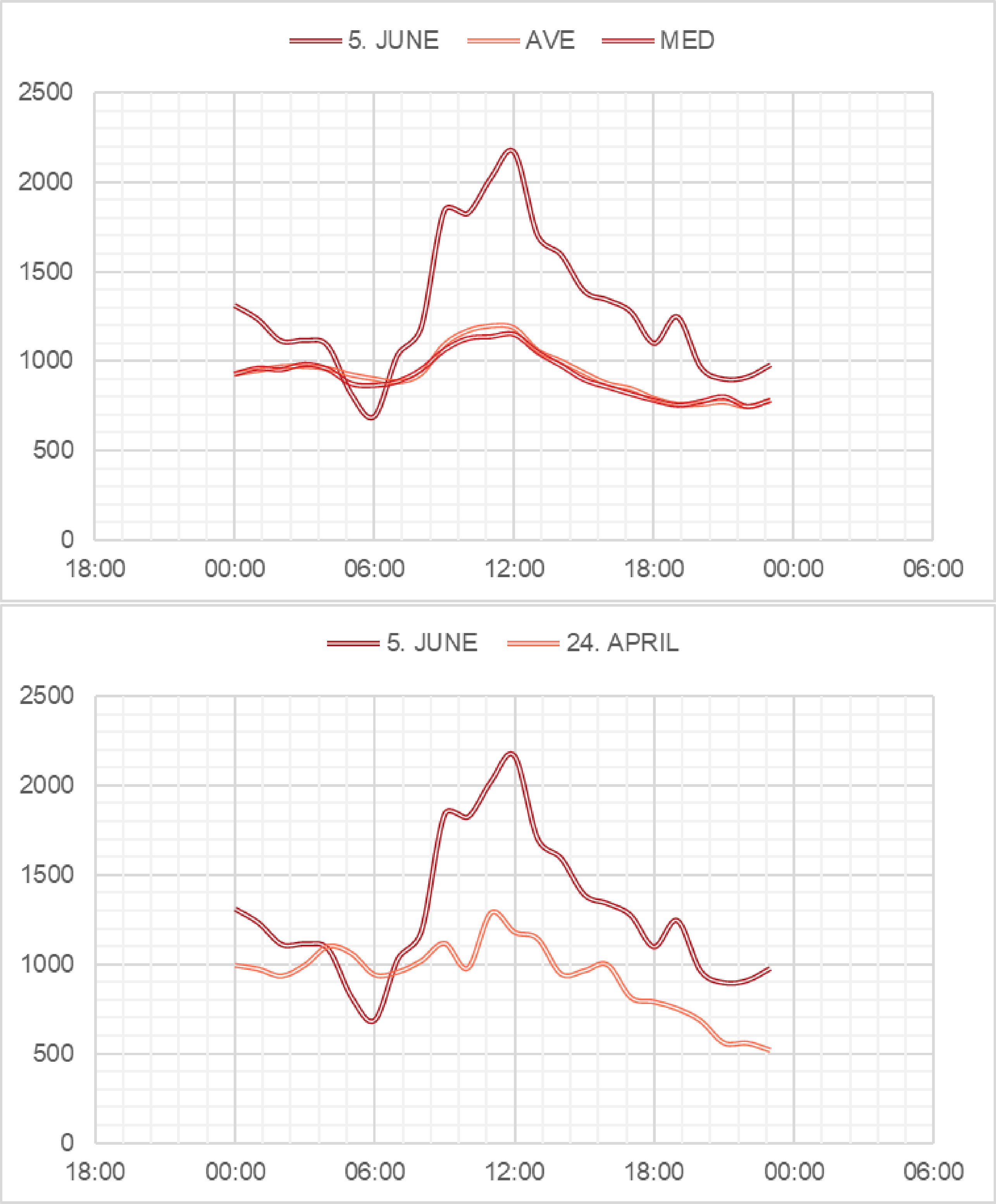
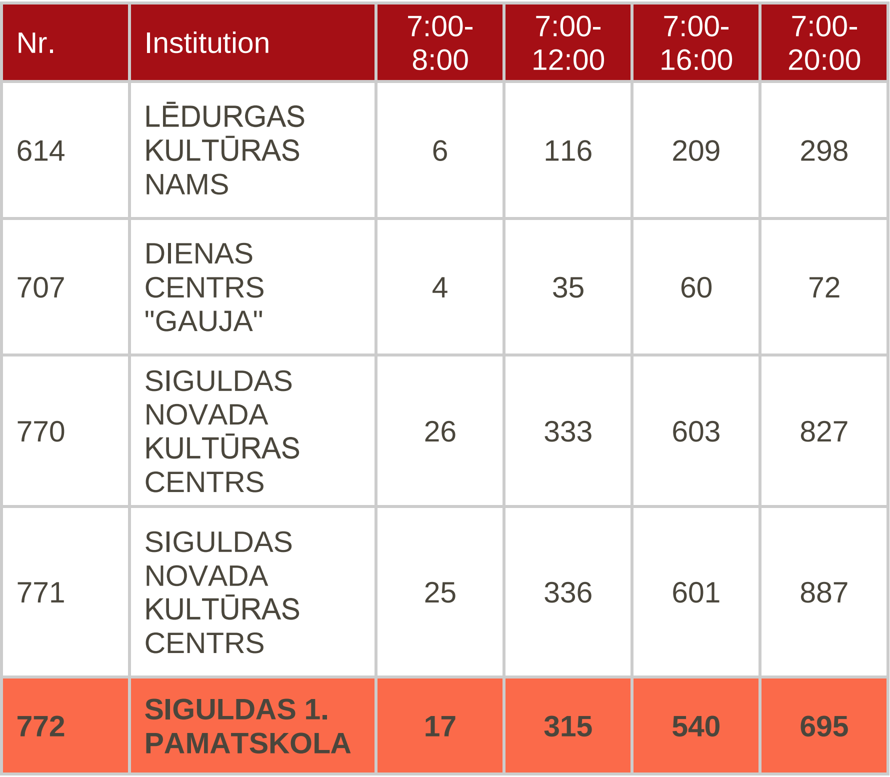


Figure 10 BS user activity at Sigulda election monitoring point – Election Day versus reference and AVE/MED patterns.

Sigulda monitoring point histograms (Figure 10.) are in line with Central Voting Commission of Latvia statistics (Figure 11) of polling station no. 770 “Siguldas 1. pamatskola” where majority of voters have expressed, they will before the lunch time. As Figure 11 suggest the average activity in selected pooling station was well above average from Sigulda municipality perspective and it correlates with network activity in period between 7:00 – 12:00.



Nr.	Institution	7:00-8:00	7:00-12:00	7:00-16:00	7:00-20:00
614	LĒDURGAS KULTŪRAS NAMS	6	116	209	298
707	DIENAS CENTRS "GAUJA"	4	35	60	72
770	SIGULDAS NOVADA KULTŪRAS CENTRS	26	333	603	827
771	SIGULDAS NOVADA KULTŪRAS CENTRS	25	336	601	887
772	**SIGULDAS 1. PAMATSKOLA**	**17**	**315**	**540**	**695**

Figure 11 Election Day activities at Sigulda city and district pooling stations.

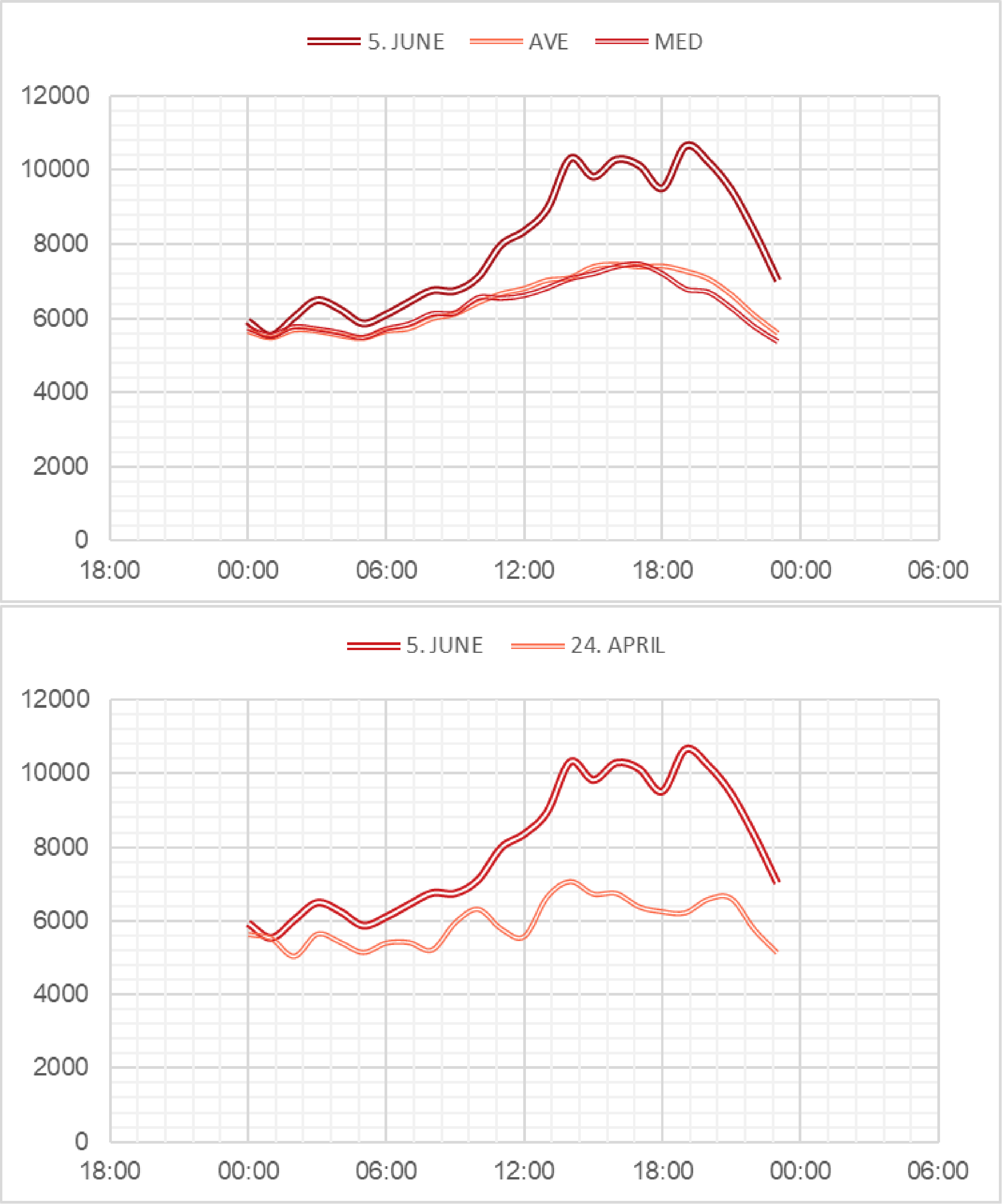
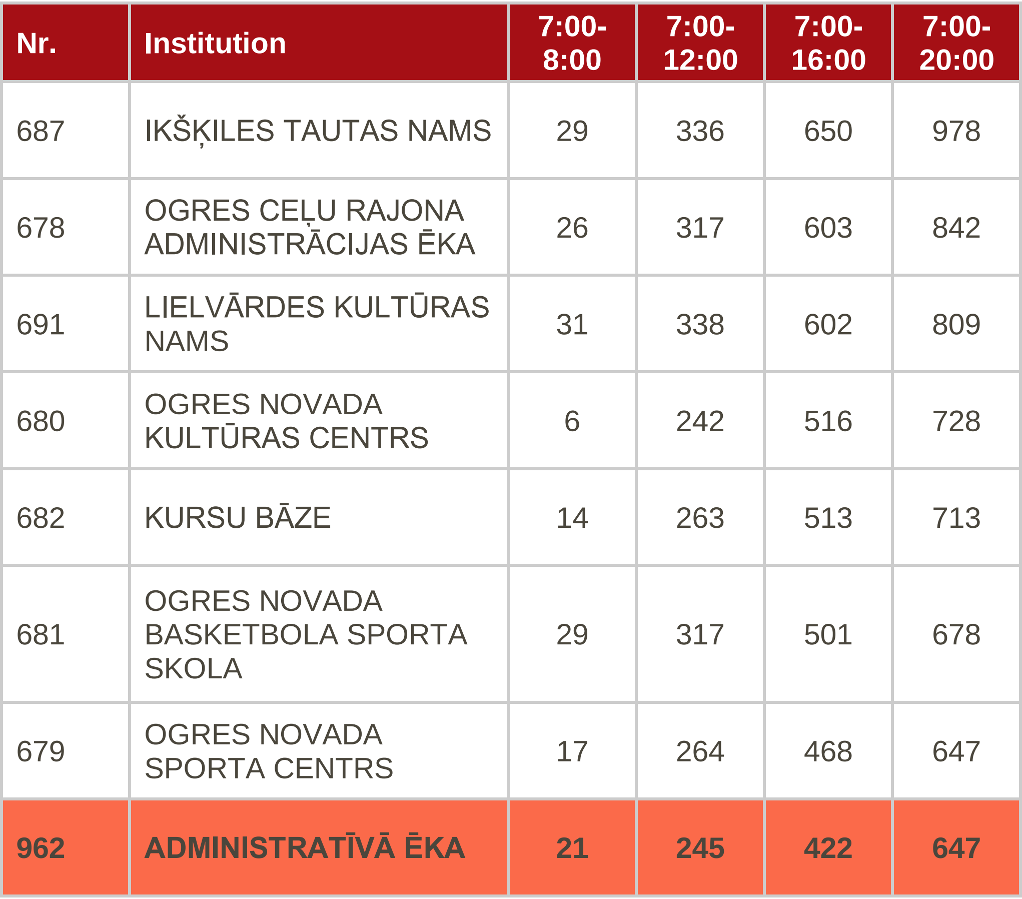


Figure 12 BS user activity at Ikšķile election monitoring point – Election Day versus reference and AVE/MED patterns.

Ikšķile monitoring point histograms (Figure 12.) are in line with Central Voting Commission of Latvia statistics (Figure 13) of polling station no. 962 “Administratīvā ēka” where constant flow of voters has been observed throughout the day. Similarly pooling station 962 was well attended above average within Ogre municipally. It shows very strong correlation between voting and network activity. Furthermore, it was noted that in particular Ikšķile mobile base station activity almost doubled during the Election Day.



Nr.	Institution	7:00-8:00	7:00-12:00	7:00-16:00	7:00-20:00
687	IKŠĶILES TAUTAS NAMS	29	336	650	978
678	OGRES CEĻU RAJONA ADMINISTRĀCIJAS ĒKA	26	317	603	842
691	LIELVĀRDES KULTŪRAS NAMS	31	338	602	809
680	OGRES NOVADA KULTŪRAS CENTRS	6	242	516	728
682	KURSU BĀZE	14	263	513	713
681	OGRES NOVADA BASKETBOLA SPORTA SKOLA	29	317	501	678
679	OGRES NOVADA SPORTA CENTRS	17	264	468	647
962	**ADMINISTRATĪVĀ ĒKA**	**21**	**245**	**422**	**647**

Figure 13 Election Day activities at Ikšķile and Ogre district pooling stations.

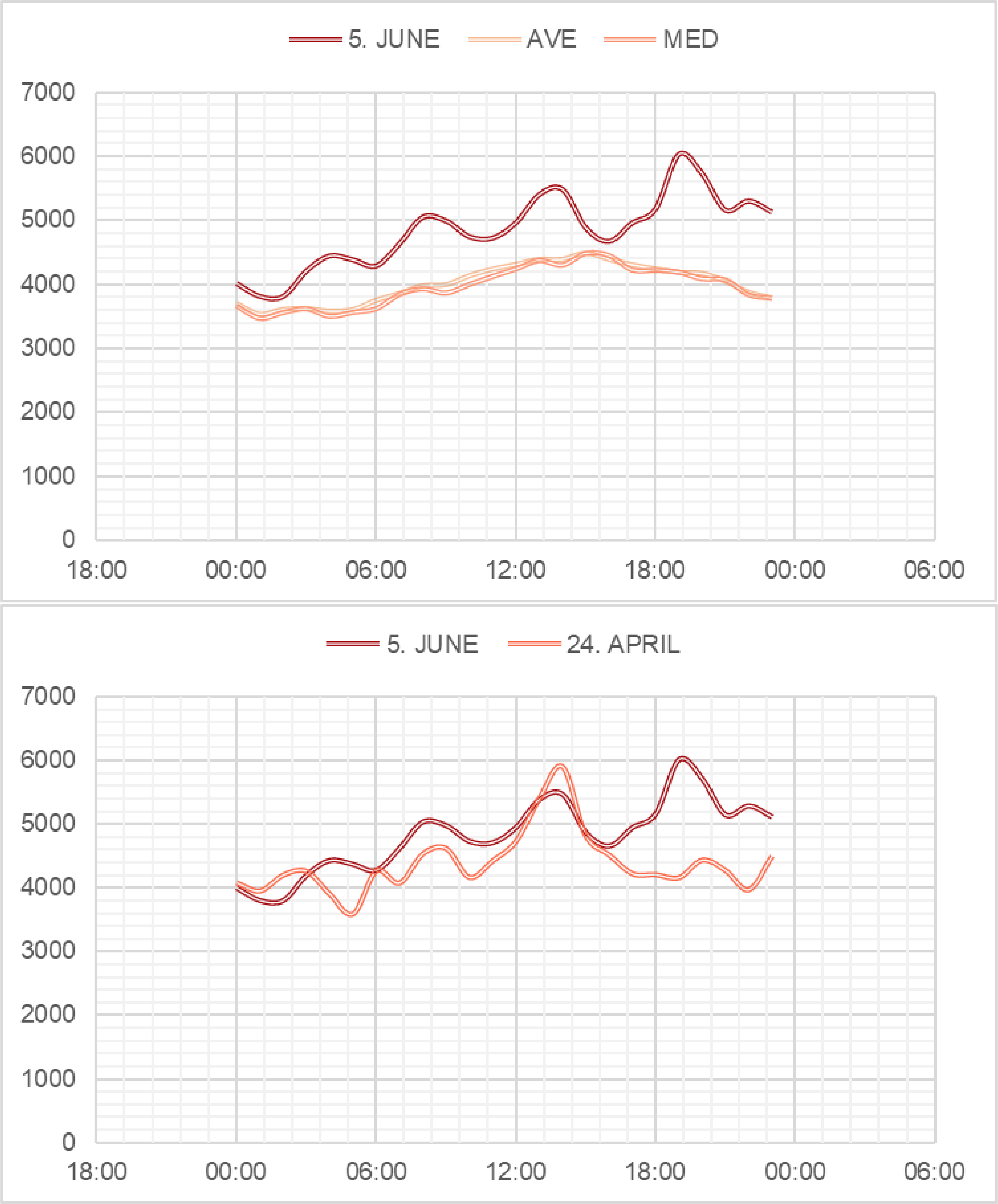


Figure 14 BS user activity at Skrīveri election monitoring point – Election Day versus reference and AVE/MED patterns.

Skrīveri monitoring point histograms (Figure 12.) are in line with Central Voting Commission of Latvia statistics (Figure 13) of polling station no. 285 “Skrīveru kultūras centrs” where constant flow of voters has been observed throughout the day. Again, selected polling station was well attended and gave strong indication of activity increment at afternoon session. It should be noted that at the noon of a reference day some untraceable local activity took place. Thus, reference day gave much higher network activity compared to annual average or median this should be further studied to understand this pattern. Not necessary this is an outlier therefore existence of such data point should be analysed to assess the reliability of proposed monitoring procedure.

Nr.	Institution	7:00-8:00	7:00-12:00	7:00-16:00	7:00-20:00
278	KOKNESES NOVADA DOME	11	278	467	607
268	AIZKRAUKLES NOVADA VIDUSSKOLAS SPORTA HALLE	19	274	464	596
285	**SKRĪVERU KULTŪRAS CENTRS**	**19**	**243**	**427**	**585**
272	PĻAVIŅU NOVADA KULTŪRAS CENTRS	21	243	451	550
267	NOVADA KULTŪRAS NAMS	11	132	262	330
271	JAUNJELGAVAS NOVADA KULTŪRAS NAMS	5	115	195	279

Figure 15 Election Day activities at Skrīveri and Aizkraukle district pooling stations.

Conclusions from the analysis of Latvia municipal elections at 5th of June 2021.

- A correlation between election day activity and its relevance with network monitoring data are evident and statistically significant.
- The mobile network monitoring data technically contain no personal data thus GDPR type infringement treat is evaded.
- It is more likely to identify an activity spike during elections at residential /suburban areas rather that in city/industrial surroundings.
- A yearly average and median activity pattern are best suited to serve as a reference base line for estimation of correlation indicators.
- Sensitivity of proposed data monitoring system are sufficient even for low attendance elections as case of Latvia municipal elections.
- Further 5G enabled data monitoring filtering by technology would further increase the quality of eventual service. Stationary devices as TV routers our smart house equipment filtering would increase reliability of provided data.
- Even a single MNO`s monitoring data gives a quantitative estimate of election day activity, nevertheless if required by governing bodies, a single day monitoring could be synchronized among several network providers to rise the quality level of data.

4 5G added features and their impact for elections

Within this study it is shared a strong believe that there are at least three aspects how fifth generation (5G) telecommunication network could improve and help to enhance over all election process:

1. 5G network architecture with its transport network, back-up data links and reserved power supplies, Multi-Access Edge Computing (MEC), Slicing and other assets and functionalities could serve as sustainable and National wide data network architecture for Elections' IT systems (it is not meant e-elections).

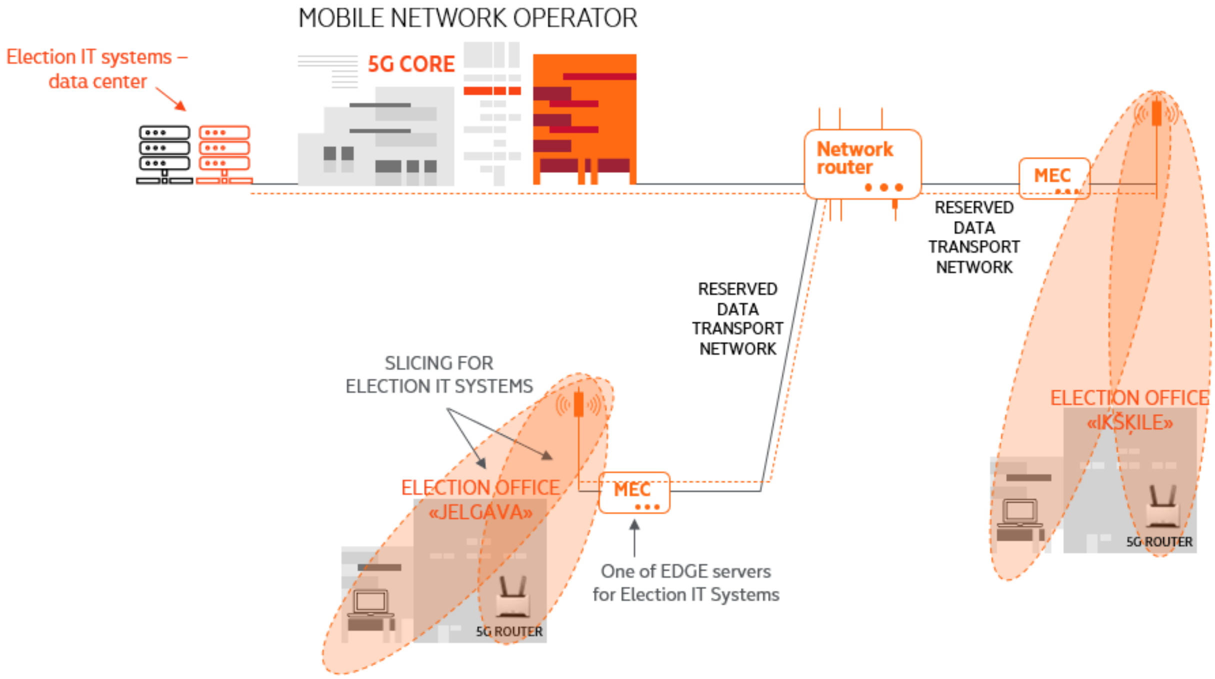

MOBILE NETWORK OPERATOR
Election IT systems – data center
5G CORE
Network router
MEC
RESERVED DATA TRANSPORT NETWORK
RESERVED DATA TRANSPORT NETWORK
SLICING FOR ELECTION IT SYSTEMS
ELECTION OFFICE «JELGAVA»
MEC
5G ROUTER
One of EDGE servers for Election IT Systems
ELECTION OFFICE «IKŠKILE»
5G ROUTER

Figure 16 Visualization of 5G network potential for serving the elections' IT systems

2. 5G network as Nation-wide macro sensor for evaluating participation of electorate who are visiting election offices during elections. But such macro sensing capability with 5G could be possible and effective only, if those electorate activity data are available from all 5G Mobile Network Operators (MNO) which are serving clients in specific country (e.g. in Latvia those are three – LMT, Tele2, Bite). Also, using MNOs networks as tool for macro sensing can be achieved already with 4G, as proven by our test (see chapter 3 done already with 4G network technology. That is what has been practically tested also within this study, see the chapter "Elections from MNO`s big data perspective", but there are limitations. 5G will have better macro sensors for improved precision and usability (see Annex Nr.1 - Technical chapter Positioning without GPS).
3. 5G can improve security of official media resources – e.g. online broadcasting of candidates press conference (see description of example scenario in a chapter "Misinformation as part of cyber warfare"). In this case 5G infrastructure would serve to media needs in similar way as it is in first case with elections' IT systems. 5G network Slicing, MEC and other functionalities can ensure that IT systems used for important broadcasts (e.g. interview of the candidates which reaches high number of listeners) done by official media can be more secured and reliable.

To summarize, with 5G technology will be provided capabilities which can positively impact above mentioned scenarios, if 5G is used properly. Those capabilities are:

- **Higher speed or enhanced Mobile Broadband (eMBB)**. To provide eMBB 5G uses sub-technologies like Massive MIMO antennas (mMIMO), millimetre wave frequencies (mmWave), Slicing functionality to provide QoS within 5G network.
- **Ultra-reliable and low-latency communication (uRLLC)**. To provide uRLLC 5G uses sub-technologies like Multi-Access Edge Computing (MEC) and Slicing.
- Higher supported device capacity per square kilometre or **Massive machine-type communication (mMTC)**. To provide mMTC 5G uses sub-technologies like mmWaves, mMIMO.
- **Longer reach, better coverage**. To provide longer reach 5G uses sub-technologies like low frequency – 700MHz, mMIMO, Non-Terrestrial Networking (NTN) which provides capacity to serve non-3GPP radio access networks with 5G core also 5G New Radio access to Unlicensed spectrum (NR-U).
- **Precise positioning** from 5G network side. To provide that 5G uses sub-technologies like mMIMO, mmWaves, MEC, API accessible for trusted 3rd party software integration with the network (including access to networks Big Data needed for precise positioning calculations), Sidelink.

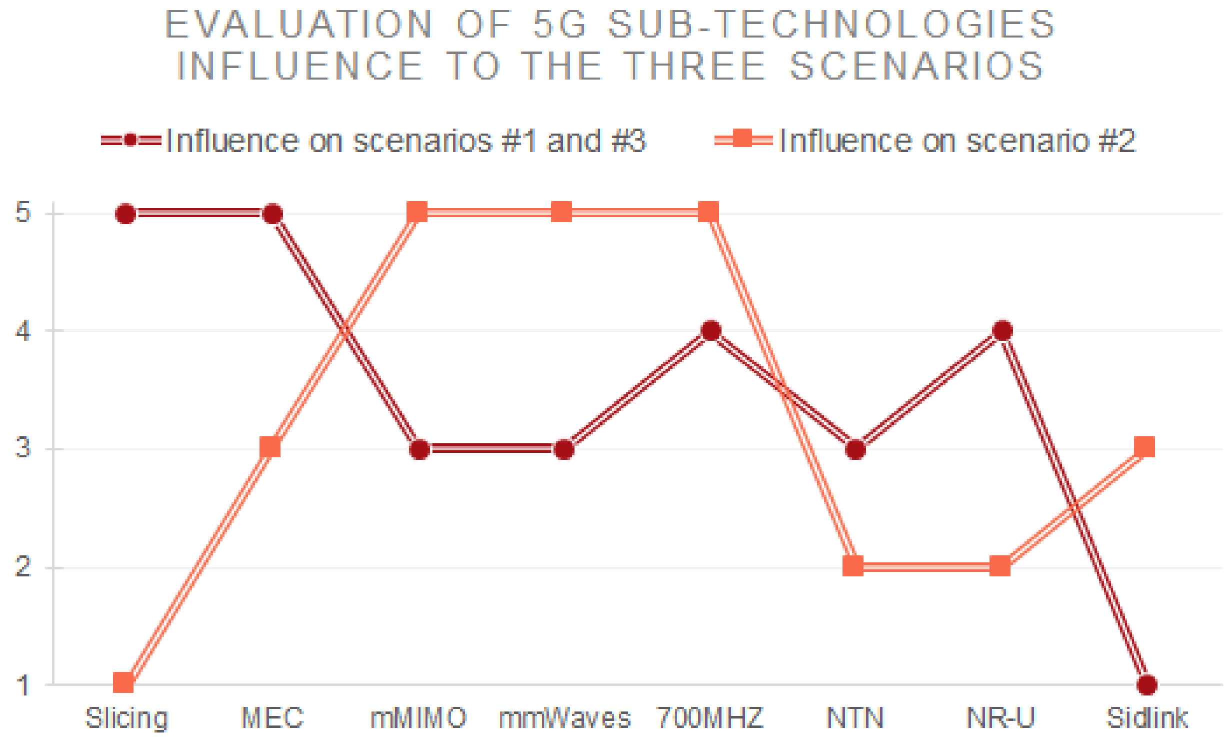


Figure 17 Evaluation of 5G sub-technologies’ influence on the three scenarios

Below are brief definitions for main 5G sub-technologies mentioned above and which are seen as most potential for election processes support:

mmWaves – are introduced starting with 3GPP Release 15 and are updated with Releases above. In telco industry by saying 5G mmWaves are understood frequency range starting form 20GHz and going up to 60GHz. And that frequency range is part of so called “Above 6GHz” range. Overall, in telco industry 5G frequency ranges are divided in three categories – Sub 1GHz, 1 to 6GHz and Above6GHz:

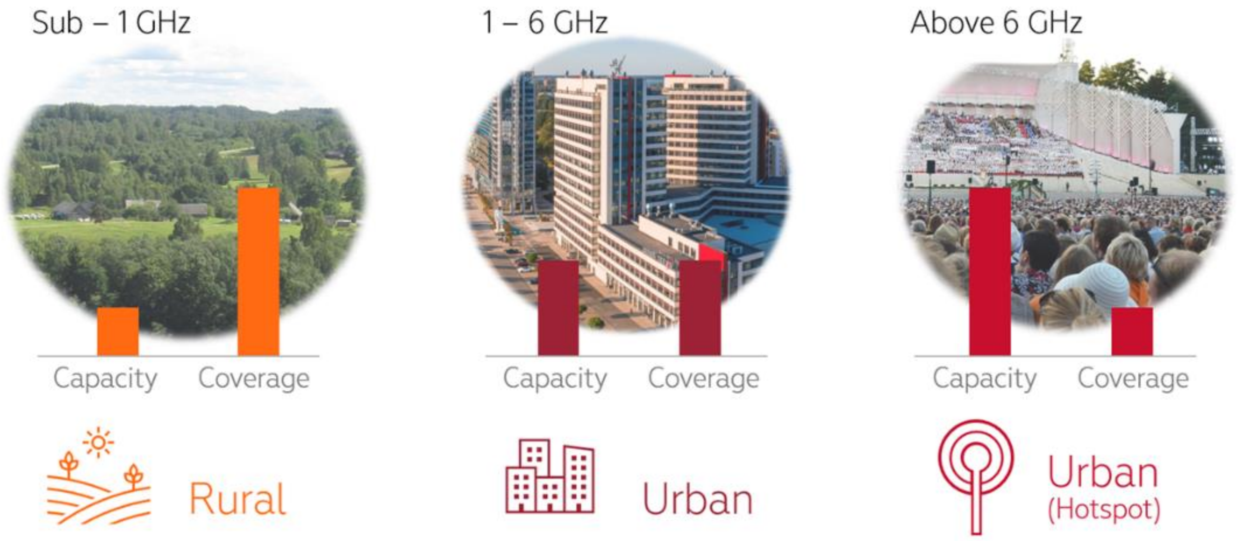
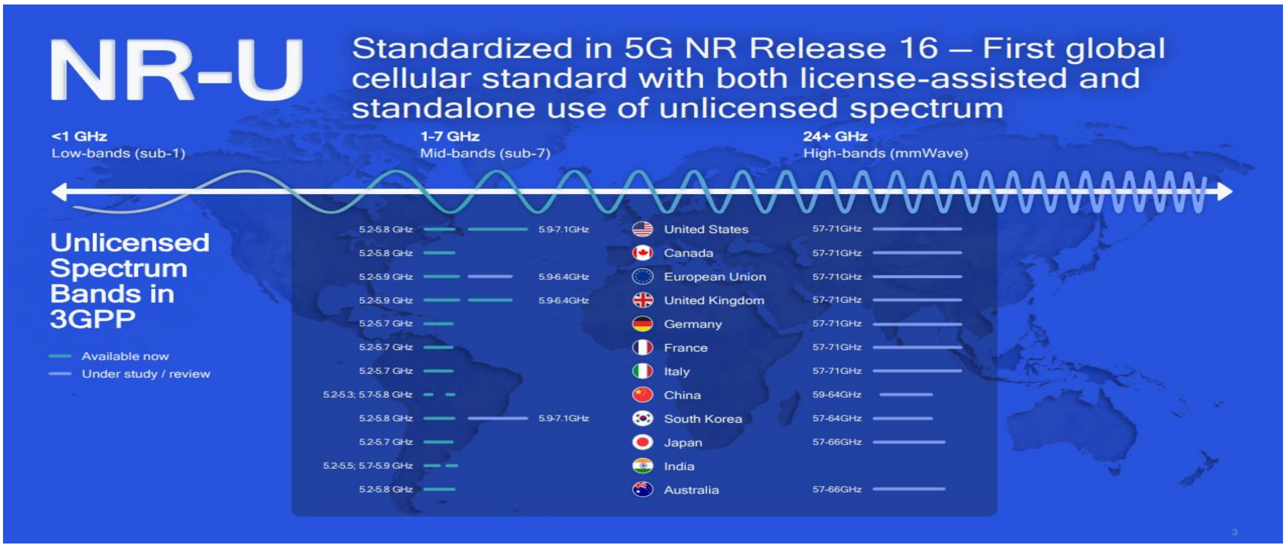


Figure 18 Spectrum bands for deployment of 5G[11]

mMIMO – massive Multiple-Input and Multiple-Output antennas. "Massive-MIMO is a key technology for mmWave. Massive-MIMO is being used as a new technology for improving MIMO characteristics for 5G by exploiting large number of antenna elements (64 and higher) to support simultaneously communication with multiple users. The purpose of MIMO (also mMIMO) is to increase throughput. MIMO builds on the basic principle that when the received signal quality is high, it is better to receive multiple streams of data with reduced power per stream, than one stream with full power.".

NR-U - 5G New Radio access to Unlicensed spectrum. Main idea behind this functionality is that starting form 3GPP Release-16 5G network can be deployed in frequencies which are accessible for public usage similar as it is done for WiFi. That brings new opportunities for overall IT industry (also in terms of elections' IT systems) as MNOs are not only entities anymore which can deploy mobile networks. Before introducing NR-U mobile networks were deployable only in licensed spectrums which were allocated (sold through auctions) to MNOs.



NR-U

Standardized in 5G NR Release 16 — First global cellular standard with both license-assisted and standalone use of unlicensed spectrum

Unlicensed Spectrum Bands in 3GPP

- Available now
- Under study / review

5.2-5.8 GHz	5.9-7.1GHz	United States	57-71GHz
5.2-5.8 GHz		Canada	57-71GHz
5.2-5.9 GHz	5.9-6.4GHz	European Union	57-71GHz
5.2-5.9 GHz	5.9-6.4GHz	United Kingdom	57-71GHz
5.2-5.7 GHz		Germany	57-71GHz
5.2-5.7 GHz		France	57-71GHz
5.2-5.7 GHz		Italy	57-71GHz
5.2-5.3; 5.7-5.8 GHz		China	59-64GHz
5.2-5.8 GHz	5.9-7.1GHz	South Korea	57-64GHz
5.2-5.7 GHz		Japan	57-66GHz
5.2-5.5; 5.7-5.9 GHz		India	
5.2-5.8 GHz		Australia	57-66GHz

Figure 19 Qualcomm. Unlicensed Spectrum Bands in *3GPP* [12]

[11] "Summary and comparison of technologies LTE-4G and LTE-5G", Naval Group, 2019

[12] Source: https://www.qualcomm.com/media/documents/files/spectrum-for-4g-and-5g.pdf, December 2020

Slicing – 5G is anticipated to be a multi-service network supporting a wide range of industries with a diverse set of performance and service requirements. Slicing a single physical mobile network into multiple dedicated logical networks has emerged as a key to realizing this vision. Network slicing is specified in the 5G specifications of 3GPP for Release 15 and later. It is seen as a fundamental technique in 5G networks to accommodate for different quality of service (QoS) requirements exploiting a single physical network. 5G network slicing can be enabled in either 5G core network (CN) and/or a 5G radio access network (RAN). Network slicing can be used, in addition to existing functions in mobile network, like QoS service differentiation, network sharing and roaming. Network slicing is an end-to-end function that requires support in both core network, radio network and end-user equipment.

MEC – Multi-Access Edge Compute, allows to move part or all of data processing closer to end users. This gives multiple benefits and opens new opportunities also in terms of elections. Saying in other words "MEC offers application developers and content providers cloud-computing capabilities and an IT service environment at the edge of the network"[13]. For elections' IT systems and IT systems of official media (the scenarios 1 and 3) MEC can improve speed, latency and data integrity of these systems (see more details in Annex Nr.1 - Technical chapter Multi-Access Edge Computing).

Sidelink – also known as Proximity Services (ProSe) and Device to Device (D2D) type communication. Main idea of the Sidelink concept is to provide direct communication between two or more User Equipment (UE) using mobile network (base stations and core network) only for providing signalization data between network and UE. And in terms of elections Sidelink could provide additional benefits for the second scenario "5G network as macro sensor". Sidelink as sub-functionality can bring up precision of positioning which is one of the identified capabilities important in terms of elections. Sidelink development has been started already in 4G network and is being continued in 5G New Radio - "In Releases 12 to 15, sidelink transmissions are designed based on the air interface of LTE-A, which however may not fulfil the service requirements imposed by the International Mobile Telecommunications-2020 (IMT-2020). To migrate to the fifth generation (5G) network, 3GPP subsequently launched the standardization progress of NR sidelink transmissions in Release 16 in Jun. 2018"[14]

NTN – "5G NTNs extend the scope of 5G NR technology and associated benefits to non-terrestrial platforms. An airborne 5G NR architecture allows MNOs to provide 5G-based services in locations where terrestrial networks are not available using the 5G NR radio interface, thus not requiring any intermediate protocol or technology conversion. 5G NTNs can be provided by satellites, high-altitude platform stations (HAPS) or any other airborne vehicle able to carry the NTN payload. Low Earth Orbit (LEO) satellites and aircraft are the most promising vehicles, due to the associated lower propagation delay. 5G NTN technology solutions are under evaluation in Release 16 work, whereas specifications are expected for 3GPP Release 17."[15]

Still, knowing mentioned opportunities one must realize that cyber security of 5G infrastructures operated by MNOs will play even more important role while 5G networks being used for election process support and/or election macro monitoring. As mentioned, with 5G network technology a lot of functional benefits are brought into the play, nevertheless, as with 5G generation network infrastructure becomes more complex it also puts in place new cyber risks which needs to

[13] ETSI, https://www.etsi.org/technologies/multi-access-edge-computing

[14] IEEE Access, 2019.12.17, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8998153

[15] NCI Agency, 2020.09.15, https://www.mindev.gov.gr/wp-content/uploads/2020/11/Enclosure-2-Working-paper-Potential-of-5G-technologies-for-military-application.pdf

be taken to account while evaluating and getting preparade 5G for using it in election process. E.g. those are:

- Added 5G complexity and security risk due to higher-degree of virtualization and potential cloud usage
- Diverse technology ecosystem renders compliance to industry standards and best practices more important than ever
- Customer's experience requires 5G to be more open and interconnected than any previous mobile generation
- Diversified service offerings complicate assurance of continuous level of security
- Grater functional disaggregating through the Radio Access and Core Network
- New and untested protocols (e.g. Protocols for Interconnect Security)
- Heavy use of common web protocols lowers barrier for unexperienced vendors as well as attackers and fraudsters[16]

Furthermore, when looking specifically at elections and 5G impact on election cybersecurity, 5G mostly inherits existing cybersecurity risks, that are there for overall electronical election systems or elections as such. Nevertheless, if used correctly, with 5G functionalities like Slicing, MEC and more advanced network monitoring capabilities in 5G have potential greatly improve resilience and cyber security of IT systems used during elections.

[16] Source: https://www.youtube.com/watch?v=XHZN3FsVNEc

5 Identified election improvement process use cases and 5G usability within use cases

With the 5G technology there are several potential benefits identified during this research. By using the technology provided by next generation mobile networking, several key aspects can be used to make election process more transparent, and more citizen involved. Both – transparency and involvement are achievable by using the precise positioning provided by 5G technology.

The transparency in election process can be achieved by using anonymized data about mobile device users in the polling stations, thus giving the opportunity to provide precise data about election activity and the concentration of voters in any given polling station. Not only this would provide the voters with information about the potential waiting time to give their vote, but it would also eliminate any doubts about the true potential vote count in any given polling station, as well as the whole elections together. To provide this, it would be necessary for all mobile service providers to give the anonymized positioning statistics data to the central election committees, central statistics bodies and authorized press as well as to the independent organizations that are performing the independent observations of election process. By enabling this option, it would eliminate any speculations about the actual election activity in any given scenario.

The second potential use case would also require for the mobile service providers to collaborate with local municipalities, by giving them the data about actual citizen activity in any given region, down to specific districts of cities. This information would provide the opportunity to crate targeted polling of the inhabitants not only by their declared living address, but by the location they are occupying daily. This would provide higher potential involvement of inhabitants to make decisions together with municipal governances about the actual necessities of the inhabitants. This would provide democratically made decisions about the development of city districts, cities, rural territories. For the inhabitants this solution could provide the opportunity to improve the environment they are inhabiting daily, either it is their place of work, education, or home. For the municipalities this would give the opportunity to develop the solutions the inhabitants would appreciate.

The data, used for the latter use-case would be anonymized and used as statistical model for identifying the general information, not by using precise positioning to identify individuals position in real time.

As a separate new opportunity from election process organizing standpoint offered by 5G technology is the capability to provide a separate network slice for election IT infrastructure communication services. This would provide total election system separation from public commercial network, therefore creating the devices in the slice much resilient to external factors and also provides fixed allocation of certain bandwidth.

6 Conclusions

During research, we concluded that election processes are evolving and introducing increased number of IT systems and devices. By increasing IT component in election process, elections become more complex and inherit cybersecurity risks, including hybrid warfare threats. Meanwhile, wide spread usage of different information sources makes misinformation a common way to influence target audience.

Nevertheless, there is certain drive for digital transformation from society and high level of acceptance of eventual digital solutions for further improvement of election process.

As demonstrated during the study and practical survey conducted during Latvian Municipal Elections in 2021 mobile network monitoring could be further elaborated for on-demand and real time monitoring of voting activity. Furthermore, some of 5G features may be used for cross validation our reassurance of voting activity to reduce fake stolen election claims.

A certain potential may be associated with 5G location-based services features enabling regional referendums our municipality posted question/decision to inhabitants of country/city/district/street. The benefit it brings those residents could be contacted more directly and frequently without costly time and resource consuming activities where simple decisions could be taken. As example a decision to pave street A our street B could be delegated to residents rather to few representatives and local activism may bring more democracy to

5G, using MEC and Slicing technologies can improve IT system security used in Election process. Slicing can guarantee system availability via QoS and boosted security via separate Slice isolation. While MEC can improve availability using edge technology, providing easily accessible solutions. MEC can also boost integrity, by storing log files in separate environment, which can be used to investigate anomalies and identify election interference in data.

Whether elections are using limited IT systems, like online voter register, or going fully online, as electronical elections, 5G can bring additional benefits to improve election system security. Nevertheless, it is important to conclude that 5G can support and improve security on the level e-elections cloud potentially require, but 5G cannot be associated as main enabler for electronic elections.

Finally, as strong conclusion of the study is that 5G main potential is associated with possibility to be used as a nation-wide macro-level sensor for elections to precisely identify mobile data activity anomalies in specific territories, for example – to identify precise difference of connected devices in a building with comparison to a baseline connection amount.

Annex Nr.1 - Technical capabilities

5G Technologies and functionalities

5G brings a lot of new technical capabilities, that will become available to use for election processes (and not only). Possible applications of new 5G features have been described, including pros and cons of these capabilities.

1.1 Higher speeds with 5G

One of 5G features that media likes to talk about is speed. Theoretical speeds can go up to 100 Gbps, compared to 1Gbps on LTE Advanced (4.5G) and 100mbps on 4G. This is 10 or 100 times increase in speeds compared to previous technologies.

Speedtest.net Global Index[17] shows, that average speeds for Mobile are 56.74mbps download and 12.61mbps upload. With leading countries, like Norway (3rd rank) having mobile download speed at 173.54 mbps.

Existing network speeds already varies a lot but bringing in new technology will help not only countries with existing good quality of mobile network speed, but also countries currently falling behind, as they progress to newer technologies.

Good quality mobile network together with increasing number of IoT devices opened new opportunities to malicious actors in regards of DDoS attacks. One of first, huge DDoS attack was done by Mirai botnet. At its peak on September 2016, Mirai botnet crippled several high-profile services, including OVH and Dyn (DNS service provider)[18]. More than 600000 vulnerable IoT devices, like home routers, air-quality monitors and IP cameras peaked at 1Tbps, at that time largest attack on public record. Since then, attack scale has only increased. For example:

- In 2018, GitHub had 1.35 Tbps large attack, caused by tens of thousands of unique endpoints[19].
- 2017 Google came out mentioning, they had 2.5 Tbps large DDoS in September 2017[20]. As well, they have seen 690 million network packets per second large DDoS from IoT botnet.
- September 2021, Yandex was hit by 22 million requests per second large DDoS[21], which is similar to what Cloudflares attack, where they reported receiving 17.2M requests per second large DDoS in summer of 2021[22].
- Microsoft customer was targeted with 2.4 Tbps DDoS attack[23]

Not always its specified, what kind of devices are performing the DDoS attack, but IoT has known concerns about their security. End users are not ready to pay for the security and rather chooses cheaper, more often, less secure, devices. 5G will be a catalyst for IoT growth, aiming to provide

[17] Source: https://www.speedtest.net/global-index for Global Speeds August 2021.
[18] Source: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/
[19] Source: https://github.blog/2018-03-01-ddos-incident-report/
[20] Source: https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks
[21] Source: https://therecord.media/meet-meris-the-new-250000-strong-ddos-botnet-terrorizing-the-internet/
[22] Source: https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/
[23] Source: https://azure.microsoft.com/en-us/blog/business-as-usual-for-azure-customers-despite-24-tbps-ddos-attack/

new opportunities. IoT market is estimated to grow from 13.8 billion devices in 2021, it can reach up to 30.9 billions in 2025.

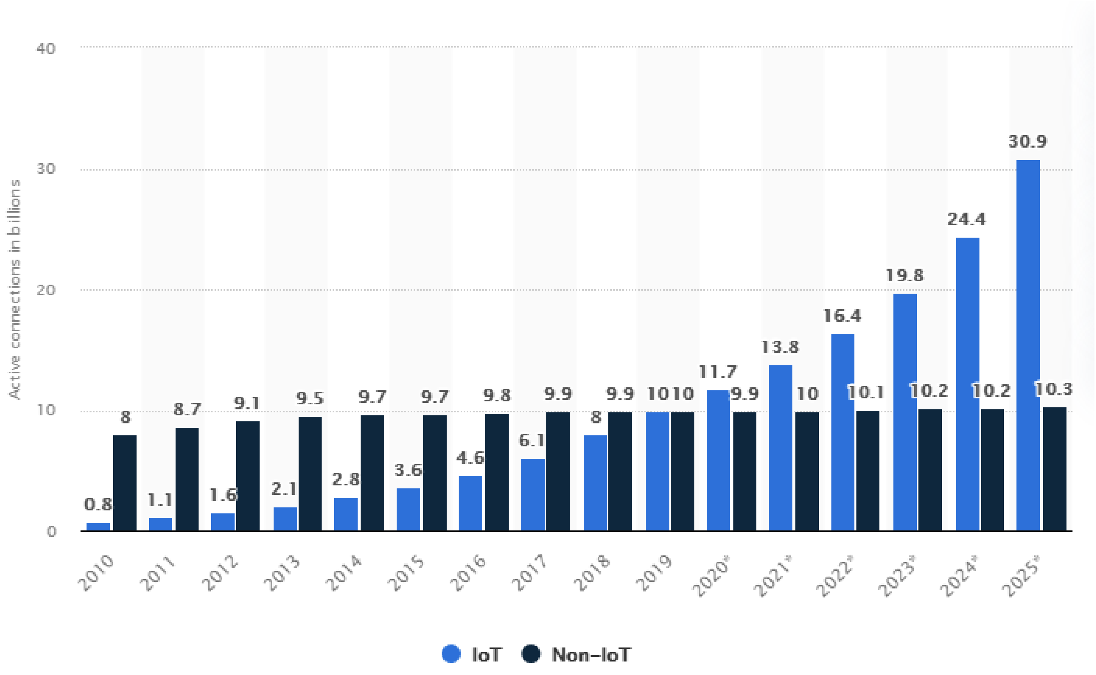


Figure 20 IoT growth estimate [24]

With Combining growing IoT market with faster speeds, its easily to imagine, how this will amplify possible DDoS attacks.

DDoS can be used in all sorts of ways, to influence elections. For example:

1. DDoS attacks on online election systems, disrupting election process and making impressions that elections are not trustable, denying people from voting. By denying people ability to vote online, it can be targeted as discrimination and not fulfilling citizens' rights to vote.
2. Even if systems are not online, DDoS attacks can be targeted at election related sites in election days, e.g. targeting sites showing official votes, citizen activity etc. Without having ability to monitor the data, malicious groups can say, that elections are rigged and not trustful as it was not possible to follow the process. It can also be pointed out, that citizens were not able to vote because they did not have access to latest data, including locations where to vote.
3. Attacks on media sites, which are highlighting objective information. This, most probably, would come together with other attacks, such as misinformation attacks, where reputable and trustful media sites are inaccessible due to DDoS and other sites, which has same goals as attackers, are available but they provide falsified information or fake news. That way its possible to feed sociality with false information affecting choices done on election day.
4. Attacks against political parties websites and initiatives forbids voters to gather additional information, e.g. candidate list, activities, aims and goals of parties, influencing them to make choices more suitable to attackers.

[24] Source: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

1.2 Lower Latency

Shorter response times (lowered latency), ability to use real time or close to real time systems. How it can affect election process?

Latency measures how long a signal takes to go from its source to its receiver, and then back again. One of the goals for each wireless generation has been to reduce latency. New 5G networks will have even lower latency than 4G LTE, with the round-trip transmission of data taking less than five milliseconds.

5G latency will be faster than human visual processing, making it possible to control devices remotely in near-real time. Human reaction speed will become the limiting factor for remote applications that use 5G and IoT—and many new applications will involve machine-to-machine communication that isn't limited by how quickly humans can respond.

While agriculture, manufacturing, and logistics will all benefit from lower latency, gamers also eagerly anticipate the 5G rollout. The combination of high speed and minimal lag is perfect for virtual reality (VR) and augmented reality (AR) applications, which are likely to explode in popularity as connectivity improvements create a more seamless, immersive experience.[7]

1.3 Longer reach, better coverage

5G is capable of working in new radio frequencies. This includes not only higher frequency for improved speed, but also lower frequency (compared to 4G) resulting in better coverage. New 700MHz frequency bands will have longer radio waves, allowing to reach more distant devices.

Better mobile network coverage enables businesses and consumers in more distant locations (e.g. factories) to use IoT to improve their daily lives. This contributes to expanding IoT market, increasing deployed IoT devices. As described by Thales group[25], IoT devices have multiple security challenges, that should be handled. Unsecure and default configuration IoT devices often become part of large botnets, that are used to perform different type of attacks. By increasing amount of internet connected devices, some percentage of them surely will be hacked and enrolled in botnets. Therefore by providing mobile network coverage to larger amount of consumers and business, will contribute to increased number of IoT devices and, consequently, increased number of IoT devices inside botnets, allowing for larger attacks.

[25] Source: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats

1.4 Slicing

5G introduces new mobile network capability called Slicing. Slicing[26] allows to create multiple virtual networks (network slices), which can be used for distinct applications with specific requirements. Previously, all network users were using same service. To guarantee access for an application, e.g. for critical and emergency services, only option was to create new physical network or deploy VPNs. Network slicing allows to create thousands of virtual, independent networks within same physical network. Slicing allows to guarantee service level for each slice, as if it were a distinct network. This is huge deal for critical infrastructure and emergency services, that can rely more on mobile networks for critical business functions. As described by Nokia[27], If an accident happens in a crowded street, the network operator can spin up a network slice dedicated to first responders enabling them to use their push-to-talk radio application and drone video monitoring fleet over the same physical network being used by the general public, without concern for congestion caused by concerned passers-by trying to live stream the event on social media.

The same functionality can be used in election process. By providing slicing, different aspects of election process can rely on mobile networks to perform critical tasks. As described in, more technologies were used in municipal elections, including high speed cameras for vote counting, digital elector registers, personal ID/Passport reading via mobile phones and other additions. Network slicing can bring multiple opportunities to enchant security and reliability of mobile networks to perform election critical tasks.

While 5G already provides increased number of supported devices, networks can still become congested in dense areas, where typically aint that many people (e.g. voting stations concentrating people from multiple areas) or due to actions performed by malicious actors. Enabling a network slice for devices used in election vote processing, can separate these devices from other mobile devices. By segregating these devices in different slice from other, we gain 2 huge advantages. First, network connectivity can be guaranteed, as long as network is running. This reduces possible connectivity issues, improves stability. Secondly, devices in segregated network have their exposure reduced (reduced attack surface), improving overall security of data transmits and devices.

[26] Source: https://www.nokia.com/about-us/newsroom/articles/network-slicing-explained/

[27] Source: https://www.nokia.com/about-us/newsroom/articles/network-slicing-explained/

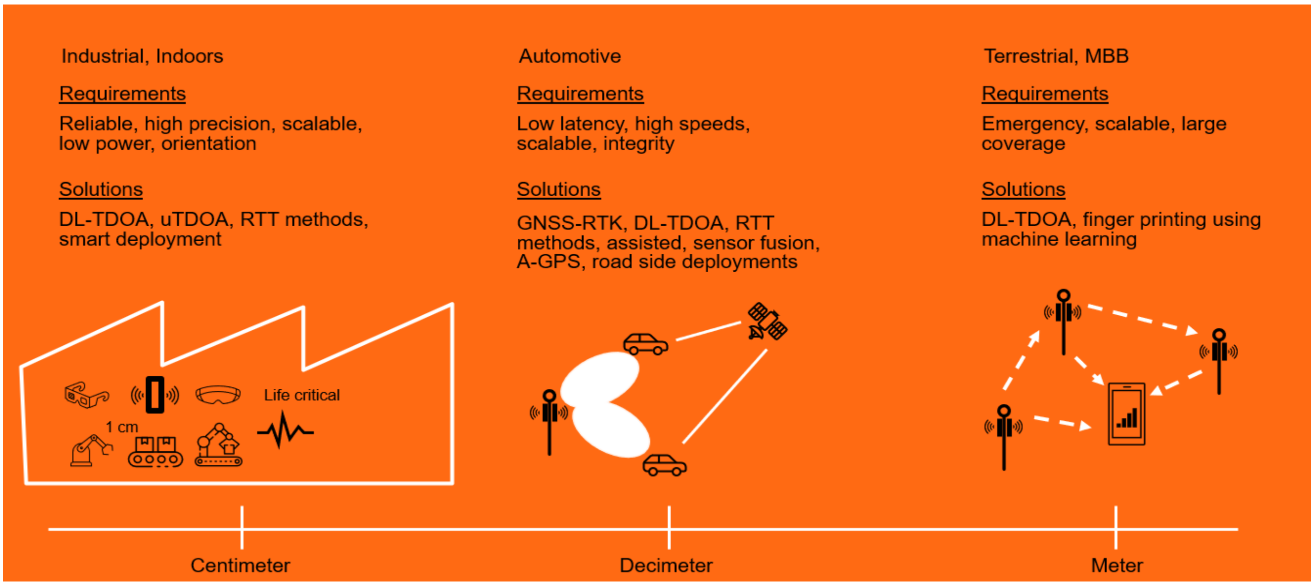
1.5 Positioning without GPS

1.5.1 5G positioning: What you need to know

The arrival of 5G delivers new enhanced parameters for positioning accuracy down to the meter, decimetre and centimetre. In this technical overview, we break down the accuracy requirements of emerging 5G use cases and explore the key features of new 3GPP 5G positioning architecture. Learn more below.

Figure 21 Potential use cases of 5G location-based services

5G positioning is a natural component in many anticipated 5G industrial use cases and verticals such as logistics, smart factories, autonomous vessels and vehicles, localized sensing, digital twins, augmented and virtual reality.The history of positioning in cellular networks dates to the mid-nineties when it was originally introduced to meet regulatory requirements of emergency call positioning. Today, with Industry 4.0, 5G positioning use cases come with a plethora of performance requirements in terms of accuracy, latency, availability, reliability, and more.



Industrial, Indoors

Requirements

Reliable, high precision, scalable, low power, orientation

Solutions

DL-TDOA, uTDOA, RTT methods, smart deployment

Automotive

Requirements

Low latency, high speeds, scalable, integrity

Solutions

GNSS-RTK, DL-TDOA, RTT methods, assisted, sensor fusion, A-GPS, road side deployments

Terrestrial, MBB

Requirements

Emergency, scalable, large coverage

Solutions

DL-TDOA, finger printing using machine learning

Figure 22 Requirements and specific solutions of 5G location-based use cases.

Some of those use cases can be seen in the figure above, together with their typical requirements, possible positioning methods and the expected accuracies. As you can see, accuracy requirements can range from meters to centimetres depending on the use case.

1.5.2 5G positioning and use cases

1.5.2.1 Mobile broadband (MBB)

Consumers with a cellular phone will also experience accurate positioning through 5G. It is expected that with some reasonable density of deployments in urban areas, 10 meters (m) positioning accuracy can be achieved. For pedestrians under a clear sky and with access to Global Navigation Satellite Systems (GNSS) such as GPS, positioning with a fusion of 5G and GNSS can be better than positioning with GNSS alone.

1.5.2.2 5G indoor positioning

Positioning of users and devices across general indoor environments, such as offices, shops, logistics, etc., was a focus area of 3GPP Release 16. The introduced features are also applicable in industrial scenarios, with possible enhancements being considered in Release 17.

1.5.2.3 Vehicular to everything (V2X)

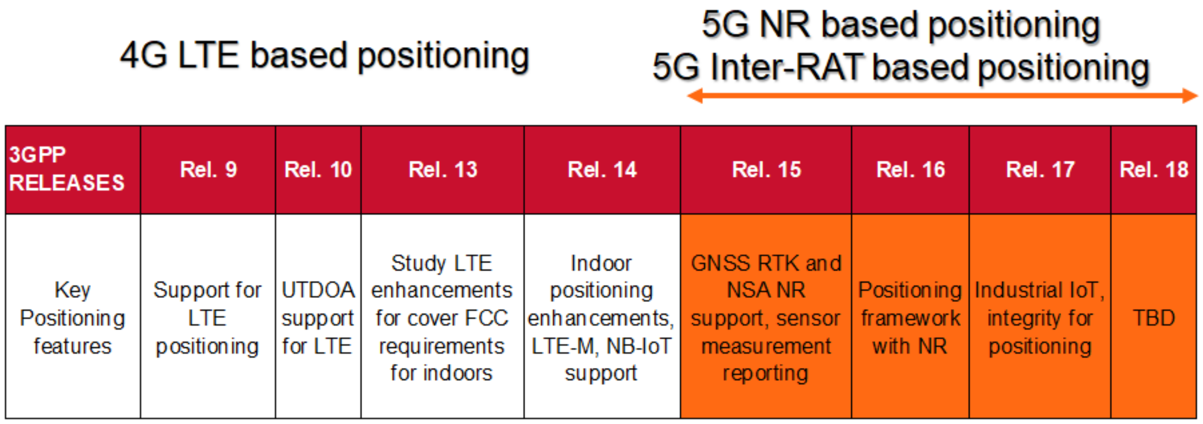
Vehicles on roads can be better positioned using a combination of GNSS and 5G positioning. The network relaying the GNSS assistance information also enables very accurate GNSS-RTK based positioning for vehicular scenarios. Street level millimetre wave (mmWave) base station deployments will play a crucial role in providing on-road very accurate positioning. Highly accurate vehicular positioning will be important for autonomous driving.

1.5.2.4 5G drone localization

Drones are expected to be widely deployed and more visible in times to come. In the future, drones can even be deployed as moving base stations and must have the ability to localize themselves for positioning. Drones will often have line-of-sight between each other and to the base stations on ground, which is a benefit. It is expected that a fusion of GNSS and 5G can provide decimetre level positioning accuracies in such scenarios, making it easier to manoeuvre drones. One example where drone localization would be necessary is in the assistance of first responders on a disaster site. Drones could be used as temporary base station deployed when the disaster site network is down and assist in keeping track of the responders' locations as well as controlling other drones.

1.5.2.5 3GPP evolution to 5G positioning

5G new radio (NR) was initially introduced as a non-standalone extension to 4G. Initially, in 3GPP Release 15, 5G device positioning was enabled by an overlay 4G network, providing 4G positioning reference signals to measure on. To leverage on the multiple sensors available in today's devices, the support for technologies independent of 3GPP radio access technologies (RAT), such as GNSS, Bluetooth, barometric pressure, WiFi signal strength, inertial sensors, and many more, was naturally extended to apply to 4G and 5G. Dedicated 5G positioning reference signals, measurements and procedures were introduced in 3GPP Release 16.



4G LTE based positioning

5G NR based positioning
5G Inter-RAT based positioning

3GPP RELEASES	Rel. 9	Rel. 10	Rel. 13	Rel. 14	Rel. 15	Rel. 16	Rel. 17	Rel. 18
Key Positioning features	Support for LTE positioning	UTDOA support for LTE	Study LTE enhancements for cover FCC requirements for indoors	Indoor positioning enhancements, LTE-M, NB-IoT support	GNSS RTK and NSA NR support, sensor measurement reporting	Positioning framework with NR	Industrial IoT, integrity for positioning	TBD

Figure 23 The features bring 5G particular releases an overview.

1.5.2.6 Key features of 5G NR positioning

5G NR provides a few enhanced parameters for positioning accuracy estimation than previous mobile generations, particularly with regards to time- and angle-based positioning methods. Below, we list a few key observations on these parameters.

- The delay error variance decreases in the order of the square of the bandwidth as the bandwidth increases. However, the angle variance is completely independent of the bandwidth. NR provides significant bandwidth improvement over LTE; while LTE provides a maximum of 20 MHz, NR provides up to 100 MHz in frequency range 1 and 400 MHz in frequency range 2.
- Received power is inversely proportional to all estimate variances. In NR, received power can be increased by beamforming. This is especially more important for numerologies with higher subcarrier spacings.
- NR provides five different choices for subcarrier spacing: 15 kHz, 30 kHz, 60 kHz, 120 kHz and 240 kHz. The subcarrier-spacing is a bit peculiar since it gives a linear increase to the angle variances, while at the same time giving only a linear decrease to the delay variance. This effect is derived from the noise variance increasing linearly with the subcarrier spacing. A natural way to counter this is to increase the RX power.
- Different antenna patterns, in terms of spacings and number of polarizations in relation to rows and columns in antenna array etc. do not affect the delay variance, but rather only the total number of antenna elements in the array matter. For the angle estimates, the variance is proportional to the inverse square of the antenna spacing. Furthermore, the number of rows and columns respectively of the antenna array gives a cubic decrease in the angle estimate variances. Typically, NR equipment carries a larger number of antennas.

1.5.2.7 5G positioning in 3GPP Release 16

The new entity, location management function (LMF), is central in the 5G positioning architecture. The LMF receives measurements and assistance information from the next generation radio access network (NG-RAN) and the mobile device, otherwise known as the user equipment (UE), via the access and mobility management function (AMF) over the NLs interface to compute the position of the UE. Due to the new next generation interface between the NG-RAN and the core network, a new NR positioning protocol A (NRPPa) protocol was introduced to carry the positioning information between NG-RAN and LMF over the next generation control plane interface (NG-C). These additions in the 5G architecture provide the framework for positioning in 5G. The LMF configures the UE using the LTE positioning protocol (LPP) via AMF. The NG RAN configures the UE using radio resource control (RRC) protocol over LTE-Uu and NR-Uu.

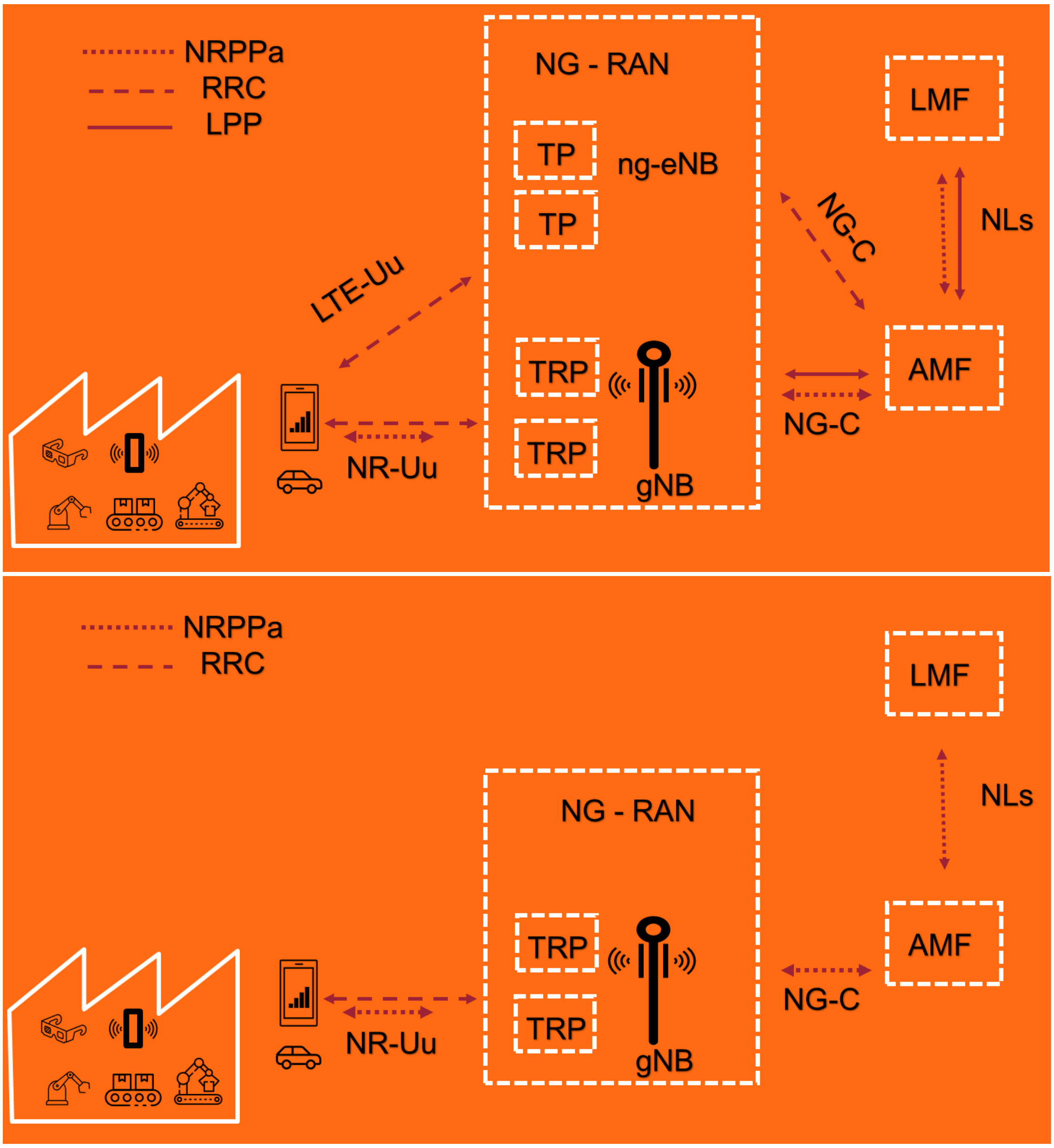
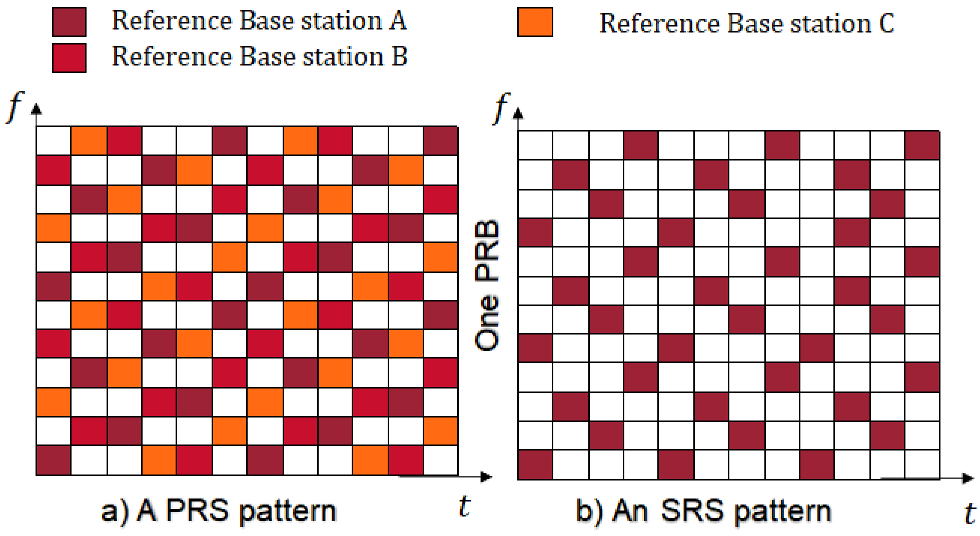


Figure 24 5G architecture supporting positioning - top: Location service 5G SA + 4G RAN network; bottom: Location service in 5G SA network.

According to ERICSON[28], to enable more accurate positioning measurements than LTE, new reference signals were added to the NR specifications. These signals are the positioning reference signal (NR PRS) in the downlink and the sounding reference signal (SRS) for positioning in the uplink. The downlink positioning reference signal (PRS) is the main reference signal supporting downlink-based positioning methods. Although other signals can be used, PRS is specifically designed to deliver the highest possible levels of accuracy, coverage, and interference avoidance and suppression. To design an efficient PRS, special care was taken to give the signal a large delay spread range, since it must be received from potentially distant neighbouring base stations for position estimation. This is achieved by covering the whole NR bandwidth and transmitting PRS over multiple symbols that can be aggregated to accumulate power. The density of subcarrier occupied in a given PRS symbol is referred to as the comb size. There are several configurable comb-based PRS patterns for comb-2,4,6 and 12 suitable for different scenarios serving different use cases. The pattern shown in the figure corresponds to comb-6 with 3 base stations multiplexed over one slot duration. For comb-N PRS, N symbols can be combined to cover all the subcarriers in the frequency domain. Each base station can then transmit in different sets of subcarriers to avoid interference. Since several base stations can transmit at the same time without interfering with each other, this solution is also latency efficient. Moreover, it is possible to mute the PRS signal from one or more base stations at a given time according to a muting pattern, further lowering the potential interference. For use cases with higher transmission loss (for example, in macro cell deployments) the PRS can be also configured to be repeated to improve hearability.

An example PRS with three base stations is shown in Figure 3 (a) below.



a) A PRS pattern

b) An SRS pattern

Figure 25: Reference signals for positioning. Shown are one configuration each of DL-PRS and UL-SRS.

In the uplink direction, 3GPP introduced the SRS for positioning in 3GPP Release 16. This new signal resolves two aspects specific to positioning. Since positioning involves measurements from multiple receiving base stations, the new signal must have enough range to reach not only the serving base station to which the UE is connected, but also the neighbouring base stations involved in the positioning process. The SRS is also designed to cover the full bandwidth, where the resource elements are spread across the different symbols so as to cover all subcarriers. Therefore, SRS is also designed with a comb-based pattern similar to the PRS. UEs can be multiplexed over the same transmitting symbol by assigning different comb patterns. To minimize interference, the UE can be configured with different SRS instances, each with independent power control loops. This allows

[28] Source: https://www.ericsson.com/en/blog/2020/12/5g-positioning--what-you-need-to-know Retrieved 14 November 2021.

SRS pointed at neighbour cells to have better hearability and keeps the interference low in the serving cell. An example SRS by a UE is shown in Fig.3 (b).

Different positioning methods may require different measurements. 3GPP has standardized power, angular and time measurement support for the PRS. A beam sweep across a resource set of PRS is illustrated in Figure 4 below.

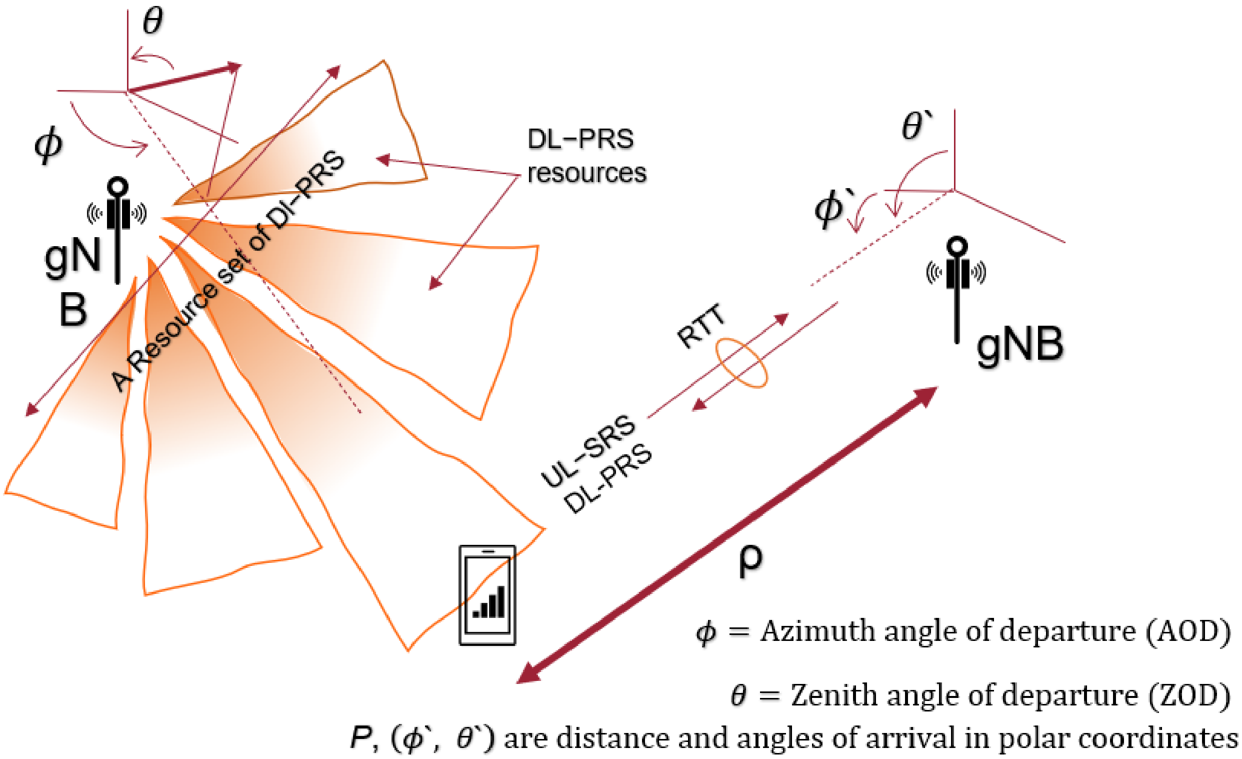

θ
ϕ
gN
B
A Resource set of Dl-PRS
DL-PRS
resources
θ`
ϕ`
gNB
RTT
UL-SRS
DL-PRS
ρ
ϕ = Azimuth angle of departure (AOD)
θ = Zenith angle of departure (ZOD)
P, (ϕ`, θ`) are distance and angles of arrival in polar coordinates

Figure 26 Reference signals for positioning. Shown are one configuration each of DL-PRS and UL-SRS.

Illustration depicting beamforming, multi-antenna aspects in 5G positioning

Each beam can be seen as a resource. Measurements are collected across one or multiple resource and resource sets. Beamforming improves the signal to noise ratio (SNR) due to beamforming gain besides providing UE location information in terms of the angle of departure (AOD) based on the beam ID accessed by the UE, while many antennas at the receiver in the uplink enables fine angle of arrival (AOA) measurements with NR. Many of these measurements are standardized to enable variety of positioning methods. Since 4G LTE, mobile networks have supported observed time difference of arrival (OTDOA), uplink time difference of arrival (UL-TDOA) and positioning methods based on power measurements. In 5G, the list of supported methods is extended to include round trip time (RTT) and angle-based positioning. The inclusion of new positioning methods and enhancements of existing positioning methods enables high accuracy positioning for several use cases in 5G.

1.5.2.8 Relevant local information

During different local elections, e.g. municipal elections, you are bombarded with information what is happening everywhere during that time. It sometimes takes time, to find relevant information for you, e.g. exact statistic for information in your region, your closest voting stations etc. Most sites are using GPS based geolocation to identify end devices location and propose local content, but its unreliable and excludes laptop and desktop computers (these might have WiFi based geo location, which does not work in rural regions). By leveraging 5G positioning in combination with MEC, its possible to detect location of user and auto-apply filtering/redirections for site content, that would highlight relevant information of elections. In more rural regions, this can highlight only their region information, while in large cities, this can reduce shown information to only your sub-part of the city. This have lots of applications:

- before elections, while looking up for candidate list, only candidates in your area are shown;
- showing voting station in your area, that you can vote in (if there are geo location-based restrictions);
- showing current voter activity in your area;
- if information is available, you could be shown how long you are expected to wait in line to vote, for each nearby voting station in real time.

While these things feel small and information can be found without use of 5G positioning, by showing local information and reducing information clutter as much as possible, can boost voter activity. When looking at situations, where voter activity in large cities are around 30%, anything that can boost voter activities can help to improve democracy and reduce effect of vote buying.

1.6 Multi-Access Edge Computing

Multi-Access Edge Computer or MEC, allows to move part or all of data processing closer to end users. This gives multiple benefits and opens new opportunities. For elections, which have some digital components, MEC can improve speed and data integrity of these systems.

From cybersecurity side, this can bring following benefits.

Faster response times

Bringing digital components to MEC, will allow faster response times. This is important aspect, when talking about missing critical system communication. Depending, what functions of election process is digitalized, MEC can provide different benefits. During Latvian Municipal Elections in 2021, digital elector registers was used, also to confirm who have voted already. By having fast response times, it makes it harder for malicious actors to do manipulations, that are time based.

By increasing digitalization within election process, MEC can be used in to achieve Machine State Integrity. Machine State Integrity is a managed security solution that captures concise machine state information and continuously monitors the machines, significantly facilitating and reducing time to threat detection. It accurately identifies, analyses and flags changes to help control risk. Such solution helps to improve security of all sorts of devices within electronical election process. When elections, like municipality elections, are usually managed by specialists in local municipalities, centralized solution with easy access to mobile networks can streamline security process.

1.6.1 Ability to communicate locally

During election process, it must be secure and transparent at same time. Any issues within process, e.g. unavailability of systems, can be used to spread misinformation of falsification of data, or reduce people rights to vote. MEC, as part of edge computing, can allow systems to easier distribute their systems and improve availability. If, for some reason, one of Edge is not available, its possible to automatically switch to another MEC and continue working.

MEC provides ability to access local services, without need to go to central core network gateway . This functionality can allow for more resilient solutions. During elections, solutions can work in real time, but if there are issues somewhere, e.g. central server becomes unavailable, or due to malicious actor, some part of mobile network gets disrupted, endpoints within MEC area can still access MEC hosted services to continue working. Of course, additional synchronization and data integrity must be performed and any error handling must be dealt with, but endpoints can keep working.

These functions can increase overall security for all sorts of elections processes. Having digital elector registers, solution can help to ensure, that data are available to voting stations and attacks, like DDoS, does not have as big impact as it could have and allows to use digital register to record voters. For situations, where more digitalized or even e-elections are being used, even more services can be protected to ensure integrity and availability of mission critical systems.

1.6.2 Improved integrity via separation

5G MEC can also boost integrity of the systems. While using MEC for different online systems, data can be stored and extracted within MEC in a way, that they are managed by MNO, instead of owner of the system. In case there are breaches, it becomes much harder to influence whole election evidence chain, as some of data are separated from original source.

MEC can be aligned to different type of use cases, where MNO role and control over the system can be adjusted, to reduce MNO influence, or allow to have more control for segregation and improve security by creating more complex system, where more parts can detect interference.

Annex Nr2 – Elections Cases Assessed

2.1 2019 European Parliament election

An election to the European Parliament was held between 23 and 26 May 2019, the ninth parliamentary election[29] since the first direct elections in 1979. A total of 751 Members of the European Parliament (MEPs) represents more than 512 million people from 28 member states[30]. In February 2018, the European Parliament had voted to decrease the number of MEPs from 751 to 705 if the United Kingdom were to withdraw from the European Union on 29 March 2019[31]. However, the United Kingdom participated alongside other EU member states after an extension of Article 50 to 31 October 2019; therefore, the allocation of seats between the member states and the total number of seats remained as it had been in 2014[32]. The Ninth European Parliament had its first plenary session on 2 July 2019[33].

On 26 May 2019, the European People's Party led by Manfred Weber won the most seats in the European Parliament, making Weber the leading candidate to become the next President of the European Commission.[6][7] Despite this, the European Council decided after the election to nominate Ursula von der Leyen as new Commission President. The centre-left and centre-right parties suffered significant losses, while pro-EU centrist, liberal and environmentalist parties and anti-EU right-wing populist parties made substantial gains[34][35].

On 7 June 2018, the Council agreed at ambassador level to change the EU electoral law and to reform old laws from the 1976 Electoral Act. The purpose of the reform is to increase participation in elections, raise understanding of their European character and prevent irregular voting while at the same time respecting the constitutional and electoral traditions of the member states[36]. The reform forbids double voting and voting in third countries, thus improving the visibility of European political parties.[10] To avoid double voting, contact authorities are established to exchange data on voters, a process that has to start at least six weeks before the elections.

The European Parliament gave its consent on 4 July 2018 and the Act was adopted by the Council on 13 July 2018. However, not all member states ratified the Act prior to the 2019 elections and therefore this election took place in line with the previous rules[37]. On May 25, 2019, regular elections to the European Parliament were held. Latvia had to elect eight representatives. In these elections Latvia was one constituency.

[29] "European elections: 23-26 May 2019". European Parliament. Archived from the original on 25 February 2019. Retrieved 11 March 2021.
[30] "Turnout | 2019 European election results | European Parliament". election-results.eu.
[31] "Size of Parliament to shrink after Brexit" (Press release). European Parliament. 7 February 2018. Retrieved 28 May 2021.
[32] "Brexit delayed until 31 October - UK and EU agree". BBC News. 11 April 2019. Retrieved 11 April 2019.
[33] "European elections 2019: what's next? (infographic)". European Parliament. 30 April 2019. Retrieved 8 June 2021.
[34] Smith, Alexander (27 May 2019). "European Parliament elections: 5 takeaways from the results". NBC News. Retrieved 27 May 2021.
[35] Mudde, Cas (11 October 2019). "The 2019 EU Elections: Moving the Center". Journal of Democracy. 30 (4): 20–34. doi:10.1353/jod.2019.0066. ISSN 1086-3214.
[36] "European Parliament elections: Council reaches agreement on a set of measures to modernise EU electoral law - Consilium". Consilium.
[37] "Reform of the Electoral Law of the EU". European *Parliament*. Retrieved 14 June 2021*.*

There were 1,000 polling stations in the European Parliament elections, of which 44 polling stations were set up in the EP elections for the first time in 38 countries outside of Latvia, as well as two special polling stations - the Riga Prison Polling Station and the postal polling station.

474,390 or 33.5 per cent of eligible citizens took part in the European elections, of which 2,955 or 91.3 per cent of the number of voters registered abroad. Compared to the 2014 European elections, voter turnout has increased by 3.3 percentage points. For comparison, 445,225 or 30.2 percent of voters participated in the 2014 EP elections.

In the European Parliament elections, 16 lists of candidates for deputies of parties and party associations participated in the Latvian elections, which included a total of 246 candidates for deputies, which was 76 candidates more than in the previous elections in 2014. Thus, 31 candidates applied for one of the eight seats of Latvian MEPs.

Five lists of candidates for deputies won seats in the European Parliament: “New UNITY” - 124,193 or 26.24 percent of the vote and two seats, the “Social” Social Democratic Party - 82,604 or 17.45 percent of the vote and two seats, the National Union for All Latvia! ”-“ For Fatherland and Freedom / LNNK ”- 77591 or 16.4 percent of votes and two seats, for Development / For! - 58763 or 12.42 per cent of votes and one deputy seat, “Latvian Russian Union” - 29546 or 6.24 per cent of votes and one deputy seat.

The following MEPs from Latvia were elected to the European Parliament: Valdis Dombrovskis, Sandra Kalniete from the list of candidates for the New Unity, Nils Ušakovs and Andris Ameriks from the Social Democratic Party of Harmony, Roberts Zīle and Dace Melbārde from the National Union for All Latvia! For Fatherland and Freedom / LNNK, Ivars Ijabs from Development / About! and Tatjana Ždanoka from the list of candidates for deputies of the Latvian Russian Union.

473,260 valid ballot envelopes and 470,460 valid ballot papers were received in the elections.

Of all the signs, 387,175 or 82.3% of the signs were changed, ie those in which voters made at least one “+” or deletion. Compared to the 2014 elections, the proportion of amended ballot papers has not changed significantly - in the 2014 European Parliament elections, 83.3% of amended ballot papers were received.

The number of ballot envelopes without valid stamps this time is 2801 or 0.6% of the total number of valid envelopes. This includes blank ballot envelopes, ballot envelopes with signs of various contents, torn signs or signs of another constituency.

The right to participate in the EP elections was granted to Latvian citizens and citizens of other EU member states who resided in our country, were registered in the Latvian Population Register and the Latvian Voter Register. To vote, a voter must be at least 18 years old on election day. Pre-established voter lists were used to register voters in the EP elections. Each voter was registered at a polling station where they had to vote on election day. Initially, voters were included in the polling station most suitable for their registered place of residence, but from March 16 to May 7, 2019 (the 18th day before the elections) the polling station could be changed. There were two ways to register to vote in another poll:

1. online - using the station exchange e-service;
2. in person - by applying for a change of district in any local government declaration of residence.

Latvian citizens were automatically included in the Voter Register, but citizens of other EU member states residing in Latvia and wishing to exercise their voting rights in Latvia had to register with the Central Election Commission by April 25, 2019 (the 30th day before the elections).

The EP Election Law provides several participations options for voters in EP elections. These options were:

1. to vote at their polling station on election day from 7.00 to 20.00.
2. to vote in advance when the polling stations worked a few hours a day - from 17.00 to 20.00 on 22 May, from 9.00 to 12.00 on 23 May, from 10.00 to 20.00 on 24 May.
3. to vote at his / her place of residence if, due to his / her state of health, it was not possible to vote at the polling station, the voter is a caregiver or is in custody in a place of imprisonment or temporary detention.
4. to vote abroad by post or at a polling station abroad.

In turn, those eligible Latvian citizens living in one of the EU member states had the opportunity to choose - to vote for the lists of candidates for Latvian MEPs or to register to vote in the host country and vote for candidates for MEPs in that country. By choosing to vote in the country of residence, the voter lost the right to vote for Latvia in the respective elections.

2.2. USA Presidential Elections in 2016

In preparing reflections on the topic of the disruption of the US presidential election in 2016, the following sources were primarily used:

- The “Report On The Investigation Into Russian Interference In The 2016 Presidential Election” (Mueller, Report On The Investigation Into Russian Interference In The 2016 Presidential Election, 2019)[38].
- The book “Securing the Vote: Protecting American Democracy” (National Academies of Sciences, Engineering, and Medicine, 2018)[39].
- And the article in news stating “NASHVILLE, Tenn. (WZTV) — A fake Tennessee Republican Twitter account is back in the spotlight after a mention in the Mueller Report. The account was linked to Russia and had more than 150,000 followers” (Abell, 2019)[40].

Cyber activities before, during and after the US 2016 elections, attributed to the Russian Federation by the above-mentioned sources, took the form of two types of infringing operations: the social media campaign and the hacking-and-dumping operation.

The first recorded, was a campaign on social networks, which was to be conducted from 2014 on Facebook and Twitter accounts managed by the Russian organization Internet Research Agency (IRA). The IRA's activities are expected to include conducting political campaigns on social media on behalf of American individuals and entities, as well as staging of political rallies within the United States (Mueller, chapter "Russian social media campaign", pp. 4, 2019). The intention of such actions was to create and obtain an appropriate community for the dissemination of misinformation. The motivation was to be the assumption that “the Russian government perceived it would benefit from a Trump presidency” (Muller, 2019).

The second of the main activities are considered to be hacker attacks in favour of further dissemination of misinformation. These are attributed to the Russian Intelligence Service, known as the Main Intelligence Directorate of the General Staff of the Russian Army (GRU), and were to

[38] Source: https://www.justice.gov/archives/sco/file/1373816/download Retrieved 18 may 2021.
[39] “Securing the Vote: Protecting American Democracy” (National Academies of Sciences, Engineering, and Medicine, 2018) https://doi.org/10.17226/25120.
[40] Source: https://www.vox.com/policy-and-politics/2017/10/19/16504510/ten-gop-twitter-russia Retrieved 18 may 2021

include cyber-intrusion and the publication of Hillary Clinton-damaging materials (Mueller, chapter "Russian hacking operations", pp. 4, 2019).

Referring to the above sources, it can be stated that Russia has used different types of cyber-attacks and technological tools in order to support disinformation needs. Those were as fake web pages and social media accounts, attacks to selected services and resources (e-mail servers, confidential data bases etc.) or stealing social media credentials and others.

In aftermath of 2016 USA presidential elections a special investigation leaded by special counsel R. Muller was conducted to investigate the level of foreign deliberated meddling of USA presidential elections of 2016. The Special Counsel's investigation recognised that Russia interfered in the 2016 presidential election principally through two types of operations. Mainly, a Russian entity carried out a social media campaign that favoured presidential candidate Donald J. Trump and disparaged presidential candidate Hillary Clinton. Secondly, a Russian intelligence service conducted computer-intrusion operations against entities, employees, and volunteers working on the Clinton Campaign and then released stolen documents. The investigation also identified a breach in a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spear phishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election.

Lessons learned and actions taken for USA 2020 president elections:

- A clear oversight is required by federal authorities rather than a local state election official. This included a preparatory cybersecurity testing of each county voting system elements, to secure resilience to the cyber-attacks and meddling actions by foreign powers.
- Awareness campaigns required for all directly involved personal in administration of the elections. This includes U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities.
- A particular focus should be given to resilience of each presidential campaign platforms and communication within.
- A monitoring and prompt action on abnormal activities on various social media platforms.

As outlined in declassified document of NSI – Foreign treats to the 2020 Federal elections. Integrated lessons learned from 2016 elections has resulted in high confidence that no indication that any attempt to interference by altering technical aspects of the voting process including voter registration, ballot casting, vote tabulation or reporting of results has been successfully conducted.

Furthermore, it was identified that high volume of unsuccessful attempts to intrude election related networks. Even those some has been breached it didn`t cause a serious leak`s compromising the outcome of elections.

After all, the report outlined that foreign actor would influence the politics have multiplied. The spectrum of interest linked to public opinion ranged from political, economic and foreign relation/military perspective. This has resulted in intangible amount of influence which are on a verge of freedom of expression thus undermining Democratic values of society.

Finally, the actions taken by outgoing president by false acquisitions of voting alterations have led to 6th January 2021 United States Capitol attack. "Stop the Steal" movement[41] have grown from right wing extremist and boiling of alternative reality on social media. This type of national meddling may become a new treat for the future and will be drawn as lessons learned from 2020 USA presidential election

[41] Source: https://www.justsecurity.org/74622/stopthesteal-timeline-of-social-media-and-extremist-activities-leading-to-1-6-insurrection/ Retrieved 18 may 2021

2.3. Latvian Municipal Elections in 2021

Year 2021 in Latvia was election year for local governances or municipalities. Traditionally, municipal elections in Latvia are organized in late May or early June (from 31st of May till 5th of June in 2021). The candidate and elector registers are organized in hard copies on paper, the same goes for ballots and voter identification process. All steps of the process (except for post-election vote counting) has been manual labour with no digitalization or automation. This approach has allowed to avoid threats and risks associated with digital domain. Human error during steps of the process, such as inputting numbers in the system, handing out ballot envelopes or identifying the voter, is considered less impactful. International voting is organized using embassies in different countries where voters are living, however, the process has been the same – all manual labour, no voting by mail or any other means that does not involve direct human-to-human contact.

The customized election IT system is designed by the Centralized Election Commission of Latvia with close collaboration with the best cyber security experts in Latvia, including, but not limited to NATO Excellence Center, the Information Technology Security Incident Response Institution of the Republic of Latvia (CERT.LV) and the Latvian state security service, thus extensive testing of the system is performed before it is used in actual election process.

In local governance or municipal elections in Latvia in 2021 electronical vote counting by high-speed scanners were introduced. The world-wide pandemic might have played a catalyst role for this process innovation. In 2021 manual labour has been minimized and even international voting by mail was organized. The solutions are based in IT technology by using:

1. digital candidate and elector registers,
2. automated personal ID or Passport readers,
3. real-time information exchange between election precincts
4. and self-registry for international voting by using Latvian national government services portal.

All these changes unburden the local election precinct commission member manual workload and reduce the physical contact between electors and the election commission members. For the elector register viewing and elector identification an application on smart devices like smartphones or tablets were introduced. In several cases, there were no alternatives for data connection as the mobile network. No practical trial in national level was organized before and no empirical data was available to base the factual security threat aversion assessment.

The new technologies and solutions used in the local governance or municipality elections in Latvia in 2021 is a necessary step to improve the efficiency of the election process, however, this also requires new cyber-security threat management. In the past the amount of computing devices in election process have been scarce. For each election precinct there had to be a computer, a high-speed scanner, and either wired or wireless network connection.

In 2021, however, the estimated amount of computing devices in each precinct increased in sevenfold. Therefore, new threats come into play, regarding mixed operating systems, mixed network connections and one of the main challenges – the use of mobile network to organize election process data exchange in real-time. As in the current 4G network there are no capabilities to allocate a specific slice of the network for secure data exchange for specific use, the threats of external forces trying to impact the election process are in the highest possibility there ever has been.

Also, potential threats by other connection protocols, like Bluetooth for example, propose new challenges for all the security services, election organizers and connection providers. There are municipalities in Latvia that have developed local closed networks with adequately high security, however, there also are others that rely only on public network solutions that are prone to potential cyber-security attacks, from local attacks using close-range connection vulnerabilities, to data transfer interceptions of false data insertions.

The potential of 5G mobile networking could provide the necessary security of network for such high sensitivity processes as elections. The potential outcome of manipulating the elections might create soil for external interventions in other country systems and processes. With the potential network slicing technology provided by 5G most of the security threats could be mitigated or averted.

Fallback solutions to the digital registers.

To ensure, that there would not be possible fraudulent actions from electors, i.e. voting in multiple precincts in case of network or register system downtime, a fallback solution to avoid these situations was implemented by providing hard copies of all electors and separate two-envelope system to ensure the possibility to identify elector, while still providing the opportunity to vote anonymously. After restoring the connection with network or restoring the register system downtime, the voters would be manually registered to ensure, that no fraudulent actions have been performed.

Overall, the elections took place with no serious violations of the election process. However, the activity of the elections was at the historical lowest level, as less than 40% of voters took place in the election process. In Jelgava city, the voter activity was under 30%. A dangerous tendency, as the number of votes needed to be elected in local municipality have decreased to around 150 votes in national importance cities and even under 100 in rural territory municipalities.

To validate the hypothesis, that election activity can be monitored using mobile provider network activity data, on the election day LMT organized exit-polling, after the voters had given their vote.

The polling was carried out as follows:

In person 05.06.2021 from 10:00 to 14:00 at polling station no. 196 “LLU Sports Hall”, Tērvetes Street 91D, Jelgava the following tasks were performed:

1. Voters counted:

Voters were added to the overall statistics when they leave the polling station. In addition, the time at which this was done was recorded.

2. A voter survey was conducted asking following questions:

    1. Do you want to take part in the survey? Yes/no
    2. Did you vote in this polling station? Yes/no
    3. Do you have a mobile phone with you? Yes/no
    4. Who is your mobile phone operator? LMT/TELE 2/BITE/Other
    5. Would you support e-elections in Latvia? Yes/no

3. It is necessary to measure how long one voter spends in the polling station.

It was important to measure at least 10% of the voters who are counted.

In practice, the measurement was performed by recording the entry time and recording the output on paper / computer.

An exit polling team of three was present in Jelgava. Two team members performed the exit polling surveys and one member took the measurements of average voter time from the whole voting process perspective – from entering and identifying himself to exiting the premises after making the decision.

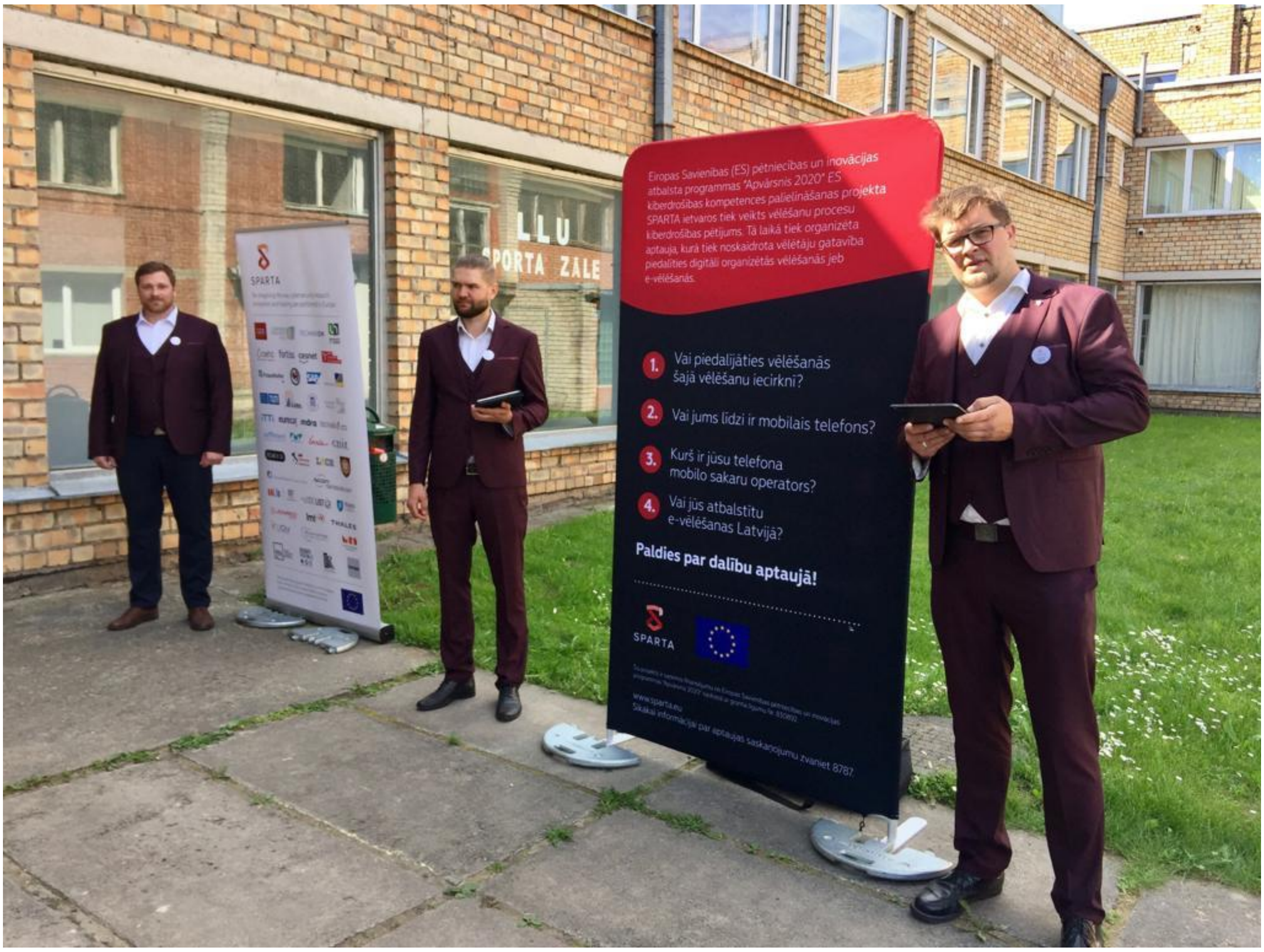

SPORTA ZĀLE
SPARTA
Eiropas Savienības (ES) pētniecības un inovācijas atbalsta programmas "Apvārsnis 2020" ES kiberdrošības kompetences palielināšanas projekta SPARTA ietvaros tiek veikts vēlēšanu procesu kiberdrošības pētījums. Tā laikā tiek organizēta aptauja, kurā tiek noskaidrota vēlētāju gatavība piedalīties digitāli organizētās vēlēšanās jeb e-vēlēšanās.
1. Vai piedalījāties vēlēšanās šajā vēlēšanu iecirknī?
2. Vai jums līdzi ir mobilais telefons?
3. Kurš ir jūsu telefona mobilo sakaru operators?
4. Vai jūs atbalstītu e-vēlēšanas Latvijā?
Paldies par dalību aptaujā!
SPARTA
www.sparta.eu
Sīkākai informācijai par aptaujas saskaņojumu zvaniet 8787

Figure 27: LMT team in Jelgava

After the activities at the Jelgava district, LMT representatives did counting (counting only) for 2-3 hours at other districts - at other pooling stations of Jegava, in Ikšķile and in Sigulda and Skrīveri.

The main purpose of this exit polling was to determine the amount of LMT clients, as well as to get the opinion on possible digital elections in future. During the exit polling 43% of all participants on the election day in this election precinct were interviewed and 34% of those were LMT clients. This gives us perfect distribution among all three Latvian mobile providers and ensures that the correlation between mobile data activity and election activity is eligible.

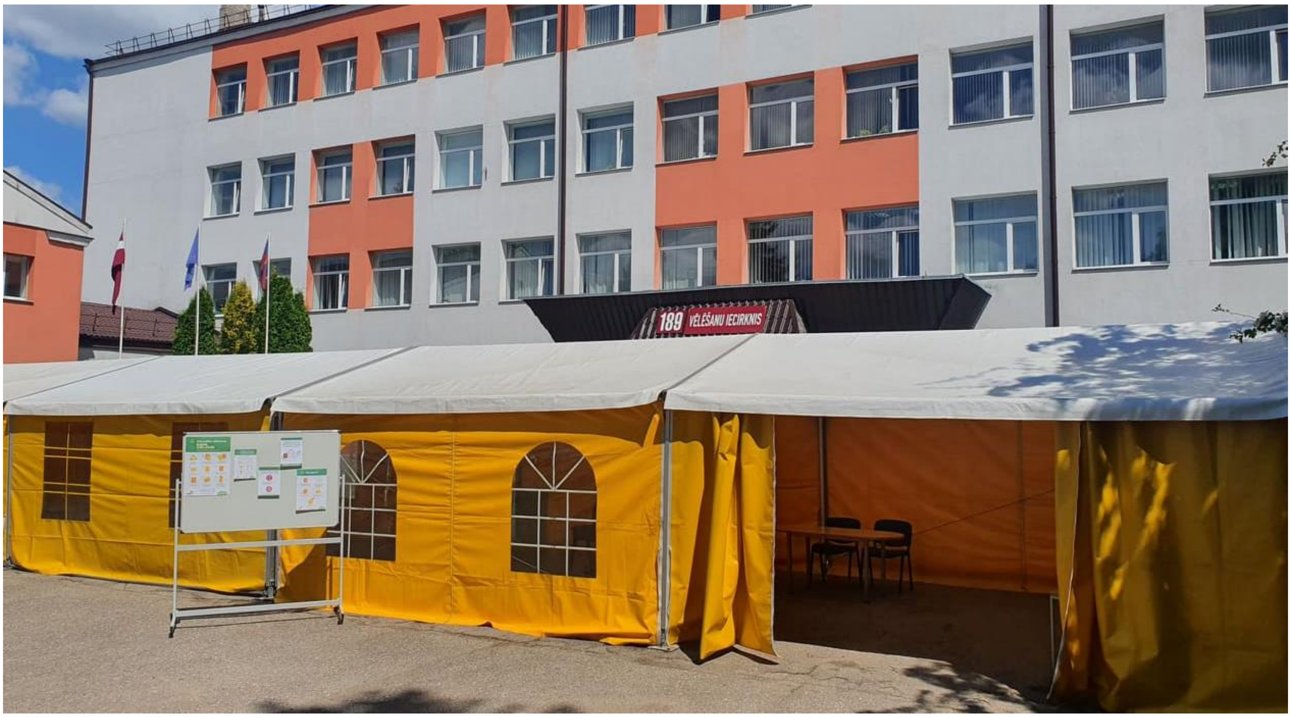


Figure 28: Outdoors polling station in Jelgava due to Covid-19 restrictions

2.4. Estonian E-elections

E-elections in Estonia as a phenomenon should be first approached from the wider perspective of Estonian strategic digital transformation context.

Estonia has been decisive about its orientation towards a digital growth strategy since it regained its independence in 1991. It was from the start defined as a national strategy rather than a set of policies. The political focus since 1992 was on developing IT as a general-purpose socio-economic skill to be shared by as many citizens as possible. Strong political decision-making regarding digital strategy is a cornerstone feature. Estonia has never had a central digital agency. Digital agendas and systems are decentralized. Government ministries and their agencies have direct responsibility for their ICT strategies, investments, and data. Information architecture and departmental ICT strategies are all decentralized.

Estonia has had relatively advanced IT human capital since, in the 1960s, it began investing in its Institute of Cybernetics (within the USSR). Other Soviet republics invested in math and engineering; meanwhile, Estonia concentrated on computer programming[42]. This strong cybersecurity tradition resulted in the NATO Cooperative Cyber Defence Centre of Excellence is set up in Tallinn in 2008 (after an unfortunate DDoS attack in 2007).

Bold strategic moves were made by Estonian Government that later enabled e-elections. Firstly, it was the launch of electronic ID for every Estonian and giving out active certificates to everyone in 2001. Second, it is the X-Road - interoperability platform for existing decentralized databases for the public and private sector. More than 2,300 public and private services use X-Road, according to

[42] Online participation in Estonia: active voting, low engagement, M. Kitsing, ICEGOV '11: Proceedings of the 5th International Conference on Theory and Practice of Electronic GovernanceSeptember 2011 Pages 20–26 https://doi.org/10.1145/2072069.2072073

Kattel and Mergel[43]. Together, X-Road and the digital ID (both introduced in 2001) make it possible to sign any contract digitally, access essentially any public service, file taxes, vote, etc. The Finnish government also uses X-Road.

Estonia ensured that most of the public services its government offers can be done online without visiting an office in person. In fact, there are only three governmental services that require physical presences in Estonia, which are getting married, getting divorced, and buying a property. The Estonian government has put a lot of effort into digitalization, but the key aspect of Estonia's digitalization strategy success relies on the digitalization of trust. That trust has been created by securing efficient services to its citizens based on transparency and highly focused on security.

In 2005 Estonia became the first country in the world to hold nationwide elections using this method, firstly, as the use-case for electronic IDs and to promote its popularity. Moreover, in 2007 Estonia became the first country to use i-Voting in parliamentary elections (e-Estonia, n.d.). In 2011, Mobile ID functionality was added. 44% of Estonians use the electronic voting option. Regular postal voting (anonymous envelope) is also a provided option besides i-Voting and visiting the polling office.

Procedural features of the i-Voting that add a layer of protection against election fraud include: (1) a vote can be cast as many times as wanted and the last vote is saved (this functionality serves as a protection layer against “buying” of votes) and (2) an option that was introduced in 2014 - to check the accuracy of vote allocation from another iOS or Android mobile device by any i-Voting participant using a QR code. About 4% of election participants use this second feature to check the correct allocation of their votes. The third procedural layer is deletion of i-Voting data to lessen the risks associated with data leakage.

i-Voting operates on all major operating systems macOS, Linux, Windows. In the case of a DDoS attack the course of action would be to block all international data traffic. 5G Slicing functionality could possibly be applied to mitigate risks, for more details, see Annex Nr.1 - Technical - Slicing.

In 2013 and 2014 a security analysis of the Estonian Internet Voting System was conducted by a group of researchers from University of Michigan. This analysis was based on in-person election observation, code review, and adversarial testing. One of the first findings was how much Estonia relies on a complicated set of procedural controls, however, those controls were found to be inadequate to achieve security or transparency. In 2014 it was concluded by this group that digital voting is too difficult a problem, “due to the need to ensure accurate outcomes while simultaneously providing a strongly secret ballot”. The researchers suggest that the fundamental advances are needed and perhaps some of the 5G functionality can come to the forefront.

[43] Kattel, R. and Mergel, I. (2018). Estonia’s digital transformation: Mission mystique and the hiding hand. UCL Institute for Innovation and Public Purpose Working Paper Series (IIPP WP 2018-09). https://www.ucl.ac.uk/bartlett/public-purpose/wp2018-09

Annex Nr3 – Interviews

During the study, in order to gain more insights into election process and current associated risks, interviews were held with experts involved in current election process from different viewpoints. Following experts were interviewed:

- Kārlis Podiņš, threat analyst at CERT.LV;
- Jānis Dēvics, Head of municipal election commission at Jelgava municipality;
- Māris Alberts, Senior researcher, Head of Real Time Systems Laboratory.

During interviews, same questions were asked to all interviewees, to understand their point of view on current and future trends and associated risks for election process. Not all of interviewed experts are directly involved in election process or activities involved in improving election process.

What are current main cybersecurity risks?

Kārlis Podiņš

CERT.LV expert sees, that data integrity is one of main risks for current election process. How to make sure, that data haven't been altered, or the algorithm behind doesn't have backdoors, that allows specific people to vote multiple times.

Another risk is how to have transparent online electorate register, so independent observers can see and understand the election process. Paper process is easier to follow and understand, it does not require specific knowledge, to follow up on vote counting etc. Digital process might require specific knowledge for independent observers of the process and how data integrity is maintained.

Jānis Dēvics

The main challenges are linked with stabile and accessible network in every polling station. There are three main network options to provide data connection to all the election equipment:

1) optical network from Jelgava city municipality, this is the most secure solution, as the network is constantly monitored and used only for the needs of city governance and infrastructure,
2) Commercial landline network. It is mostly stable, but the security measures are in hands of network provider, thus the threats are unknown in potential amount,
3) In polling stations with no hard-line network, we are using commercial mobile network and the threats are like the commercial landline networks.

To mitigate these risks, it would be necessary to provide closed network solution, covering all polling stations in Latvia.

Māris Alberts

Main cyber threats are associated with possible vulnerabilities embedded in election digital equipment allowing to manipulate election outcome. Persistent and highly motivated third parties could breach election process systems and processes to deploy backdoor which enables them to manipulate the election outcome. Vulnerabilities can be found in different sources, e.g. from existing, undocumented functionality at hardware and software levels. Finally, the insider treat should not be neglected, and more mitigating actions should be implemented to reduce such risk. Insider threat – a major risk.

How they see digital transformation in election process within next 5 years?

Kārlis Podiņš

Electronical Online electorate register is already huge step into digitalized voting system. Process might move towards online voting. But it will have increased number of cybersecurity risks, which do not exist at this point, as most critical processes were in paper.

Voting using Mobile e-signature might be an option, if process moves towards online voting. If solution is there for digital signatures, it might be valid for voting.

Jānis Dēvics

It is hard to say. The Municipal elections of 2021 already came with huge digital transformation when compared with the previous elections. The lists of voters are digitalized. Documents can be scanned with phones. Faster information exchange with Central Election Commission and real-time data delivery about the activity. The next steps might be linked with the opportunity to vote from home using a computer or smart device. Will this happen in next 5 years is hard to say. The rate of digital transformation in Latvia is growing, so, it might be possible.

Māris Alberts

A voter’s register is a must. Open digital voting for conducting referendums etc. at municipal level and improve process transparency in digital voting, by allowing anyone to validate if votes have been counted currently and gain confidence.

What will be the main challenges for digital transformation in elections?

Kārlis Podiņš

Digital transformation might increase integrity risks of election process, if during digitalization, low cost options will be chosen. For example, during transformation, election process might lose paper trail documents. By attacking election systems and erasing evidence, it can become harder to follow up on what has happened, because there are no digital evidences left and paper trail no longer exists.

Conspiracy theories can make bigger impact, the more complex election process becomes, the harder it is for average voter to understand all the critical controls in the process. This can spark more conspiracy theories of all kind. Overall, it might be easier and cost-effective to rig elections by creating fake news and misinformation around elections to influence voters, than to hack the systems.

Jānis Dēvics

As with everything – competent specialists, funding, and clear vision of the result we want to achieve. The election commission members also will have to be ready to adopt to the new solutions, so proper education in digital solutions will be required. We, however, cannot fully give up the non-digital election process, as there are a lot of elderly persons who will not be able to participate in digital elections, but democracy requires that each and every person should be able to give his vote.

Māris Alberts

A paper trail should be kept in any election to reassess the results of voting, if that's needed. Any new element introduced in election digitalisation process should be extensively verified first. As a best practice referencing to principles governing German law of elections are advised.

What are current IT challenges?

Kārlis Podiņš

Currently there might be challenges, how to collect log files of all the activates done by involved parties. During municipality elections, mobile phones were used to mark voters in online register. If something happens, log files from end devices might be needed to review, who performed what type of activity.

Jānis Dēvics
Mostly network connection in remote areas. The competence of polling station staff is sometimes an issue, the digital skills are not sufficient to react to unforeseen complications and find solutions without expert on premises.

Māris Alberts
Digitalisation of election by no means are more rapid than a “paper voting”, underwater stones may throw back or halt digitalisation process for ages. In case of Latvia digital voting transformation, I would recommend dumping provincialism and narrow-mindedness by rigorously analysing Germany`s secret ballot process. Furthermore, to start with drawing a full threat tree for any secret or open ballot process to derive most sustainable risk management plan. Risk management plan should be valid for pre-election and post as well as Election Day. Moreover, a paper trail storage time should be extended.

How cybersecurity risks are validated, when improving election process?

Kārlis Podiņš
CERT is involved in validating security of digital components of election process, but this can be improved by involving their experts in earlier stage of designing new parts of election process. That way they can provide suggestions earlier in the process.

Jānis Dēvics
This is mostly done by Central Election Commission. They are assessing the potential threats by inviting experts from the specific discipline. IT, physical security and others. It would be beneficial to include the local election commissions in earlier stages, so we would be able to prepare more accordingly.

List of Abbreviations

Abbreviation	Translation
3GPPP	3G partnership project
5G	Fifth generation of Mobile Network
5G NR	5G New Radio
5GC	5G Core
API	Application programming interface
BS	Base station
D2D	Device to Device communication
DDoS	Distributed Denial of Service
eMBB	enhanced Mobile Broadband
ETSI	European Telecommunications Standards Institute
HAPS	high-altitude platform stations
ISP	Internet Service Provider
LEO	Low Earth Orbit
MEC	Multi-Access Edge Computing
MIMO	multiple-input and multiple-output
mMIMO	Massive MIMO
mMTC	Massive machine-type communication
mmWave	millimeter wave
MNO	Mobile Network Operator
NR-U	New Radio Unlicensed
NTN	Non-Terrestrial Network
ProSe	Proximity Services
QoS	Quality of Service
UE	User Equipment
uRRLC	Ultra-reliable and low-latency communication

List of Definitions

- Slicing – 5G network slicing is a network architecture that enables the multiplexing of virtualized and independent logical networks on the same physical network infrastructure. Each network slice is an isolated end-to-end network tailored to fulfil diverse requirements requested by a particular application.

- Enchanted Mobile Broadband - mobile broadband services, with faster connections, higher throughput, and more capacity.

- MEC – a network solution that provides services and computing functions required by users on edge nodes. It makes application services and content closer to users and implements network collaboration, providing users with reliable and ultimate service experience.

- Non-Terrestrial Network - term for any network that involves non-terrestrial flying objects. The NTN family includes satellite communication networks, high altitude platform systems (HAPS), and air-to-ground networks

- 5G – 5G is a fifth-generation mobile network technology, operating on sub-6 GHz and 20–60 GHz millimetre-wave (mmWave) frequencies. Its technological enhancements include a dramatically faster speed, greater connectivity, greater reliability and reduced latency. 5G standard is developed by 3GPP, starting from 3GPP. Releases 15 to 17 were used for this study.