FINDINGS AND ASSESSMENT REPORT

OF

INTERNET VOTING TASK FORCE (IVTF)

ON

VOTING RIGHTS OF OVERSEAS PAKISTANIS

EXECUTIVE REPORT 2018

Confidential

Table of Contents

1 EXECUTIVE SUMMARY

1.1 INTRODUCTION

On April 12, 2018, the Honorable Supreme Court of Pakistan convened a historic session (Ref: Const.P.NO.2/20118-SCJ) pertaining to the voting rights of overseas Pakistanis. This session was presided over by Chief Justice of Pakistan, Justice Saqib Nisar, and included members of various political parties, IT experts from Pakistani universities, concerned citizens, and members of the media. On this occasion, NADRA demonstrated iVOTE, an e-voting platform that would allow overseas Pakistanis to cast their votes for the forthcoming General Elections using the Internet.

All parties in attendance strongly affirmed the right to vote for overseas citizens. However, invited IT experts aired concerns about the potential security issues posed by deployment of this system. As a result, on directions of the Supreme Court of Pakistan, the Election Commission of Pakistan constituted a Task Force on April 19, 2018, to undertake a technical audit of the iVOTE platform.[1]

This document presents the views and findings of this Task Force.

1.2 IMPLICATIONS

To put Internet Voting in proper context and to highlight the magnitude and gravity of this decision before us, we would like to draw the reader's attention to the following points:

1. Online voting systems have thus far catered to relatively small numbers of voters. If we consider the largest deployments of Internet voting in the world, a mere 70,090 online votes were cast in the Norwegian elections in 2013, 176,491 in the 2015 elections in Estonia, and over 280,000 votes in the state election in New South Wales, Australia. In contrast, iVOTE, if deployed in the forthcoming General Elections, will cater to an estimated more than 6 million overseas voters, and will be the largest ever deployment of Internet voting in the world by far.

2. Leading international cybersecurity professionals have repeatedly voiced serious concerns regarding the security of Internet voting. Researchers have discovered vulnerabilities and launched devastating attacks on such systems (including those deployed in the US, Estonia and Australia) that impacted tens of thousands of votes.[2] These demonstrations have played a determining role in discouraging deployment of Internet voting in several developed countries.

3. In the case of the aforementioned examples, the risk of system failure or mishap has been restricted to relatively small populations and geographical regions. However, in

[1] For details and ToRs of this exercise, please consult the ECP Order of 19 April, 2018, F. No. 6(1)/2011-IT.
[2] Halderman, J. A. (2016). Practical attacks on real-world E-voting. Real-World Electronic Voting: Design, Analysis and Deployment, 145-171.

our case, failure or electoral rigging overseas is not confined to a few seats and can potentially impact each and every constituency in Pakistan, thereby playing a critical role in formation and composition of the next government.

4. Over time Western countries have established strong and resilient mechanisms to investigate and resolve electoral disputes. In comparison, our mechanisms, as evidenced in the aftermath of the General Elections of 2013, are still very fragile. Therefore, electoral improprieties in the overseas voting process (or even the impression of such) can potentially lead to political deadlock and turmoil. To successfully deploy a new technology, we should be cognizant of the relevant social factors.

1.3 FINDINGS

Our team undertook a review of iVOTE as per the ECP Order of April 19, 2018 (Ref: F No 6(1)/2011-IT). We identify numerous security vulnerabilities and oversights.

The following is a summary of our most important findings:

1. iVOTE categorically does not provide ballot secrecy as required in Clause 94 of the Elections Act 2017 and Article 226 of the Constitution of the Islamic Republic of Pakistan. This shortcoming is inherent to this particular model of Internet voting systems. Certain territories have explicitly legislated for it: for instance, several states in the US that offer Internet voting require citizens to waive their right to a secret ballot.[3]

2. Casting votes outside a poll-booth environment typically enables vote buying and voter coercion. In our particular case, there is a very real possibility that votes may be bought and sold and coerced overseas in regions where the ECP has no mandate to investigate or prosecute such attempts.

3. We discover that users can easily mount attacks on this system using their web browsers whereby they can cast votes for whichever national and provincial seat they choose, regardless of their constituency. These attacks can be launched with moderate technical ability and can easily be automated to manipulate votes at a large scale.

4. We investigate the possibility of phishing attacks, whereby an attacker creates doubts and confusion in the minds of voters with fake and misleading emails. We successfully sent fake emails addressed from NADRA, with content of our choice, which directed voters to a fake voting website, identical to the iVOTE portal in appearance. These

[3]Orcutt, M. (2016, August 18). Internet Voting Leaves Out a Cornerstone of Democracy: The Secret Ballot. MIT Technology Review.

attacks are exceedingly common and are especially effective against a population, which is not very tech-savvy. The banking sector typically deploys verifiability mechanisms and additional checks to prevent these attacks, but iVOTE has no such mechanism.

5. Distributed Denial of Service (DDos) attacks are a persistent threat on the Internet. NADRA has deployed a leading international filtering solution to protect against these attacks. However, as election security researchers have pointed out recently, this arrangement again compromises ballot secrecy by enabling foreign entities to decrypt and view (and potentially even modify ballot contents of voters in an undetected manner).[4]

6. iVOTE employs certain third-party security components which have been phased out because their security has been demonstrably compromised. These components can be exploited by attackers using freely available tools.

We note that many of these security vulnerabilities are not specific to iVOTE but are inherent to this particular model of Internet voting systems. Therefore, even if the voting system itself has ironclad security, these attacks will still be effective because they do not target the voting system, but instead they focus specifically on the voter's computer and the underlying network, both of which are not under NADRA's control. For this reason, certain territories (such as Estonia) have recently announced that they are abandoning this particular model of Internet voting in favour of a rigorous cryptography-based solution.[5]

Here we list some pertinent observations and concerns regarding iVOTE:

1. No usability studies or tests have been undertaken on iVOTE to ensure ease of use for voters. Ideally such a critical system would go through multiple large scale mock trials for Pakistanis from all walks of life, (especially those with low literacy). This is an extensive and time-consuming process, which may necessitate alterations in the design, which in turn will require further development and security analyses.

2. iVOTE emails are dispatched from an unauthorized email server with the result that emails to voters typically end up in the Spam folder. If these emails are dispatched at high volumes, this may result in wholesale blocking of emails and this can considerably hinder the voting exercise.

3. Certain Internet voting systems provide superior security compared to iVOTE by enabling a measure of redundancy, ballot secrecy, coercion-resistance, and

[4]Culnane, C., Eldridge, M., Essex, A., & Teague, V. (2017, October). Trust Implications of DDoS Protection in Online Elections. In International Joint Conference on Electronic Voting (pp. 127-145). Springer, Cham.
[5]Ummelas O. (2017, July 18) World's Most High-Tech Voting System to Get New Hacking Defenses. Bloomberg

verifiability. For instance, Internet voting systems in Estonia, Norway, and New South Wales were deployed alongside precinct-based paper voting systems. In the event that the Internet voting system failed, citizens in these territories would have been able to vote using paper ballots. Citizens could ensure ballot secrecy and avoid coercion by casting their vote multiple times using different modalities. Moreover, voters could also verify that their votes were correctly recorded in the system via the Internet or telephone. In contrast, iVOTE does not offer any such fail-safe, ballot secrecy, coercion resistance or verifiability features.

4. We note serious governance issues: for instance, we did not find any formal Solution Requirements Specification (SRS) for this project or proper code documentation, which is standard practice when building such systems. We also did not find any formal specification of the Threat model, which was considered when building this system.

5. We did not find any documentation related to key operational processes regarding iVOTE. It has still not been determined which party will administer this system, which premises it will be hosted on, and which personnel will ultimately be responsible for certain critical processes. As a result, at this stage we are unable to assess for certain important security attacks.

6. We anticipate that the monitoring requirements for such a system on Election Day will be considerable. We are not aware of any resources or planning done thus far to provide for this requirement.

7. This lack of planning also poses a considerable security risk in that certain critical security processes are vulnerable to insider attacks, i.e. certain system operators may be in a position to attack the system from within and modify the results. Protection against such attacks requires formulation of security policies, procedural controls, security clearances, etc. which are very intensive and time-consuming processes.

8. Members of the committee observe that even though iVOTE is built using certain mature and well-established technologies, certain others are being replaced by new advanced architectures and technologies. We recommend these should be considered in developing such systems.

We have included remediation measures, wherever possible, in the detailed report.

We would also emphasize here some fundamental limitations of our study. Our committee comprised members with diverse backgrounds, working within a very small-time window, with limited resources, and our analysis is necessarily limited. We did not use specialized hacking tools or mount highly advanced attacks that are more characteristic of cyberwarfare

and attacks undertaken by security agencies. Our report should therefore be considered a preliminary analysis of this system. It is our firm recommendation that iVOTE be subjected to a comprehensive security audit, specifically undertaken by qualified cybersecurity professionals.

1.4 RECOMMENDATIONS

Considering all these points, it is this committee's unanimous opinion that deploying Internet voting for overseas Pakistanis in the General Elections of 2018 would be a hasty step with grave consequences. **We do not recommend the deployment of the iVOTE system in its current form for overseas Pakistanis in the forthcoming General Elections of 2018.** However, we do not believe there is cause for pessimism. In our report, we provide suggestions for alternative solutions and long-term strategies to facilitate overseas voters.

Our findings are consistent with those from technical audits conducted on Internet voting systems in the past (such as those deployed in Estonia, New South Wales, and Washington DC). Developers typically approach design these applications as they would build typical commercial or enterprise applications in e-commerce and banking. What is notably missing is a **bottom-up security culture** that is more appropriate to a critical national application such as political elections.

1.5 FUTURE DIRECTIONS

Devising a complete alternative mechanism is beyond the scope of this committee, but we have attempted to identify some promising options. Here we present a summary:

1. Ideally new voting systems should be deployed progressively, starting with mock trials, deployment in surveys and non-political elections, followed by small-scale elections, and then scaling up over a period of years. This approach – undertaken by countries like Switzerland and Estonia – has the advantage of identifying vulnerabilities at every step, while at the same time, containing the risk appropriately. This also enables voters to become more familiar with the system and for developers to incorporate improvements in the system. We recommend a similar roadmap be devised for iVOTE along with appropriate milestones at every stage.

2. We recommend that ECP reconsider other remote voting modalities, which are less controversial than Internet voting and have been successfully deployed in many other countries. We note that postal voting is significantly safer than Internet voting in that, even though both modalities compromise ballot secrecy, postal voting is nevertheless not susceptible to hacking attacks which can completely compromise election integrity.

3. Furthermore, embassy voting, while it poses significant logistics challenges and financial constraints, is even safer than postal voting because it preserves ballot

secrecy and protects against coercion. In fact, our strongest recommendation of an alternative option for voting for overseas Pakistanis is to consider deployment of iVOTE in embassies using a closed intranet solution.

We also propose certain general recommendations and long-term strategies:

1. There is a critical shortage of cybersecurity skills and expertise in Pakistan, particularly within the field of election security. We therefore strongly recommend that ECP launch a dedicated and well-funded research and development (R&D) cell with long term and broad ranging objectives. This cell will be specifically tasked with building much-needed technical capacity and skills in this domain, in informing and guiding the public debate on election technology, and in developing secure new technological solutions for elections in Pakistan.

   This effort may be undertaken in partnership with universities and local and international experts. The US government has a strong record in this regard of partnering with leading academics and specialists to develop next-generation voting technologies. Engagements such as these can serve as the model for this R&D cell.

   We understand the ECP has considered such an option various times in the past but has not followed through. Due to this lack of dedicated technical expertise, we witness past mistakes being repeated and no tangible progress on the development of election systems in Pakistan.

2. As part of this R&D cell, we recommend the ECP initiate research and development in revolutionary new models and technologies for secure voting, especially the revolutionary new paradigm of end-to-end (E2E) verifiable voting. E2E voting systems offer cryptographic guarantees of ballot secrecy and election integrity, and these systems are already being trialed in various parts of the world in small-scale binding elections. [6] Most notably, Estonia has announced it is shifting to this new technology. We believe it holds considerable promise for the future, especially in Pakistan.

3. We would urge the ECP to strive towards strengthening electoral dispute resolution mechanisms in Pakistan, such that the deployment of new technological solutions is facilitated in the future.

[6] Ali, S. T., & Murray, J. (2016). An overview of end-to-end verifiable voting systems. *Real-World Electronic Voting: Design, Analysis and Deployment*, 171-218.

1.6 CONCLUSION

We hope our report serves as an informative and useful resource in the development of election technology in Pakistan. Internet voting is a controversial issue and we have made every effort to situate this debate on strong technical foundations. Furthermore, we have attempted to focus on one critical element that has been notably missing from the public debate, which is the experience of other countries using this modality. Some of the most technologically advanced countries in the world have either rolled back online voting or have deliberately chosen not to deploy it. In this document, we have highlighted the key features of their arguments and explored their application to our situation.

In conclusion, the members of this committee would like to thank the Election Commission of Pakistan for assisting us in our work. It has been a privilege and an honour to serve the nation in this regard. And we are particularly grateful to NADRA for their kind hospitality, for patiently answering our questions, for providing us timely technical support, and for facilitating this Task Force in all of its efforts.

2 INTERNET VOTING TASK FORCE (IVTF) AND OTHER STAKEHOLDERS

2.1 IVTF MEMBERS

S #	Name	Designation/Organization
1	Dr. Muhammad Manshad Satti	CEO, IT Butler, Dubai, U.A.E
2	Brig (R) Sultan Mehmood Satti	M.D, IT Butler, Dubai, U.A.E
3	Dr. Umer Saif	Chairman, PITB, Lahore
4	Mr. Sajjad Ghani	Director IT Infrastructure, PITB, Lahore
5	Mr. Bilal Ibrahim	Program Manager, PITB, Lahore
6	Mr. Haroon Rasheed	Senior Program Manager, PITB, Lahore
7	Dr. Syed Taha Ali	Assistant Professor, SEECS NUST, Islamabad
8	Dr. Shahbaz Khan	M.D, KPIT Board, Peshawar
9	Mr. M. Asim Jamshed	Director (Projects), KPIT Board, Peshawar
10	Dr. Rafi us Shan	Chief Cyber Security, KPIT Board, Peshawar
11	Mr. Zubair Khalid	Sr. Manager, LUMS, Lahore
12	Mr. M. Qayyum Ahsan	DM Application, LUMS, Lahore

2.2 IVTF AFFILIATE MEMBERS

S #	Name	Designation/Organization
1	Ms. Hina Binte Haq	Researcher, SEECS NUST
2	Mr. Bilal Ahmed	Researcher, SEECS NUST
3	Mr. Zohaib Shaheen	Researcher, SEECS NUST
4	Mr. Saad Ahmed Khan	SOC System Analyst, IT Butler
5	Mr. Rafay Baloch	Sr. Manager Info Security Global Eagle Dubai

2.3 NADRA SUPPORTING TEAM

S #	Name	Designation/Organization
1	Mr. Zulfiqar Ali	D.G (Projects), NADRA
2	Mr. Waqas Ali	Info. Security, NADRA
3	Mr. Mohammad Abid	Director (Networks), NADRA
4	Mr. Junaid Zafar	D.D (Networks), NADRA
5	Mr. Aftab Ahmed	P.M, NADRA
6	Mr. Ahmerin Hussain	G.M, Technology, NADRA
7	Mr. Usman Javed	Head of Software Development, NADRA
8	Mr. Usman Cheema	Head of R&D, Technology Directorate, NADRA
9	Mr. Usama Munir	Team Lead Development -iVote System, NADRA

2.4 ECP SUPPORTING TEAM

S #	Name	Designation/Organization
1	Dr. Akhtar Nazir	Additional Secretary (Admin), ECP
2	Mr. Muhammad Arshad	Director General(Law), ECP
3	Mr. Muhammad Khizer Aziz	Director General (Information Technology), ECP
4	Mr. Qasim Mahmood Khan	Director (Information Technology), ECP

2.5 SCOPE AND TERMS OF REFERENCE (TORS)

1. To get access from NADRA for testing the software code, hardware, network, connectivity, web services, email services, load balancing, security at all levels, database services and its optimization

2. To evaluate the endpoint security protection that detects malicious behavior and prevents malicious files from attacking NADRA networks and systems

3. To Evaluate the Data Security during transmission, applications and web servers commonly using Transport Layer Security (TLS) for encrypted communication

4. To audit the Remote Identity Proofing (RIDP), a process for validating sufficient information that uniquely identifies voter's eligibility (e.g., NICOP, personal demographic information, and other indicators)

5. To evaluate the hosting facility of Overseas Voting Server for Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks on Voting Day or even earlier

6. To assimilate the Man-in-Middle Attacks for ensuring the Data integrity of voting data

7. To identify various types of vulnerabilities and propose optimum solutions

8. To perform comprehensive 'penetration testing' of whole systems

9. To make efforts for compromising the website (www.overseasvoting.gov.pk)

10. To break or hack the iVOTE system and mark its loop-holes

11. To perform load testing activities to check the expected humongous traffic load

12. To give technical recommendations for further enhancing its security

13. To give recommendations on secure use of I-Voting in election activities

14. To submit 3rd party technical audit report to the ECP along with its recommendations for improving or upgrading all aspects of Internet Voting System

15. To give any concrete suggestions, or a proposal for a more secure architecture for I-Voting

3 MANAGEMENT INTERVIEWS

In response to complaint assessment of iVOTE application's efficacy, secrecy, and coercion-resistance, it was deemed necessary to conduct informal interviews of Key Stakeholders to ascertain their perspectives and past history of electronic voting systems.

During our meeting with the NADRA chairman, we asked regarding the iVOTE application and its agreed Technical Specification Requirement (TSR) or General Specification Requirement (GSR) from NADRA Management for sign-off process. We found that no formal TSR/GSR has been exchanged or signed off between ECP and NADRA, which reflects the fact that the iVOTE project was hastily instigated to comply with Supreme Court orders.

We also observed that NADRA presented the iVOTE model to Supreme Court with insufficient illustrations of such systems, mostly significantly the fact that no other sovereign state has thus far successfully used such a system at this scale in political elections.

NADRA has undertaken a project to enable over six (06) million overseas voters, and a project of this scope generally takes six to eight months for development. NADRA, under immense pressure, had agreed to develop and test the application in ten (10) weeks' time, which resulted in the lack of software testing processes, no mock elections, and disregarding standard best practices. As a result, IVTF has identified six CRITICAL vulnerabilities and some HIGH categories risks in iVOTE application.

IVTF team has tested the application Vulnerability Assessment (VA) and Penetration Test (PT) from Pakistan and from Overseas (UAE & KSA) and exploited the above weakness and achieved successful penetration in manipulating the data during the voting process. All evidence of our findings (screenshots) are attached in Appendix-A

S #	Name	Designation/Organization
1	Mr. Babar Yaqoob Fateh Muhammad	Secretary ECP
2	Mr. Muhammad Khizer Aziz	Director General (IT) ECP
3	Mr. Usman Y. Mobin	Chairman NADRA
4	Mr. Zulfiqar Ali	D.G (Projects), NADRA

During ECP interviews and meetings, we discovered that options for iVOTE and online voting have been evaluated previously during the year 2014 to 2017 but none of those solutions have been fully compliant with voting criteria described in Article 226 of the Constitution of Pakistan and the Election Bill 2017 proposed by the Parliamentary Committee for Electoral Reforms.

It is also worth mentioning here that NADRA and ECP extended us every support, provided us whatever information we requested and assisted the IVTF team during this project.

Likewise, NADRA has facilitated us with a state of the art office environment with a dedicated room, Internet connectivity, on-site visits, and kind hospitality.

4 BACKGROUND

Election security is a rich and diverse domain of study and expertise. In this section, we present essential background material on security for Internet voting systems. We start with brief descriptions of the key security properties of voting systems, and we consider how they relate to each other. We describe how Internet voting is distinct from typical Internet applications using the particular example of Internet banking and e-commerce. This is followed by a discussion of how Internet voting faces fundamentally different threats as compared to common Internet applications and how the design of Internet voting systems often fails to take this fact into account. We also briefly consider the legal ramifications of deploying fundamentally new voting technology.

We have attempted to situate this discussion on a firm technical foundation and especially highlight an aspect that is often overlooked in discussion on Internet voting, i.e. the experience of other countries with using this election modality.

4.1 SECURITY PROPERTIES

Here, we briefly define various security properties of a voting system.

1. **Voter Eligibility:** The system should only permit eligible voters to cast votes and restrict each voter to one vote.

2. **Ballot Secrecy:** The privacy of the vote is widely recognized as a fundamental human right and is enshrined in Article 21 of the Universal Declaration of Human Rights[7]. The rationale behind this, dating back to ancient Greece and Rome, is that if outside parties become privy to a voter's choice, it opens the door to bribery and intimidation, thereby ultimately corrupting the electoral process. This realization directly motivated the invention of the secret ballot.

   In Pakistan, ballot secrecy for voters is specified as a key requirement in Clause 94 of the Elections Act 2017 and Article 226 of the Constitution of the Islamic Republic of Pakistan.

3. **Coercion Resistance:** The voting system should not allow third parties to force a voter to cast the vote in a certain way. This property directly follows as a result of ballot secrecy.

   Forms of coercion include 'family voting' where one family member casts the votes on behalf of his/her family members or pressurizes them to vote a certain way. Employers may likewise force or incentivize employees to vote for specific candidates. Voters can also choose to sell their votes.

[7] Universal Declaration of Human Rights, 1948

Voter coercion is particularly facilitated in remote voting modalities, such as postal, telephone, or Internet voting, and is a key threat in most of these systems. We quote here renowned cybersecurity expert, Dr. Ross Anderson[8]

"When you move from voting in person to voting at home (whether by post, by phone or over the internet) it vastly expands the scope for vote buying and coercion, and we've seen this rising steadily in the UK since the 2001 election where postal votes first became a right. All the parties have been caught hustling up the vote in various ways."

4. **Election Integrity:** The system should instill confidence in voters that the elections have been conducted in a fair manner and that the election results reflect the public will. Typically, election integrity is ensured by **instituting redundancy, transparency,** and **verifiability** measures at key steps in the electoral process. In paper-based election systems, these processes include exit polls, random audits, and opening the tallying process to members of all political parties and citizens. Election integrity is more problematic in electronic and Internet voting systems, as these systems typically do not maintain a paper trail of votes and they are susceptible to large scale hacking.

We list here certain additional non-security properties of voting systems, which are also of critical importance.

1. **Usability:** The system should enable voters to cast their votes easily and effectively.

2. **Accessibility:** The system should provide equal opportunities for access and participation.

3. **Logistics:** This pertains to the cost and ease of setting up a reliable and secure voting system.

Several of the key properties described thus far conflict with each other, giving rise to a variety of technical and legal challenges, which have to be carefully addressed. We consider one of these conflicts next, the clash between vote verifiability and ballot secrecy.

4.2 INTERNET VOTING VS. INTERNET BANKING

A very common question, which arises in conversations regarding Internet voting, is that if applications such as banking or commerce can be conducted online, then why not voting? This is a fair question as banking and e-commerce are critical applications and considerable effort is made to secure them. Are the same techniques applicable to Internet voting?

There are two important differences to be considered here: first, online banking and e-commerce systems are vulnerable to cybercrime with attacks costing the economy up to

[8] Nicole Kobie, (2015, March 30) "Why electronic voting isn't secure – but may be safe enough," The Guardian

hundreds of billions of dollars every year. A recent study estimates cybercrime revenue at $1.5 trillion per year and indicates that not only is cybercrime a fast-growing phenomenon but also that cybercriminal outfits may actually be making more money than small and mid-size companies. Banking and e-commerce websites get hacked routinely and the costs of these attacks are typically counted as 'the cost of doing business'.[9]

Second, and most important, the key tools that banks use to fight cybercrime are not applicable to Internet voting. For instance, financial institutions maintain detailed records and audit trails of every transaction. In the case of voting, maintaining audit logs or trails that identify the voter is a direct violation of the secret ballot property. Moreover, Internet voting cannot recover from attacks in the same way that banks can: miscast votes cannot be easily detected or reversed the way banking transactions can. Furthermore, elections are a far more sensitive matter than banking and news of a hacking incident may have a serious negative impact on citizen confidence in elections and long-lasting political repercussions.

In case of an incident, banks and merchants have recovery protocols in place, which include blocking stolen credit cards, reversing irregular transactions, compensating clients for lost funds, etc. Again, these mechanisms do not apply to Internet voting. In the words of election security expert, David Jefferson[10]:

"Vote fraud is much less manageable than ecommerce fraud. There is no election analog to the natural business practice of "spreading the cost" or "spreading the risk". There is no way to pass on to other voters the "losses" due to illegal ballots cast by ineligible voters or attackers, or to recover votes changed by malicious software. There is no "insurance" that one can buy to cover those losses. There is just no way to compensate for damage done to an election."

For these reasons, in the election security community, paper is still considered the gold standard when it comes to elections. To quote renowned cybersecurity expert, Bruce Schneier[11]:

"Today, we conduct our elections on computers. Our registration lists are in computer databases. We vote on computerized voting machines. And our tabulation and reporting is done on computers. We do this for a lot of good reasons, but a side effect is that elections now have all the insecurities inherent in computers. The only way to reliably protect elections from both malice and accident is to use something that is not hackable or unreliable at scale; the best way to do that is to back up as much of the system as possible with paper."

[9] Glick, B. (2018, Feb. 23) Is cyber security becoming a cost of doing business - to the detriment of our data? ComputerWeekly

[10] Jefferson, D. If I Can Shop and Bank Online, Why Can't I Vote Online? Verified Voting

[11] Schneier, B. (2018, Apr. 18) "American elections are too easy to hack. We must take action now", The Guardian

4.3 THE THREAT MODEL

Another crucial distinction between Internet voting and other Internet applications that we overlook in our national discourse is the threat model. Applications such as Internet banking and e-commerce are typically targeted by insiders, hackers or in organized gangs, whereas an Internet voting system used in binding political elections is far more likely to be attacked by foreign governments and intelligence agencies.

Foreign government agencies pose an entirely different class of threat as compared to standard hackers. These organizations typically have unsurpassed resources and capabilities at their disposal. For instance, in 2007 hackers from Russia crippled Estonia's online infrastructure for several days with concentrated Denial of Service attacks that disabled the websites of banks, government ministries, political parties, and media.[12]

These attacks can also be extremely stealthy and powerful and of a magnitude that is sometimes difficult for the layman to even comprehend. We have the example of Skynet, a US NSA operation, specifically deployed in Pakistan.[13] The NSA had actively hacked into Pakistan's communications infrastructure and was surreptitiously engaged in bulk collection of phone metadata of 55 million mobile phone users. This information was then used to identify potential terrorists who could later be targeted via drone strike. This infiltration was undetected for several years and only revealed as part of the Snowden leaks.

Foreign intelligence organizations also possess a wealth of expertise unavailable to the typical hacker. A compelling example is that of a zero-day exploit, i.e. an attack that exploits a previously unknown vulnerability. The Stuxnet worm, designed jointly by the US and Israel, contained four such exploits.[14] Stuxnet infected Iranian nuclear enrichment facilities and destroyed a significant number of centrifuges, launching a new era of cyberwarfare. And since these vulnerabilities are unknown at the time of the attack, there are no defenses against them.

These examples are not isolated cases and hopefully convey the magnitude and gravity of the threat posed by foreign intelligence organizations. These examples particularly apply to Internet voting.

For instance, in 2010, a team from University of Michigan successfully infiltrated a mock Internet voting exercise conducted by the Washington DC Board of Elections and Ethics. Among their findings, the team reported that while they had control of the system, they detected intrusion attempts made by parties in China and Iran.[15]

[12] Tryanor, I. (2007, May 17) Russia accused of unleashing cyberwar to disable Estonia, The Guardian
[13] Naughton, J. (2016, Feb. 21) Death by drone strike, dished out by algorithm, The Guardian
[14] Szoldra, P. (2016, Jul. 7) A new film gives a frightening look at how the US used cyberwarfare to destroy nukes, Business Insider
[15] Wheaton, S. (2018, Oct. 8) Voting Test Falls Victim to Hackers, The New York Times

Similarly, in 2014 Russian hackers attacked Ukraine's presidential election, deleting key parts of the vote tallying software, and came very close to disrupting the election.[16] Russian hackers have also been accused of penetrating voter registration databases in the recent 2016 US elections.

Furthermore, security researchers who successfully attacked the New South Wales Internet voting system (iVOTE), in 2015, successfully demonstrated how zero-day exploits could be used to view and modify votes while they were being cast.[17]

4.4 SOFTWARE SECURITY

A last point of note is the poor state of commercial software solutions. We quote election security expert, Dr. Alex Halderman:

"Real-world internet voting systems tend to be built on top of commercial-off-the- shelf (COTS) software, which, despite the use of the term "commercial," includes most everyday open-source software. Unfortunately, the dominant security practice for COTS developers is still "penetrate and patch." While this approach is suitable for the economic and risk environment of typical home and business users, it is not appropriate for critical security systems, such as voting applications, due to the severe consequences of failure."

"Getting web security right is complicated, and small mistakes in the implementation and configuration of web applications can result in total compromise. In this sense, the web is a brittle platform for secure application development. This is illustrated by the vulnerabilities in the Washington, D.C., and New South Wales web-based Internet voting systems… In both cases, vulnerabilities resulting from small oversights—which could have been prevented by changing single lines of code— jeopardized the integrity of election results. Mistakes like these are common in web applications, and they are hard to eradicate because of the multitude of places in the software that they can exist, any one of which might be overlooked."

This argument particularly applies in our case. In our analysis we discovered that iVOTE relied on a third-party text-based CAPTCHA mechanism that is now retired and demonstrated to be insecure.[18]

4.5 VOTING TECHNOLOGY: LEGAL AND POLITICAL ASPECTS

Here we discuss how the introduction of new voting technology interacts with fundamental election security properties, such as ballot secrecy, verifiability, and election integrity, and

[16] Clayton, M. (2014, Jun 17) Ukraine election narrowly avoided 'wanton destruction' from hackers, Christian Science Monitor
[17] Halderman, J., Teague V. (2015, June 5) The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election
[18] Bohannon, J. (2013, Oct. 28) CAPTCHA Busted? AI Company Claims Break of Internet's Favorite Protection System, Wired Insider

the resulting legal and political implications. The examples we discuss also highlight the fact that thus far, advanced technology has mostly fallen short of delivering on election security.

1. **United States:** Over thirty states in the United States allow citizens to cast votes via email, fax, or via the Internet.[19] These options are mostly available to overseas voters and military personnel. However, some twenty states have laws and regulations requiring that voters who vote via the Internet waive their right to a secret ballot. In a further eight states, there is no such legislation but this waiver is still required by election authorities.

   The state of Alaska goes even further and warns voters that their ballot may be corrupted in transit. Voters who visit the voting website are shown a disclaimer from the State Division of Elections[20]: *"When returning the ballot through the secure online delivery system, you are voluntarily waving [sic] your right to a secret ballot and are assuming the risk that a faulty transmission may occur."*

   Alaska has since announced it is suspending its Internet voting program over fears of Russian hacking.[21]

2. **Germany:** For instance, in Germany in 2009, the country's electronic voting program was rolled back after concerned citizens mounted a legal challenge in court, arguing that the average voter could not verify the inner workings of these machines and therefore needed to place "blind faith" in the technology. In its ruling, the Federal Constitutional Court of Germany stated[22]: *"The very wide-reaching effect of possible errors of the voting machines or of deliberate electoral fraud make special precautions necessary in order to safeguard the principle of the public nature of elections."*

   The ruling concludes with: *"In a republic, elections are a matter for the entire people and a joint concern of all citizens. Consequently, the monitoring of the election procedure must also be a matter for and a task of the citizen. Each citizen must be able to comprehend and verify the central steps in the elections."*

3. **Poland:** In December, 2014, Poland's electronic voting system suffered major technical glitches during local elections, delaying results, and leading to widely unexpected outcomes. An estimated 60,000 people marched in protest, including

[19] Orcutt, M. (2016, Aug. 18) Internet Voting Leaves Out a Cornerstone of Democracy: The Secret Ballot MIT Technology Review
[20] Horwitz, S. (2016, May 17) More than 30 states offer online voting, but experts warn it isn't secure, The Washington Post
[21] Juneau Empire, (2018, Feb. 21) To boost election security, Alaska suspends electronic absentee program, Juneau Empire
[22] NDI, The Constitutionality of Electronic Voting in Germany

extremist nationalist groups. Polish courts were flooded with more than a thousand legal challenges contesting election results.

4.6 CONCLUSION

Hopefully this discussion thus far demonstrates to the reader why Internet voting is recognized by security experts to be a controversial and risky undertaking. We have described the security properties of voting systems and discussed how they fundamentally differ from those of typical Internet applications. We have also highlighted how the threat model is different and why this is a critical factor that is unfortunately often overlooked in the national dialogue.

We have further summarized findings from attacks on three key Internet voting systems (Washington DC, Estonia, and New South Wales) in Appendix B. It also summarizes key concerns raised in other countries regarding the implementation of Internet voting. The primary issues that other countries have wrestled with were the same security concerns that we raise in this report.

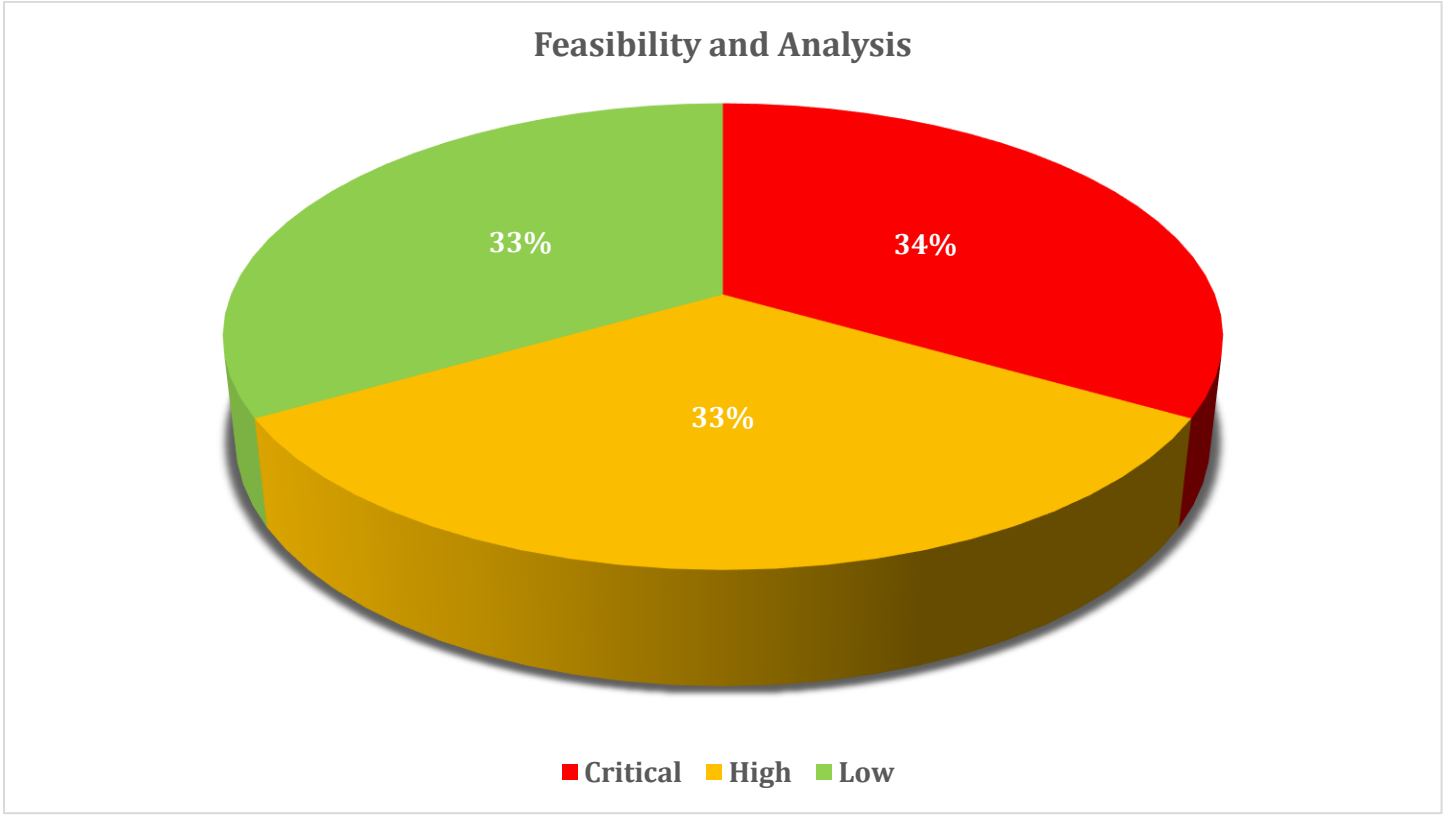
In these cases, researchers were able to exploit very minor flaws in the systems to completely compromise the elections. In the case of the Washington DC Internet voting system, the error was as trivial as using single quotation marks instead of double quotation marks at one point in the code.

We would therefore urge all stakeholders to exercise extreme caution in approaching the question of Internet voting.

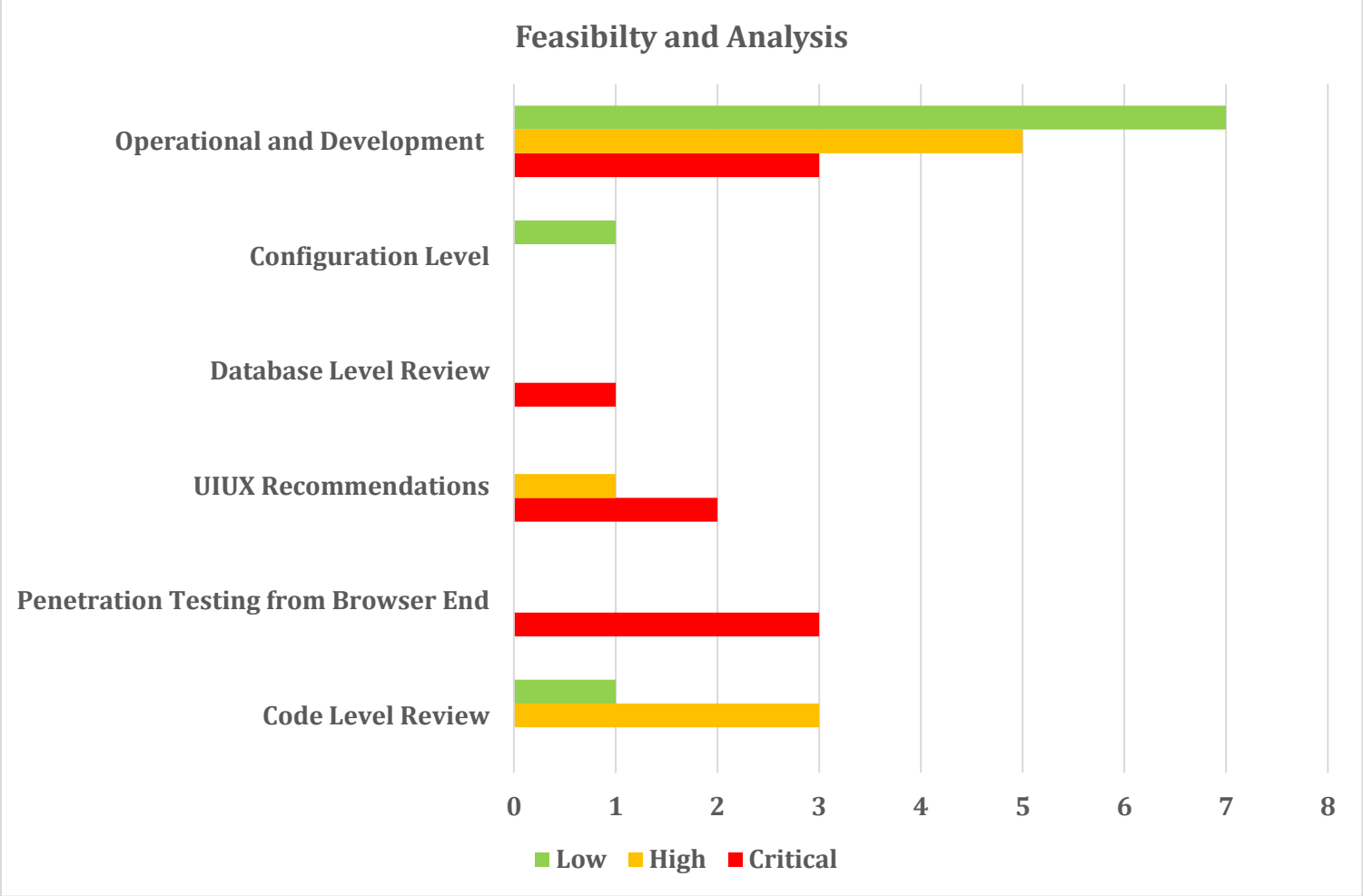
5 FEASIBILITY AND ANALYSIS

This section of the report is composed of following areas, each addressed in detail below:

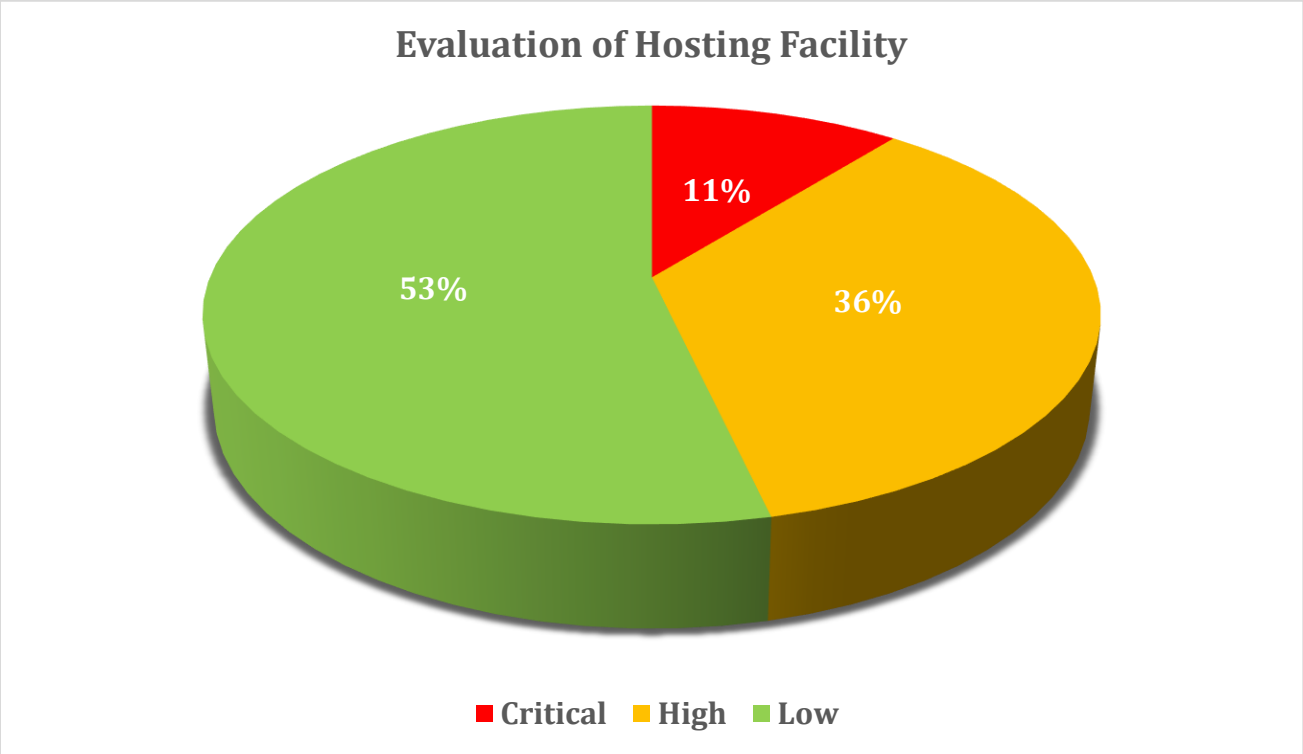
1. Code Level Review
2. Penetration Testing from Browser End
3. UIUX Recommendations
4. Database Level Review
5. Configuration Level
6. Operational and Development



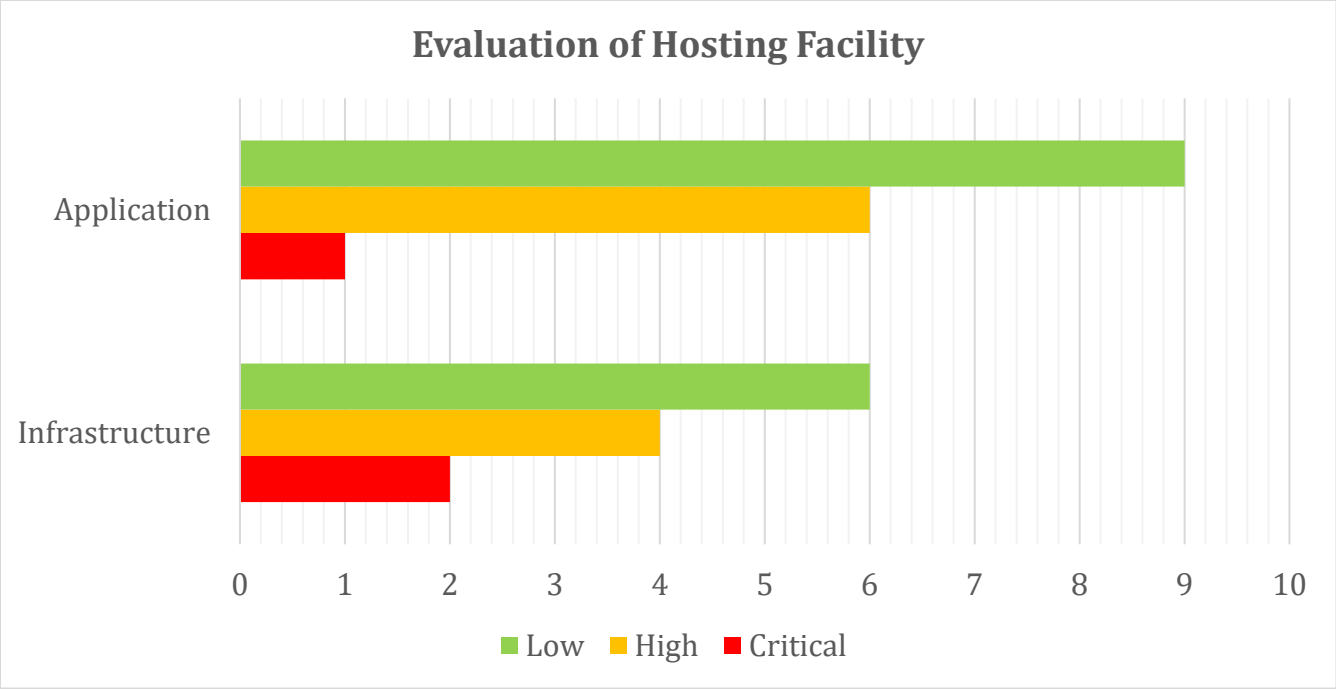
Sr No	Category	Critical	High	Low
1	Code Level Review	0	3	1
2	Penetration Testing from Browser End	3	0	0
3	UIUX Recommendations	2	1	0
4	Database Level Review	1	0	0
5	Configuration Level	0	0	1
6	Operational and Development	3	5	7
	Total	9	9	9


Feasibilty and Analysis
Operational and Development
Configuration Level
Database Level Review
UIUX Recommendations
Penetration Testing from Browser End
Code Level Review
0
1
2
3
4
5
6
7
8
Low
High
Critical

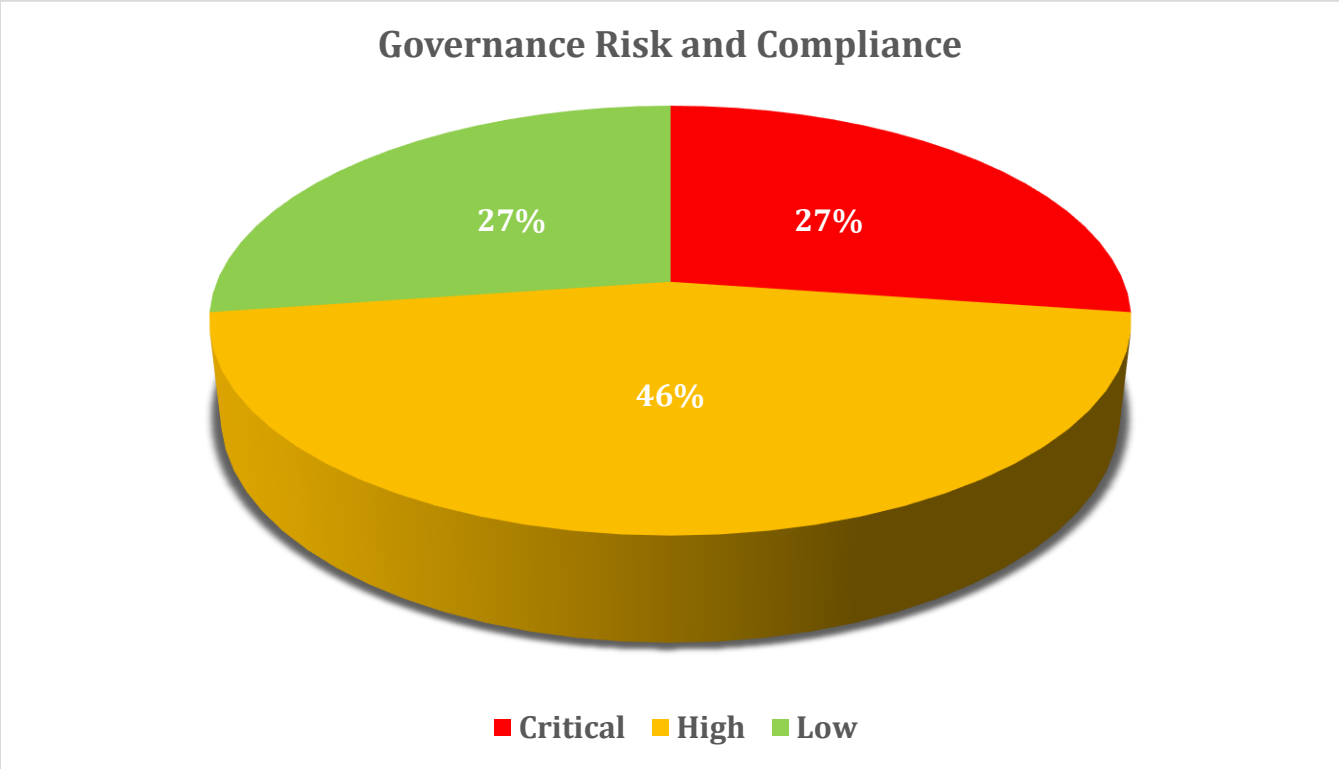
6 Evaluation of Hosting Facility



Sr No	Category	Critical	High	Low
1	Infrastructure	2	4	6
2	Application	1	6	9
	Total	3	10	15


Evaluation of Hosting Facility
Application
Infrastructure
0
1
2
3
4
5
6
7
8
9
10
Low
High
Critical

7 GOVERNANCE, RISK AND COMPLIANCE



8 THE WAY FORWARD

In this section, we would like to present our humble recommendations on the way forward. We do not believe there is cause for pessimism in this endeavor. Technology has made great strides recently, especially in election technology, and we anticipate that Internet voting will be a reality in the near future.

First, we present our recommendations for Internet voting. This is followed by a consideration of other remote voting modalities such as postal and embassy voting. We believe that iVOTE, deployed in an embassy-voting scenario, may be a workable technological solution for overseas Pakistanis to vote in the short term.

We then present long-term recommendations, namely that ECP invest wholeheartedly in a Research and Development cell to investigate new cutting-edge election technologies (especially end-to-end verifiable voting) and to educate and guide stakeholders on technological questions.

8.1 RECOMMENDATIONS FOR INTERNET VOTING

We recommend that Internet voting, if needed, be deployed in a piecemeal organic manner[23] starting with multiple small non-political elections (e.g. trade organization, bar councils, engineering bodies, etc.), followed by small-scale political elections (intra-party elections, local government polls, by-elections), and slowly expand in scope.

This strategy allows for review and further improvement at every stage in terms of usability and security. The electorate also gets a chance to adjust to this new system and provide valuable feedback. Verifiability measures could be incorporated piecemeal at different stages of the election process. The technical challenges and threat model for deploying such a system also become clear and system administrators develop valuable experience in the process.

Additionally, in the event of technical glitches, hacks, or system failure, the political risk is proportionately restricted. Furthermore, if there are legal challenges to this system (as have been observed in several countries including Germany, India, and Poland), then they can be addressed in a timely manner without wasting resources on a very large deployment.

We would also strongly recommend periodic security audits of this Internet voting system as well as regular sponsored hackathons and bug bounties (similar to those conducted in India[24] and at DEFCON[25]) where hackers are invited to attack the system for monetary reward.

[23] Ali, T. (2015, May 21) How (not) to deploy an electronic voting system, Express Tribune
[24] Bhatnagar, G. V. (2017, May 21) Election Commission Says EVM Hackathon to Begin From June 3, The Wire
[25] Newman, H. L. (2017, Jan. 8) To fix voting machines, hackers tear them apart, Wired

We suggest that all stakeholders contribute to a roadmap for a phased deployment of Internet voting along the lines that we have suggested with appropriate milestones and KPIs to be met at every stage.

8.2 ALTERNATIVE REMOTE VOTING MODALITIES

1. **Postal Voting:** Postal voting also suffers from a critical weakness of remote voting paradigms in that ballot secrecy and coercion resistance cannot be ensured. Voters may pressure family members to vote a certain way, votes may be bought and sold in secret, and employers may use incentives or intimidation techniques to force votes for candidates of their choice. For this reason, several countries, including Austria and Germany, require postal voters to sign an explicit disclaimer, where they commit to casting their vote in an unobserved and secret manner.

   However, postal voting has one fundamental security advantage over Internet voting: coercion and rigging efforts on postal ballots are classed as 'retail' attacks which require physical effort and coordination and are considerably difficult to mount on a very large scale. On the other hand, Internet voting systems enable 'wholesale' rigging, i.e. tens of thousands of votes may be altered in a single successful hack. In essence, Internet voting carries a far greater threat to election integrity than postal voting. Furthermore, unlike Internet voting, postal voting has been successfully employed in dozens of countries to date and its risks and methodology are well understood.

   For these reasons, we conclude that postal voting, although it bears heavier logistics and financial costs, is a considerably more secure option than Internet voting. We understand that ECP has conducted mock trials of postal voting in the past without much success. We would recommend ECP consider revisiting this modality as a short-term solution to enable overseas Pakistanis to vote.

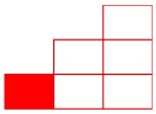
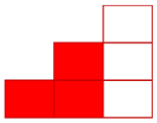
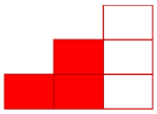
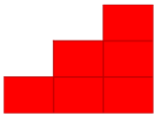
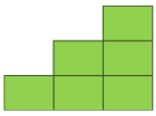
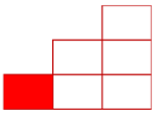
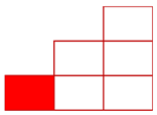
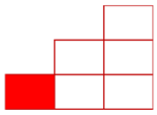
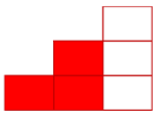
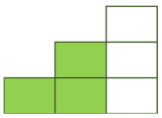
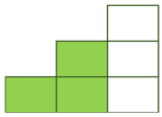
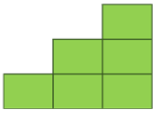
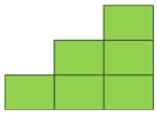
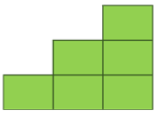
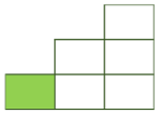
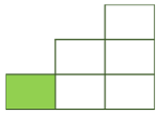
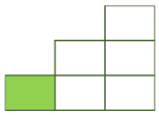
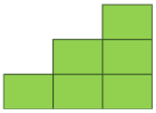
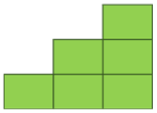
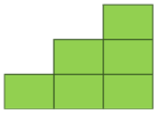
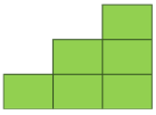
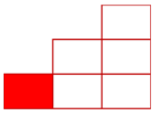
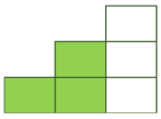
2. **Embassy Voting:** Another desirable modality for remote voting is the embassy-voting paradigm, where voters cast votes in person at the nearest consulates and embassies. This bears significant logistics and financial costs than postal ballots but offers the strongest security of all remote voting paradigms. The embassy environment serves as a makeshift precinct or polling booth, which automatically protects ballot secrecy and prevents voter coercion.
   There is also significant precedent for embassy voting from the examples of other countries. Election security specialists have also recommended it in certain cases specifically as a more secure alternative to Internet voting.[26]

[26] Jefferson. D, (2004, Jan. 5) A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)

In fact, it is even possible to reduce costs by deploying an online voting system on consoles in embassies over a closed network (Intranet), which is not accessible via the public Internet. This protects the system from online hackers and reduces reliance on foreign entities (such as web-based filters e.g. Cloudflare).

We believe this is the most technically secure option to be considered for forthcoming elections. However, as we noted earlier, this modality has various political, financial, and logistics aspects, the study of which is beyond the scope and expertise of this committee. We therefore recommend that the concerned parties undertake a feasibility study of embassy voting for overseas voting.

A summary comparison chart of all three remote voting modalities (postal voting, embassy voting, and Internet voting) is provided below: -

System	Voter Eligibility	Ballot Secrecy	Coercion Resistance	Election Integrity	Logistics	Usability
Internet Voting						
Postal Ballots						
Embassy Voting						
End to End Verifiable Voting						

8.3 Long-term Strategy: Research and Development (R&D)

We urgently recommend that ECP institute a dedicated cell to research and develop cutting edge election technologies as well as provide informed and timely technical expertise to stakeholders in the electoral process. We find these two factors to be critical shortcomings in our national dialogue regarding voting technology. We understand the ECP itself has weighed this option over the past few years but has yet to give it a green light. A dedicated cell that is staffed with experts, with funded resources, a wide-ranging scope, and a long-

term vision will hopefully rectify this deficiency and provide sound advice on future decisions.

There is strong precedent for this step. In the wake of the infamous US elections of 2000, as part of the Help America Vote Act, the US government directly engaged with academics from top American universities and cybersecurity specialists and activists to fund think tanks, research groups, and local conferences which led to significant breakthroughs in the development of election technology. Electoral bodies in other countries also directly fund research and development in new election technology.

Among its first tasks, we would strongly recommend that this R&D cell investigate the use of end-to-end (E2E) verifiable voting technology for potential deployment. This is a revolutionary new paradigm for secure elections that has emerged over the last decade where voters and election officials alike can verify various steps of the election using cryptographic guarantees without compromising ballot secrecy.[27] This technology is being developed and is being actively promoted by some of the most renowned cryptographers and security specialists in the world.

Developed countries worldwide have recognized the revolutionary potential of this new development. E2E voting systems have been trialed in various pilot projects and non-political elections and are now being deployed in binding political elections on a small scale (for instance, in intraparty elections in Israel, in mayoral elections in Maryland, US, in state elections in Victoria, Australia, and at the county level in gubernatorial elections in Texas). Electoral experts in Switzerland and Canada have recommended this new technology be explored for use in forthcoming elections. Most notably, Estonia, on the recommendation of security experts and the Organization for Security and Cooperation in Europe, has announced that it is transitioning to E2E technology, referring to it as the 'Holy Grail' of electronic voting.[28]

Furthermore, the blockchain also presents considerable opportunity for building reliability and trust in the voting infrastructure. Sierra Leone made headlines recently when observers demonstrated how votes cast in the recent presidential election could be stored on a blockchain-based platform[29]. Russia has recently launched a blockchain-based system for voting on municipal initiatives[30] and for preserving exit poll results in recent Presidential

[27] Ali, S. T., & Murray, J. (2016). An overview of end-to-end verifiable voting systems. *Real-World Electronic Voting: Design, Analysis and Deployment*, 171-218.
[28] Ummelas, O. (2017, July 18) World's Most High-Tech Voting System to Get New Hacking Defenses. Bloomberg
[29] Zuckerman, M. J. (2018, Mar. 8), Sierra Leone Uses Blockchain To Track Election Results, Swiss Company Provides Expertise. CoinTelegraph
[30] Castillo, M. (2018, Feb. 21) Russia Is Leading the Push for Blockchain Democracy. CoinDesk

elections[31]. Moreover, researchers have also successfully demonstrated E2E verifiable voting systems, which are powered by the blockchain.[32]

As these new developments indicate, there is a bright and exciting future ahead for electronic and Internet voting technologies. The formation of a cell that is empowered and exclusively dedicated to research and development in these domains would potentially save us considerable time in updating our technical base, reduce our reliance on foreign expertise, develop indigenous and trustworthy solutions, and provide non-partisan, informed and valuable guidance on the way forward.

We strongly urge action on this R&D recommendation. We urge all stakeholders not to overlook or minimize the importance of informed technical research and expertise as has been done multiple times in the past, and which has resulted in this current political deadlock and continues to deprive our citizens of contributing to our democracy.

***** Report Ends Here *****

[31] Suberg, W. (2018, Mar. 6) Russia: Blockchain Will Be Used To Protect 2018 Presidential Exit Poll Data. CoinTelegraph

[32] Castor, A. (2017, Apr. 6) An Ethereum Voting Scheme That Doesn't Give Away Your Vote. CoinDesk