ACE
Focus On
'Elections and Security'

by Sean Dunne

Introduction

An election is a contest for legitimate power that can be described as a non-violent competition, fought within a political forum. It is important in this context to recognise that elections do not avoid confrontation, but rather, focus on its management and containment within accepted boundaries. In practice, the assurance of equitable security during an electoral process is essential to retaining the participants' confidence and commitment to an election. Consequently, security is both integral to the goal of an election and an inseparable part of the electoral process.

There is no single model of elections or democracy that is universally applicable to all countries. An election is unique – defined not only by the electoral rules, but also shaped by the social values, politics, religions, history and culture of the people. In the same way, the security of an election is unique to the circumstances in which it is conducted. The stakes of any given election are different – even if it is held periodically in the same country – due to the changing forces that shape the national interest and corresponding political agenda.

Similar to a sporting event, the rivalry between opposing teams entails competition within an accepted set of rules, but does not allow for the use of violence to seek victory. Extending on this comparison, if violence does occur, it can lead to the disqualification of players (candidates), teams (political parties), an amendment of the results or the abandonment of the competition altogether. As such, the emergence of electoral violence is not a result of the process being followed, but signals a critical departure from the accepted rules that govern the process.

Principles of Elections and Security

The organisation and conduct of credible elections demand adherence to principles and rights, which in practice, impose significant challenges for ensuring effective security, including: (a) *transparency* requires that the steps of an electoral process be well advertised to the public; (b) elections must be held in *compliance with national laws* that usually create immutable timeframes; (c) *freedom of speech and association* can create a politically-charged atmosphere which may polarise communities; (d) the institutions responsible for the administration and security of an election must fulfil their mandates *impartially*, and may be constrained by the need to avoid perceptions that they are favouring a particular political competitor; (e) *inclusiveness* requires that an election be a highly decentralised operation, with massive logistical requirements involving the recruitment of tens of thousands of temporary staff, and the operation of polling places and offices.

To operate effectively within these electoral requirements, security forces need to be guided by their own principles, including:

- *Equitable and rights-based*;

  Participants in an election must be treated in an equitable manner by both security forces and electoral officials. Reasonable and proportionate responses to actions must be consistent, which cannot be influenced by arbitrary factors, such as, political affiliation. An election is a mechanism by which people are able to exercise their political, civil and human rights. Security protocols must consider and acknowledge these rights, as well as the heightened sensitivity and scrutiny to the respect for these rights that occur during an election period.

- *National ownership*;

  Elections are a sovereign process. However, in some circumstances such as, post-conflict or transitional elections, national security forces may need to be strengthened by international forces. To the degree permitted, the security of an election should fall within the ownership and control of a national authority to reflect sovereignty and

avoid allegations of international interference. Advantageously, indigenous security forces are the most sensitive to their cultural practices and may therefore be best positioned to interpret and respond to emerging threats.

- *Strategic*;

  Elections are normally planned 18 to 24 months before polling day and occur as a widely dispersed exercise requiring significant planning and preparatory activities. Security forces (police and/or military) rarely possess sufficient standing resources to secure an election, and simultaneously carry-out their regular duties. Integrated strategic planning by the electoral and security institutions is essential to prioritise, allocate and coordinate necessary resources.

- *Non-partisan and impartial*;

  To be effective, security forces must avoid allegations of partisan bias. If security forces are found to behave in a partisan way, rather than defusing tensions they may heighten them and undermine their own function in the process. During the election period (especially during the campaign period) normal security actions may become the subject of analysis which evokes political dimensions. In politics in general, and in elections in particular, perception is as important as reality. As such, senior security managers must actively consider these political dimensions to preserve not only the reality, but the perception of impartiality.

- *Flexible and efficient*;

  Electoral processes can face late-stage amendments to accommodate emerging legal, operational or political conditions that arise. In the first instance, security planning should include a range of contingency plans and resources to ensure flexibility. Alternatively, clearly defined constraints on security capabilities and resources based on efficient planning should be available to inform decision makers on the range of options that are feasible to accommodate. The efficiency of these operations, both in delivering substantive security services and adjusting to changes, is an important indicator for the confidence of the electoral participants.

- *Transparent and accountable*;

  In security operations there is always a tension between operational security policies of 'need to know' and the public interest. In an election period, disclosure policies

> are normally best weighted towards the public interest, recognising the importance and value of transparency. In cases where it is necessary to protect information, extra accountability measures may be necessary to ensure post-event justifications. Transparency in this context also refers to enhancing consultative mechanisms with political groups, civil society and other organisations to ensure the role and functions of security forces are well understood in the process.

A favourite saying of this author is: 'The best operational solution is rarely politically feasible'. In many cases, the political dimensions of an election can create obstacles to otherwise seemingly simple security decisions. This feature of the electoral process highlights the potential frustrations that can arise between security and electoral officials. Ultimately, an operational solution cannot be considered desirable if it does not address the necessary political conditions. This discord emphasizes the need for strong communication and coordination between security forces and electoral institutions.

Election Security Threats and Analysis

The nature of an election makes it vulnerable to a range of security threats against participants, infrastructure, information and materials. Effective election security analysis must draw on information and expertise from multiple arenas. A high-level of communication and coordination among the agencies responsible for the administration and security of an election is a significant advantage. Neither can security analysis and planning be effective when it occurs only in a period shortly before the electoral process starts, nor depend solely on reactive strategies. Anticipating and pre-empting security risks, mitigating their impact or probability of occurrence, is a strategic endeavour of both the electoral authorities and their security partners.

An electoral process is constituted from a complex series of interdependent sub-processes, generically including: boundary delimitation, civic education, voter education, voter registration, party registration, candidate nomination, the campaign period, polling operations, tallying and counting, dispute resolution and the official announcement of results. With the

exception of boundary delimitation (which often occurs following a decennial census exercise) these sub-processes occur in some form during each election cycle. Each of these sub-processes can be characterised by different types of threats, influenced by: the particular approach adopted, cross-influence between sub-processes and the individual circumstances of the election. Further, the circumstantial conditions of an election can alter quickly, requiring the rapid reprioritisation or invalidation of initial security assumptions. Accordingly, the analysis of threats and risks is a continuous task throughout the electoral process, and is not simply event driven.

The types of security threats likely to arise in a particular election are influenced by both structural and circumstantial aspects of the election process. The structural design of the electoral process such as the choice of electoral system may foster or deter certain threats. For instance, an electoral system that uses a single national district (the national borders form a single electoral constituency) and allows voters to cast their vote at any polling station, will offer no direct incentive to forcibly move voters within the territory – since irrespective of where the vote is cast, it will be counted in the final tally. On the other hand, this arrangement may promote efforts to forcibly migrate eligible voters across national borders, so they cannot participate. In security terms, this scenario reflects a heightened structural risk for border control operations during the voter registration and polling phases of an election.

Circumstances will dictate in each election, and at each stage of the electoral process, the level and priority of risk posed by different threats. For example, when an election is a presidential run-off (the final two candidates competing), the danger of political assassination represents a significantly higher risk than an election of several hundred parliamentarians to an assembly. Similarly, if an election is being conducted as part of a post-conflict peace agreement, it has a very different risk profile to an election held in a country with an unbroken history of democratic elections.

One methodology to map an election's risk profile is by the identification of mission critical assets (people, infrastructure, information and materials), without which, the election cannot reasonably proceed. In combination, the unique structural and circumstantial aspects of an election will dictate at what phase of the process an asset is critical, and notably, if this may change between sub-processes. Some electoral processes by their nature are better able to adapt to certain types of attack. For instance, the destruction of ballot boxes at a polling station after polling has been completed may or may not cripple the ability of the electoral authorities to produce a result from the election. The impact of such an attack will vary significantly depending on a range of both structural and circumstantial factors. Separating 'mission critical' from 'recoverable' threats is a key step in building the election risk profile and determining priorities.

Against the backdrop of these regular security challenges, several new threat trends have emerged in the past few years. These include international terrorism and organised crime:

- *International terrorism*

  As a well-recognised ritual of democracy, elections can attract threats from diverse groups, whose motivations may have no connection to the national stakes of an election. As recent events have demonstrated, international terrorists have the capacity and motivation to conduct "spectacular attacks" geared towards fulfilling their own propaganda agendas. The intensity of media coverage during an election is a highly visible period, affording an attractive opportunity for such attacks to occur.

- *Organised Crime*

  The political tensions that arise during an election offer organised crime groups an appealing opportunity – at a time when the authorities' ability to differentiate between politically motivated violence and criminally motivated violence can be extremely difficult. Paradoxically, a group committing politically motivated offences may try to have their actions interpreted as purely criminal, whereas criminally motivated groups may wish to obscure their actions behind a political façade. Of further concern, these interests have become convergent in some post-conflict settings, where organised

criminal groups have been known to kidnap individuals and sell the hostages to political groups for propaganda value.

It is necessary in any section on electoral threats and analysis to highlight a cautious approach in carrying out this function. As noted in the principles above, non-partisanship and impartiality as well as transparency and accountability are important guides for electoral security. The choice of methods and subjects of information collection, during an election period, must be sensitive to the possibility of interpretation as a political intent and possible backlash. As such, extra emphasis on procedures that adopt checks and balances, are an important safeguard of the analytical process during elections.

Security Actors

In broad strokes, security arrangements can be divided into three main types: static (e.g. protection of warehouses, polling stations and offices), mobile (e.g. protection of voter registration teams or campaign rally sites) and reserve (e.g. contingency forces to support either static or mobile forces as required). Within these three broad categories, the types of security tasks involved vary widely and depend upon significantly different capacities (skills and numbers) and lawful authorities. In many cases, the assignment of these tasks will be dictated by 'best fit' to function (involving a division of labour among several security institutions or contractors), but can be constrained by legal, financial and political conditions.

Legally, the assignment of security responsibilities to institutions for an election varies significantly worldwide. In many cases, the police force is designated with the primary responsibility for election security, due to constitutional limitations imposed on the domestic deployment and use of military forces. In some countries, the involvement of the military forces is outright prohibited and uniformed personnel are required to stay in barracks on polling day. In other countries, the military is integrally involved, but may do so under special arrangements, such as the head of the electoral management body temporarily assuming the mantle of

Commander-in-Chief of military forces. Elsewhere, police forces may be able to utilise military personnel and equipment through regular legal provisions (such as secondment arrangements).

The financial arrangements for security services can become a controversial issue between security and electoral institutions. This controversy (if it arises) principally stems from the high costs associated with such large scale operations, additional costs incurred by late amendments, and whether the costs should be borne as part of the electoral process (and therefore by the electoral management body) or as a function of the security forces (and therefore by the budget of the security forces). The resolution of this problem will depend on the formal arrangements of government in a particular country, but is also influenced by the electoral and security institutions ability to identify the problem early in the strategic planning phase, and find a mutually satisfactory solution.

Political constraints may also affect the assignment of security forces to particular tasks in the electoral period. If a security actor has been the subject of controversies relating to partisan bias, the use of these forces in some aspects of the electoral process may be counter-productive to gaining the trust of the participants. For example, in a post-conflict environment, the involvement of the State security forces in the conflict may have created a level of distrust that can necessitate alternative arrangements. In this post-conflict scenario in particular – especially if military and police forces are undergoing major reforms in parallel to the election process – the deployment of these forces can be detrimental not only to the election, but to the reforming institutions.

Neither are security actors in an election process limited to formal security institutions. Political parties, civil society groups, non-governmental organisations (NGO's), the media and election observer groups can all have an influence on the security environment through various mechanisms. Political parties may enter into a mutually agreed Code of Conduct that guides the behaviour of their supporters and candidates. Civil society and NGO's (national and

international) may undertake information campaigns, public debates or use other strategies to assist in defusing political tensions. Media outlets may also follow a Code of Conduct that deters speculative reporting that could unnecessarily heighten political tensions. And, electoral observers may also mitigate intimidation and other threats to the process, by virtue of their presence and scrutiny of the process.

Electoral Special Security Measures

Several measures have evolved in different countries to enhance security during an election. The applicability of these measures varies given the unique circumstances. Listed below is a non-exhaustive list of special measures or arrangements that might be considered by election and security officials:

- *Joint Operations Centre (JOC)*

  The establishment of a Joint Operations Centre (JOC) has become a common feature of efforts to coordinate security and electoral operations. Normally established some months before an election, the JOC contains representatives from a range of institutions and acts as a nexus for information sharing, planning, briefing and monitoring the electoral process.

- *Dedicated Training on Security*

  The development and delivery of a training package for security officials involved in an election. Normally this step is reinforced by the distribution of 'Election Cards' to security force personnel – outlining key points about the process, their expected behaviour and lawful authorities. Similarly, the training delivered to electoral staff should include a component that outlines the role and integration of security personnel into their activities.

- *Weapon Exclusion Zones*

  During registration, campaigning, polling and counting exercises, special legal provisions may come into force that create a 'weapon exclusion zone' around these sites. Normally, the only persons legally bearing arms within these zones are appropriately authorised security personnel.

- *Coordination of Campaign Rallies*

  Under relevant Public Law and Order provisions, electoral and security officials may require political parties to register the date, time and place of campaign rallies. In these circumstances officials may impose schedules, to ensure opposing rallies do not occur in a proximity that could create conflict. Arguably, this may be deemed to be a restriction on the right of freedom of association in some circumstances; however, this constraint can be justified if public law and order issues are a valid risk.

- *Campaign 'Cooling-Off' Period*

  Several countries impose a "cooling off" period between the end of the campaigning period and polling day. This cooling off is intended to reduce the amount of political rhetoric and tension between opposing parties, as their respective supporters go to vote together at polling stations.

- *Security Media Component (Proactive and Reactive)*

  In the course of an election, security forces may become the subject of disinformation campaigns. Disinformation campaigns may seek to misinform voters about the role, behaviour or credibility of security forces. In the first instance, a proactive information campaign seeks to explain the role of security forces in the process, which can deter disinformation efforts. In reactive circumstances, security forces should have the capacity to respond quickly and effectively in the media to journalist enquiries or disinformation.

- *Enhanced Communications Network*

  An effective communications system is well recognised as a 'force multiplier' for operational activities. For an election, ensuring that both election and security officials have appropriate communications equipment and interoperability at key levels – significantly enhances responsiveness and efficiency, as well as avoiding misunderstandings.

- *Security Consultative Meetings and Liaison*

  In certain circumstances, it may be necessary for security officials to pursue liaison and consultation with local communities to explain their role in an election. Offering an opportunity to exchange expectations, these meetings can be highly productive in alleviating concerns. If follow-up is necessary, a reliable security focal point (or

team) may be appointed as a dedicated channel for election related security issues. It is strongly recommended that if this type of engagement is initiated, representatives of the electoral authorities are directly involved to avoid inconsistent messages.

- *Rules of Engagement or Use of Force Policies*

  Security forces often outline a policy framework termed a 'Rules of Engagement' (RoE) or 'Use of Force Policy' (UoF) to guide the actions of their personnel in certain circumstances. Usually, these policies guide security forces on what action is considered to be a reasonable and proportionate response to certain types of threats. During an election these policies may need to be reviewed with an emphasis towards ensuring that security forces are not 'baited' into actions that may later be politicised. In the case that security providers are contracted by an electoral institution, a use of force model should be clearly outlined in the contracting arrangements.

- *Code of Conduct*

  As has been mentioned earlier, several different groups, such as political parties and the media may enter into a Code of Conduct to guide their behaviour during an election. Security forces may also enter into a Code of Conduct to administer the behaviour of their personnel during an election.

- *Investigation Taskforce*

  Irrespective of the forum to which an electoral dispute is brought, the ability to rapidly and competently investigate the asserted facts is essential to defusing uncertainty. The awareness that any allegation will be thoroughly and competently investigated, can in itself, deter frivolous or malicious disputes from arising. Assembling a credible, impartial and competent investigation taskforce, solely for electoral matters may therefore pre-emptively defuse unnecessary disputes.

The measures outlined above offer a sample of the range of security solutions that might be considered during an election process. The desirability and suitability of certain measures, or their combination, should stem from the threat analysis and strategic planning stages.

Conclusion

Elections are a potent tool to defuse conflict and create a means of finding negotiated resolutions. As these peaceful means seek to resolve *inter alia* social, political, ethnic, religious

and economic divisions, an election is a period of heightened tensions. Security is pervasive in this process and can affect both the actual, and perceived, legitimacy of the electoral outcomes. An equitably secure environment for electoral participants is fundamental to their engagement in the process, and by extension, the goal of an election itself. Whether or not an election lifts a conflict out of violence, or generates conflict, is strongly influenced by the integration of effective security policies and practices, into the electoral process.