Unchecked Powers of the Ethiopian National Intelligence and Security Service in the Prevention and Countering of Terrorist Crimes: Some Disquiets at a Glimpse

Shimels S. Belete (Dr. juri.)
Europa-Universität Viadrina, Frankfurt (Oder), Germany

Doi:10.19044/esj.2018.v14n29p211 URL:http://dx.doi.org/10.19044/esj.2018.v14n29p211

Abstract

This article questions the supreme role of the Ethiopian National Intelligence and Security Service (NISS) in the prevention and countering of alleged terrorist acts vis-à-vis its institutional legitimacy and operational integrity. With no exception to other states, Ethiopia also re-established the National Intelligence and Security Service in 2013 but as a sole and unique institution of its kind with multiplex mandates both on general and specific intelligence and security matters. Having in mind the more sensitive powers conferred to the institution and its unrivalled authority in masterminding all the preventive and punitive measures against alleged terrorist conducts as enshrined under the Anti-Terrorism Proclamation of the country, this article examines whether the establishing proclamation has set the required normative standards and watchdogging institutional platforms to ensure its functional accountability. After investigating the Service's organizational structure, the public, judicial and political watchdogging apparatuses, the lack of administrative and financial transparency, as well as the alleged alliance of the institution to the regime in power, this article submits that the Ethiopian National Intelligence and Security Service lacks the key attributes of a politically independent and functionally autonomous institution that strives to protect the nation's politico-economic and security interests. As it stands, much of the Services's mission rather appears to have been constricted to serving as an untouchable guardian of the party or the regime in power, or as a rising unique entity that roams on its own impervious orbit.

Keywords: Ethiopia, National Intelligence and Security Service, counter-terrorism, Intelligence, watchdogging, accountability

> *"Intelligence report prepared in relation to terrorism, even if the report does [not] disclose the source or the method it was gathered shall be admissible by the court."* (FDRE Anti-Terrorism Proclamation 652/2009, Art. 23(1)).

1. Introduction

Needless to say – particularly at this time when the world is confronting the threat of terrorism as one of the gravest trepidations to the international peace and security – only few would contest the irreplaceable role that national intelligence and security service agencies could play in making state's action for the prevention and countering the crime a success (Hughbank & Githens, 2010). As a preliminary note, infiltrating deep into all the multi-disciplinary views based in philosophical, political, military and/or security discourses on matters relating to intelligence and security organs of any government is beyond the reach of this article. It is rather restricted more into the minimum legal tin-tacks that the law is normally expected to regulate, and if not, the malfunction of which would cause some unjustified or at least unintended grim to the entire system.

With this scope in mind, an attempt is made to pinpoint some of the very grand issues relating to the overtly extended but unfettered powers of the Ethiopian National Intelligence and Security Service in light of its role in the prevention and combating terrorism. In so doing, the organisational accountability and oversight or supervision mechanisms, budgeting and issues of transparency, and more specifically, the actual and potential use of intelligence information in the overall national counter-terrorism normative settings, as well as its impact on the daily functioning of the ordinary law enforcement in the criminal justice system are roughly inquired.

2. Re-establishment of the National Intelligence and Security Service: A Rogue Elephant?

It goes without saying that 'Intelligence and Security Services' – no matter how shadowy – are one of the very crucial aspects in the success or otherwise story of any government in all its political, economic, diplomatic, security and overall national interest affairs – be it democratic, authoritarian or any other form or system of government (Omand, 2010; Johnson, 2010; Svendsen, 2012). With no exception to its counterparts, Ethiopia has also been accustomed to the system mainly after the establishment of the National Security, Immigration, and Refugee Affairs Authority back in 1995 (FDRE, Proclamation No. 6/1995). With no need to look back into the former intelligence and security frameworks, the current institutional setup, i.e.; the National Intelligence and Security Service (NISS) was re-established pursuant to Proclamation No. 804/2013 (Art. 4).

A sift probe to some of the provisions of this proclamation may definitely be a stirring factor to raise multiple questions. For one thing, it is only this

institution that the Proclamation entrusted as a sole operator of all matters of intelligence and security – including that of international intelligence cooperation (Ibid, Arts. 7-9). Neither a regional nor other federal intelligence and/or security services can be established (Ibid, Art. 4(3)). Even within the NISS intra-institutional setup, there is no explicitly mounted organisational subdivision with a separate functional autonomy that takes into account the various purposes and goals of intelligence and security. In fact, article 11 of the Proclamation appears to indicate the internal organogram and structure of the institution by dictating the Service to have a Director General appointed by the Prime Minister, Intelligence Organs, Security Organs, Support Organs, and the necessary staff. However, none of the powers and duties of each department are explicitly defined. Nor is their horizontal and functional autonomy explicitly stated and regulated so that it is only the NISS as a single entity established and recognized by the Proclamation in its legal personality.

In some other national jurisdictions, there are independent and specific task-oriented intelligence and security agencies. At the federal level alone, Germany has, for example, four distinct and functionally autonomous intelligence and security departments: the Federal Intelligence and Security service (*Bundesamt für den Verfassungsschutz)[BfV*]; the Federal Foreign Intelligence and Security Service (*Bundesnachrichtendienst*) [*BND*]; the Federal Criminal Intelligence and Security Service (*Bundeskriminalamt) [BKA*]; and the Federal Military Intelligence and Security Service (*Amt für den Militärischen Abschirmdienst) [MAD*] (FAS, Pike & Aftergood, 2018). They are explicitly established and recognised by law with their own independent legal personality and maintaining visible demarcation of their respective missions - besides the general policy-based cohesion and collaboration expected among the divisions, given the reality that it is the national interest, which all are understandably pursuing to ensure (Heyer, 2007; Wetzling, 2016; Wetzling 2017).

Also in the United Kingdom, the Secret Intelligence Service (MI6); Government Communications Head Quarters (GCHQ), and the UK Security Service (MI5) are the three main agencies mandated to carry out the national intelligence and security matters within their own distinctive veins under the supervisory oversight role of the Intelligence and Security Committee (ISC) (Morrison, 2007; FAS, 2018). Alongside, additional four intelligence agencies – the Joint Intelligence Organisation (JIO), the National Security Secretariat (NSS), the Defence Intelligence (DI), and the Office for Security and Counter-Terrorism (OSCT) – are also operating to carry out specifically assigned security and intelligence missions (ISC Annual Report, 2017). Likewise, in the US, out of the reportedly seventeen functionally active intelligence and security agencies, the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) are the two principal institutional platforms that

are undertaking the intelligence and security activities in light of their own respective missions and objectives (Johnson, 2007; FAS, 2018; ODNI, n. d.). In Bulgaria, almost in a similar fashion, divisions containing: The Foreign Intelligence; the Domestic Counter-Intelligence, the Military Counter-Intelligence, the Technical Intelligence, and the VIP Protection and Political Counter-Intelligence are established with their own prioritised mandates and missions (Born & Capparin, 2007).

Back to the continent of Africa, in South Africa, for instance, the National Intelligence Co-ordinating Committee (NICOC), South African Secret Service (SASS]), National Defence Force Intelligence Division, National Intelligence Agency (NIA), and South African Police Service (SAPS) are the five main divisions that possess their own exclusive intelligence and security powers and duties (Ford, 1997; Nathan, 2010); Dietrich, 2016; FAS, 2018).

What can be grasped from these varied national experiences is the reality that there is no uniformity among states in their institutional structural approach while setting the intelligence and security sector. Indeed, there should not be a necessity for sameness as there is nothing more 'national' than the issue of 'national intelligence and security' itself (Scheppele, 2010, p.437). Accordingly, expecting similarity would be an ignominy to the reality. This said, however, a more thoughtful observation of the models adopted in the aforementioned states would indicate some aspects common to all, and the rationales behind thereof. In most States, at least three or more institutions are established with mandates to handle such a sensitive task but in a separate, autonomous, well-defined and varied objectives. The raison d'être behind all these arrangements seems apparently clear. For one thing, 'intelligence' in itself as a secret information obtained in secret" (Morrison, 2007, p. 42), it is not a *'single-purposive*' ingredient in any decision making. Some intelligence information is used for military policies, decisions, and strategies while others are referenced for diplomatic and foreign relations. Still, other intelligence feedbacks are collected to analyse the internal security whereas a range of other clandestine information is often deployed as inputs to justify the overall economic, political and technological policy directions (Johnson, 2010).

But not all these bunch of intelligence information have, or even need the same level or degree of secrecy, credibility, acceptance, and consumable status (Selth, 2009; Giupponi & Fabbrini, 2010; Rebugio, 2013; Gainor & Bouthillier, 2014). Accordingly, the more non-compacted and systematically clustered intelligence and security institutions are organised in a State – assuming full ownership and responsibility with particular reference to each of the traditionally known purposes of intelligence information as narrated above – the highly it becomes pursuable to maintain accountable, legitimate, public interest-oriented, flexible and purpose-based management of the entire intelligence and security operation of the state. To the contrary, leaving such a

complex intelligence and security mission simply with a mingled arbitrarily listing of a range of powers and authorities to a single institution might trigger the gradual creation of an uncontrolled intelligence and security agency as a sole and vicious animal that roams alone; that is a rogue Elephant.

That was what Germany experienced during the Nazi regime that had led to the creation of the 'Gestapo' state secret police (*GeheimeStaatPolizei*), which was known for its notorious brutality. Establishing the current special unit of the Federal Police, i.e., the Federal Criminal Intelligence and Security Service [Bundeskriminalamt] (BKA) is, therefore, largely regarded as an institutional readjustment which aims rectifying such a historical discontent by curbing some unsolicited fusions with that of the works of the general intelligence service (FAS, 2018).

In light of the existing legislative and practical quirks, it would be nonsensical to neglect the risk for the emergence of a similar 'Gestapo' in the Ethiopian context. The National Intelligence and Security Service (NISS) – as an exclusive and *sui generis* organ of its kind – is endowed with all unbridled powers and duties in arbitrarily listed twenty-seven major activities under three major categories of general powers and duties, Intelligence powers and duties, and security powers and duties.

3. Powers and Duties: Merging Irreconcilable Operations?

As stipulated under articles 7 to 9 of the Proclamation, the NISS's principal mandates range from that of the power to follow up and investigate any internal and external activity intended to overthrow the constitution and constitutional order to that of heading and coordinating national counterterrorism cooperation and represent the country in international and continental counter-terrorism relation, and cooperation as a leading representative (NISS Re-Establishment Proclamation No.804(2013), Art. 8 (1 & 2)). The NISS is also entrusted with the power to investigate terrorism and extremism and collect intelligence and evidence. It also carries out the task of following up and investigate espionage activity against the interest of the country and its people and collect information and undertake counter-espionage activity (Ibid, Art. 8(3 & 5)). Alongside, NISS is also empowered to pursue and collect intelligence and evidence on other serious crimes which are threats to the national interest and security and can conduct surveillance on any person suspected of having committed any of the aforementioned criminal activities (Ibid, Art. 8(6 & 7)). By the same token, the task of preparing and submitting to the government, of criteria for the classification and level of protection of confidential information and follow up its implementation upon approval remains its mandate. Besides, the NISS also assumes the duty of providing security to the heads of the state and the government as well as critical institutions (Ibid, Art. 9(5, 8 & 12)). It is also the duty of the NISS to

lead the national aviation security (Ibid, Art. 9(3)). Other missions such as detecting threats to the national economy and development; serious problems of good governance and conspiracies; providing nationality and immigration service to Ethiopians alongside monitoring services to refugees; licensing and issuing security clearance for private security organisations; and overseeing the issuance of the national identity card are also singlehandedly undertaken by this institution (Ibid, Art. 8 (1, 4) and Art. 9 (1, 2, 4,5,6 and 11).

4. Specific Powers of the NISS in the Prevention and Countering of Terrorism

With regard to the specific institutional deficits of the NISS associated to its unalloyed powers in the prevention and countering of terrorism, one has to methodically analyse the various authorising provisions of the anti-terrorism proclamation. Accordingly, for a heuristic purpose, the towering clouts of the NISS can be summarised and displayed from three overarching functions entrusted to this institution.

Firstly, article 30 of the Anti-Terrorism Proclamation bestows the leadership role in the operation of the National Anti-Terrorism Coordinating Committee to the NISS. The Committee – which is in charge of preventing and controlling terrorist acts by drawing up a counter-terrorism plan with a joint task force – is composed of the NISS, the Ministry of Justice (replace by the recently established Office of Attorney General), and the Federal Police Commission represented by their respective heads. Needless to say, this compositional setting depicts nothing but the hierarchical supremacy of the NISS over the other two ecumenically acknowledged law enforcement organs of the state that are left merely as subordinate bodies for the task of preventing and countering terrorism in the country. Such an intelligence and security-based approach to a perceived or actual threat of terrorism have put in limbo, of the very demanding duty of the state to scrutinize and normatively harness the proper functioning of the NISS. At the same time, such a virtual portrayal of the ordinary law enforcement organs as subservient bodies to intelligence and security service also egregiously undermines the already deteriorated values of rule of law and the various due process rights to have no place in the daily operations undertaken under the guise of the prevention and countering of terrorism.

Secondly, as an institution in charge of leading the operational task of averting terrorist acts, article 14 of the Anti-Terrorism Proclamation empowers the NISS to intercept and conduct surveillance on the telephone, fax, radio, internet, electronic, postal, and other similar communications of a person suspected of terrorism, and this includes the power to enter into any premise in secret to install and enforce the interception (Anti-Terrorism Proclamation, Art. 14(1)). To this end, every communication service provider is duty-bound

to cooperate when requested to do so by the NISS. This same provision also requires the information gathered through such a method to be kept in secret (Ibid, Art. 14(2)). Even if securing a court warrant is stipulated as a requisite in order for the NISS to exercise these powers, a careful reading of article 23 of the Proclamation would denote that the requirement of a court warrant is virtually inconsequential (see the discussion infra).

The third fundamental authority of the NISS emanates from its role and direct involvement in dictating the ordinary criminal litigations on cases relating to terrorism. This is mainly because of the emphatically unchallengeable trust commended to it by recognizing its intelligence reports, *ipso facto*, admissible in court proceedings. As clearly provided under article 23 (1) of the Anti-Terrorism Proclamation, even if the NISS does not disclose the source or the method used to gather the information, intelligence report prepared in relation to terrorism is deemed valid and admissible in court.

The key but comprehensibly unreciprocated question is, therefore, how logical and legitimate would it be to statutorily declare the admissibility of the information obtained by such an inundated, effusive and overwhelmed organ which is fully packed with multi-purposive tasks that may or may not require secrecy? Above all, the Proclamation's firm stand in blocking any chance of judicially probing the validity of the source and the methods deployed to extract the information exacerbates the risk of abusing the Institution's mandate while dealing with politically motivated cases frequently instituted against individuals targeted as threats to the regime in power rather than the public and the nation at large.

For that matter, the issue of whether intelligence and security sources have to be credible evidence in ordinary criminal litigation is highly debatable (Voorhout, 2005; Vervaele, 2005; Forcese & Waldman, 2007; Born et al, 2011). Obviously, it is irrefutable that – given the present-day complexity of the threat of terrorism – the work of gathering intelligence and prosecuting alleged perpetrators of the crime are becoming the two sides of a coin both in the preventive and retributive aspects of countering terrorism. Accordingly, cooperation and information-sharing between intelligence and security services and law enforcement institutions could be both strategically and practically effective (Završnik, 2013).

This said, however, as soundly submitted by Eijkman & Ginkel (2011), such a concurrent approach has to be compatible with fundamental rights and basic principles of rule of law and the right to fair trial. The later is a principle that demands ensuring the right of everyone – including terror suspects – to be presumed innocent until proved guilty, and their right to be tried publicly within a reasonable time by an independent and impartial judiciary (Ibid, p. 4). Moreover, even in states where such cooperation between the intelligence and security institutions and law enforcement organs is persistently increasing,

those evidences emerging from the intelligence are usually used only for the purpose of alarming the police so that the later may initiate investigation, instead of directly forwarding those intelligence sources as end products to serve as valid evidence in court without any judicial scrutiny and authentication (Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights, 2009).

Accordingly, if such an institutional nexus is to enhance the realistically and synergically expected outcome in the prevention and countering of terrorism, there needs to have a strict normative and procedural standard that should properly govern the admissibility status and the manner of (un)disclosing information, but without diluting the undeniable right of the accused to refute such information, not only substantially but also by challenging the source and the modus the evidence was procured.

This requisite emanates from the very grand purposive difference between the work of intelligence and that of the ordinary law enforcement organs. That is, intelligence and security agencies are tasked with a mission of collecting information for the purpose of national security whereby – for all the possible reasons – 'keeping confidential of all the sources' becomes the governing rule. The law enforcement agencies (police and public prosecutor), on the other gather evidence for criminal investigations in which case, a "fair trial principle" serves as a guiding rule that allows both the prosecutor and defence counsel or the suspect to enjoy equal access to the evidence (Eijkman & Ginkel, 2011, pp. 5-6).

Looking at the Ethiopian approach as adopted in the two proclamations – the Ethiopian Anti-Terrorism Proclamation (Art. 23) and the National Intelligence and Security Service Re-establishment Proclamation (Arts. 4, 7-9) – its indefensible consequential pitfalls can be summarised in threefold: First, there is a *sui generis* intelligence and security organ (NISS) entrusted to undertake several but mingled and effusive intelligence and security powers and duties. Secondly, its intelligence information are intrinsically recognised as admissible evidence in ordinary criminal litigations involving terror suspects; and such admissibility is to be reckoned irrespective of the secrecy as to the source from where and the means how the information was extracted – leaving unguarded the accused's absolute and non-derogable protection from torture and other forms of ill-treatment. Moreover, such a blurring role of the NISS is diminishing the unwavering right to fair trial and the constitutional guarantee of presumption of innocence of the suspect, which at the end, facilitates arbitrariness in depriving the suspect's liberty on long-term sentence after conviction relying on these evidence.

The judiciary and the ordinary criminal law enforcement organs are not the only institutional settings of the state that are suffering from the NISS's extended hand influence in their decision making. In this regard, article 25 of

the Anti-Terrorism Proclamation has also exposed the decision-making authority of the House of Peoples' Representatives (HPR) – which is the supreme legislative and political organ of the state – to remain under the shadow of the NISS. This is mainly because, even if the HPR holds the final power to proscribe a certain entity or group as a terrorist organization, its decision exclusively relies on the information to be submitted by the NISS as the only intelligence wing of the government in power. This one-sided-source oriented approach makes the decision of the Parliament problematic. On top of such an immutable pitfall is the absence of any intra-reviewing mechanism or other external platforms to challenge the decision either through a proper judicial review or at least through a quasi-administrative appeal options. Accordingly, the sketchy and forceful hands of the National Intelligence and Security Service in dictating decisions on proscription of entities as a terrorist organisation also needs a special attention.

In view of all the afore-highlighted sensitive powers and functions of the NISS, it would only be logical if one expects normatively tightened and institutionally robust mechanisms of monitoring and controlling its activities. In the section underneath, an attempt is made to examine whether such indispensable oversight platforms are put in place to ensure the institution's accountability and independence in its daily functioning.

5. Oversight and Accountability Mechanisms

The other trepidation relates to the capricious oversight mechanisms incorporated in the NISS establishment proclamation. Ensuring the political independence and accountability in the work of the National Intelligence and Security Service demands estimable tools of oversight (Wetzling, 2016; Parliament of Australia, 2017). In this regard, there are critical issues that need to be analytically confronted.

As a point of departure, the National Intelligence and Security Service is established having a 'Ministerial Status' (NISS Re-Establishment Proclamation No. 804/2013, Art. 4(1)) like that of, for example, the National Revenue and Customs Authority (Customs Proclamation No. 859/2014). This implies its equal *status* with other ministerial offices of the federal government in terms of channels of hierarchical accountability to the House of Peoples' Representatives as the highest legislative and political body of the country.

Having this in mind, the FDRE Constitution (Proclamation No. 1/1995) under articles 55 (13) and 74 (2) requires parliamentary approval of nominees for ministerial positions and other top officials by the House of Peoples' Representatives. As a result, the authority of the Prime Minister is limited only to propose qualified nominees for the positions, and to request the House for final endorsement (Ibid, Art. 55(13) & Art. 74(2)). More contiguously, the House is unconditionally authorised under article 55 (7) of the Constitution to

determine the organisational structures of the National Defence, Public Security and the National Police, and to investigate and take necessary measures in case when the conduct of any of these organs infringes upon human rights and the Nation's Security (Ibid, Art. 55(7)). Accordingly, this constitutional mandate is supposed to have an indispensable value in any argument demanding for a conceivable oversight of the National Intelligence and Security Service beyond the more preferred executive-centered supervision mechanism as stipulated in the Proclamation.

The multifarious deviations in approach from the aforementioned constitutional expectations could be extracted from the various provisions of the Proclamation that govern matters of accountability and supervision or oversight. To begin with, unlike the other Ministerial Heads (Ministers), the Director-General – as Chief Executive officer of the Service (NISS) – is directly appointed by the Prime Minister with no need to submit the nominee to the Parliament for a final endorsement (NISS Re-Establishment Proclamation, Art. 11(1)). Then again, the NISS as an institution is accountable to the Prime Minister (Ibid, Art. 12(1)), and hence the same person monitors and supervises the activities of the Service in the course of exercising his power of executive oversight (Ibid, Art. 23)

Likewise, reports regarding the activities of the Service have to be submitted to the same person - the Prime Minister (Ibid, Art. 12(2(g)). Moreover, this same Head of the Executive has the authority of approving NISS's institutional budget (Ibid). Under these circumstances, it is plainly observable that the Prime Minister is everywhere in the works of the institution, from the very initial stages of appointment and budget-related powers to those of monitoring and superintending the overall functioning of the organisation.

At the outset, two arguments in descent to this conclusion might be inferred from articles 22 and 24 of the Proclamation as these provisions seem to recognise non-executive oversight mechanisms by incorporating the legislative and judicial supervision platforms respectively. Alas, a careful reading of these provisions in conjunction with the other components of the proclamation, however, would compel one to be sceptical of their efficacy as asserted as follows.

To begin with, the judicial oversight as stated under article 24 is manifested by the court's power of issuing a warrant for the National Intelligence and Security Service to authorise the later to conduct surveillance against individual targets. Conversely, however, this power of the court becomes trivial by the fact that Art. 23 of the Anti-Terrorism Proclamation has blocked all the possibilities of probing the source and the methods used by the NISS while gathering the reported information. As a result, from the very beginning, the procedural issue of whether the Service was authorised by the

Court through a warrant to legitimize its act of surveillance would not be raised as an issue to the attention of the Court. To put it in other words, there is no any effect as to the validity of the information collected by the NISS even in cases where its actions were not backed by the blessing of the Court via the issuance of the required warrant. For that matter, the law has plainly stipulated that these intelligence information are admissible in the ordinary criminal court litigation with no need to disclose the source and the method implemented while procuring the evidence (See above, Section 4).

On the part of the judiciary – let alone in the presence of such a legislative restriction on its inherent power of probing the commendable value of evidences submitted to it, plus, the politically sensitive nature of cases on terrorism – there seems to have inconsistency and lack of well-articulated judicial precedence in its interpretational jurisprudence on matters relating to evidence even on matters relating to ordinary crimes (Assefa, 2012). The judicial understanding of the doctrine of '*proof beyond reasonable doubt*', as a standard of proof in the criminal litigations may be cited as a typical illustration of this aspect. One writer noticeably submits that:

> "[...] plenty of court cases prove that Ethiopian courts and litigating parties ritually invoke proof beyond reasonable doubt. This does not mean, however, that they always employ this same standard, understand what it means and apply it in its proper sense" (Wodaje, 2010, P. 128).

This floundering practice and unwarranted flexibility in the application of the standard of proof is visible not only in the judicial works of lower courts but also at the highest appellate courts. As insightfully observed by Zemichael (2014), nor is the practice of the Federal Supreme Court Cassation Bench – the highest judicial organ legislatively empowered to render binding judgments on issues of law (Federal Courts Re-Amendment Proclamation, Proc. No. 454/2005, Art.2(4)) – far from such an inconsistent understanding of the principle. The Court's slack standard in its application of the principle has been demonstratively visible in some of the cases it has rendered (Assefa, 2012). In light of this, the oversight role of the judiciary resembles to be more of a cosmetic than that of a profoundly adjusted and dependable monitoring mechanism with a capacity to cement accountability in the work of the NISS as an institution and its individual intelligence and security personnel.

Coming to the legislative oversight, article 22 of the NISS Re-Establishment Proclamation requires an appropriate 'Standing Committee' of the House of Peoples' Representatives to oversee the general activities of the Service. Out of the eighteen standing committees formed in the present Parliament (2015-2020), the Foreign Relations, Defence (Military) and Security affairs Standing Committee is in charge of this mandate (FDRE, House of Peoples' Representatives Office of Spokesperson, 2017). This same

Committee also oversees the Ministry of Foreign Affairs, the Ministry of National Defence, as well as, the Ethiopian Peace and Development International Institute (Ibid). More stunningly, a bird's eye review of the listed responsibilities and powers of the Committee would reveal that almost all the monitoring activities that the Committee pledged to follow-up are more directed and concentrated to the works of the other organs other than the NISS (Ibid). Such an aversely asserted monitoring power is further decayed by the overtly restrained power of the Committee under the guise of National Security. As clearly cemented under article 22 (2) of the Proclamation, "The Committee's oversight under sub-article (1) of this-article may not be conducted in a manner that jeopardizes the national security of the country." This very general and imprecisely articulated restriction diminishes the watch-dogging authority of the Committee and its genuine impact on ensuring the democratic accountability of the institution. In this context, therefore, the Committee is overseeing the National Intelligence and Security Service not as a very sensitive organ which requires a watertight scrutiny rather as an ordinary federal government office that would the Committee visits once in a while (if at all).

Furthermore, neither is the Parliament, as the highest politically authoritative body of the federal government capable of evaluating the general works of the NISS. While other ministerial offices are directly accountable to the Parliament at least through their duty of appearing before the House for questions and by submitting their quarterly, half, and annual performance and budget reports (FDRE Constitution, Art. 55(17)), the NISS on the other hand is not required to submit its report directly to the Parliament given that its accountability goes to the Prime Minister (NISS Re-Establishment Proclamation, Art. 12(2(g)).

As a point of comparison, referring some experiences from other jurisdictions would be of help, lest to highlight the missing elements in the Ethiopian context and its impact in maintaining effective and accountable supervision mechanism of the works of the intelligence service (European Parliament, 2011; Australian Parliament 2017). In view of this, in Germany for example – aiming to retain the balance between the need to keep secrecy of the intelligence work on the one hand and the need to uphold a transparent and accountable operational system indispensable in a democratic society on the other – a citable model of parliamentary oversight is adopted in auditing the works of the intelligence services since 1978 and as later strengthened in 1999 (Heyer, 2007). With due cognizance to some concerns about its efficiency (Wetzling, 2016, Wetzling 2017), a Parliamentary Control Panel which is accountable to the *Bundestag* (German Parliament) is in charge of this sensitive task.

The composition, its working procedures, and the substantial and effectual deepness of its mandate makes the Panel one of the most creditable intelligence monitoring and supervisory mechanisms. Firstly, the Panel is required to be composed of members that represent all competing political parties in the Parliament. Secondly, the Parliament has to set its working procedures, and each member of the Panel needs to have the trust of the majority of the Parliament. With such composition and vote of confidence granted to it by the Parliament, the Panel is mandated to scrutinize both the general matters of policy and finance but at the same time, the daily operational details and routine activities of the intelligence community (Act of 11 April 1978 (Federal Law Gazette I. p. 453), last amended by a law of 26 June 2001, Federal Law Gazette I. pp. 1254, 1260). For this task to be effective, the Federal Government is obliged to provide as complete as possible information (ENNR, 2012). Even in some cases, if it is deemed necessary by the majority of the members of the Panel, it may appoint external and neutral experts to conduct inquiries into specific cases, the results of which could be used by the Panel in the course of exercising its watchdogging power (Heyer, 2007, p.72). Aside such overwhelming powers of the Parliamentary Control Panel, the intelligence and security works are also subject to supervision by other committees such as The Interior Committee, Defence Committee, *ad hoc* Committees of Inquiry, the G10 Commission, and the Bundestag itself. Moreover, courts in the form of judicial review have also general mandates to oversee the overall activities of the intelligence community (Wetzling, 2016).

Albeit with a different model, the UK has also political supervision on the intelligence service through a sophisticated system of monitoring different intelligence operations. This said the principal power of oversight is vested in the quasi-parliamentary body called the Intelligence and Security Committee [ISC] (Morrison, 2007; ISC Annual Report, 2017). There are also other responsible bodies, such as the Intelligence Services Commissioner, the Interception of Communications Commissioner, and the Investigatory Powers Tribunal; all exercising the power of controlling the proper functioning of the intelligence community (Ibid). Also, other states, inter alia, Canada (Collins, 2002; Australian Parliament, 2017), South Africa, Norway, and Poland have standardised their controlling systems either through robust parliamentary or via non-parliamentary, independent and specialised over-sighting bodies (ENNR, 2012).

Turning now to the Ethiopian context in contrast, what can be deduced from the current arrangement is nothing but the loosely (if not none) inculcated legislative oversight and an effectual exclusion of the judicial review; leaving the lion's share of this thin-skinned authority in the hands of the executive. This, coupled with the overall tendency of the waning role of the legislature, and the *de-facto* monopoly of the executive in a one-party system casts doubts

as to the legitimacy of this organ and its priorities – expounding mingled interests; public interest versus government interest; national interest versus party interest debates – in the domestic politico-legal quagmire.

With this arrangement whereby the head of the executive is masterminding the operation of the intelligence and security service, there is no guarantee against the political abuse and illegitimate functioning of the National Intelligence and Security Service as an institution and the staffs in their individual capacity. This might trigger twofold shortcomings: on the one hand, the unwanted risk for executive manipulation and the tendencies for hijacking the natural functioning of the National Intelligence and Security Service cannot be ruled out which may expose the Service being instrumental in achieving some illegitimate and arbitrary ends orchestrated by the executive.

On the other hand, the longer such a non-transparent and loosened supervisory structure of the intelligence and security landscape is maintained, the higher is the risk that NISS might eventually evolve as a rogue Elephant even without the knowledge and/or beyond the controlling power of the head of the executive itself, i.e. the Prime Minister. In view of this, the very recent bomb attack blast at the rally at *Meskel* Square in the capital Addis Ababa where tens of thousands gathered in support of the new Ethiopian Prime Minister could be cited as an example in substantiating such an inevitable concern (East African News, 2018). The attack was also reportedly aimed at targeting and assassinating the Prime Minister himself. No doubt that it's too early to conclude but as it stands, the then Head of the Anti-Terrorism Task Force of the National Intelligence Security Service and other top officials are currently on trial as suspected culprits charged with crimes of planning and orchestrating the explosion (ESAT, Ethiopia 2018).

The grand question is, therefore, having in mind all the aforementioned legislative and practical pitfalls in monitoring the Service's operation, how logical is it to rely on information gathered by this institution, at least in the absence of a methodical inspection mechanisms aimed at verifying the legitimacy of the methods and the procedures employed in procuring the evidence during the criminal litigation in the court of law? In highlighting the practical scenario with specific reference to the majority of terrorism cases, a group of Ethiopian Human Rights Activists reported that:

> "[...] the search for terrorists and the investigation process have been similar and unchanged. First victims are arrested by national intelligent and security services, detained in one of the detention centres and beaten and tortured until they confessed their crime. Then, the federal police crime investigation centre or "*Maekelawi*" will start investigation while they are in custody. The investigation will proceed under this department in its anti-terror unit that deploys over twenty investigators. Lastly, all

needed evidence will be cooked by the anti-terror unit investigators using different mechanisms." (Ethiopian Human Rights Project, 2014).

What appears rather disquieting is, therefore, such a delicate and practically ineffective monitoring setup, which lacks the necessary normative, procedural and institutional capacity and integrity. As a result, there is no guarantee that this critical gap in maintaining NISS's institutional accountability might gradually lead to a consequential risk of creating a landscape where the National Intelligence and Security operates as a rogue Elephant cementing itself beyond the reach of all the possible politico-legal and institutional controlling mechanisms of its activities.

6. Conclusion

To sum it up, looking at the role of the National Intelligence and Security Service in the prevention and countering of terrorism, the article submits that the two legislative frameworks – the Ethiopian Anti-Terrorism Proclamation No 652/2009 and the National Intelligence and Security Service Re-Establishment Proclamation No. 804.2013 – have cemented the Service as a 'lone-wolf' institution portrayed as unique organ of its kind. In so doing, two paradoxical and perplexing approaches seem to have affected its original institutional legitimacy and its functional integrity. On the one hand, the two proclamations have unwarrantedly merged a multitude of mandates and powers, and have entrusted this organ as a sole authority to lead and carry out all the functions. On the other hand, these same legislations are short of firmly stipulating the strict normative standards, and in creating a commendable politico-legal controlling platform that is capable of watchdogging and monitoring the daily functioning of the Service. Notwithstanding the delicately articulated indications for executive, judicial, and legislative oversight mechanisms, given the very demanding nature of scrutinizing its operation, and in comparison to the corresponding regulatory and institutional frameworks adopted in other jurisdictions, the Service appears to enjoy unfastened immunity. And hence, the key task of ensuring its accountability is largely compromised if not totally overlooked.

The repercussion of such an untied approach can be asserted in twofold standpoints. Firstly, in the context of the general institutional standing of the NISS, the most essential task of balancing its autonomy with that of the required level of transparency and accountability is left without a proper regulatory threshold. As a result, there seems to have no surety of preventing the two undesirable outcomes: i.e. either the risk that the NISS becomes too feeble to the extent fully controlled by the regime in power, or to that of the opposite upshot with the danger of gradually emerging as a completely unrestrained and powerful organ postulating itself as a *de facto* government that runs on own pact.

The second impact relates to the specific threat that the work of the NISS would pose to the rights of individual suspects. The Anti-Terrorism Proclamation has not only explicitly endorsed admissibility of evidence gathered by the intelligence but also has forfeited the fundamental procedural requirement of probing their validity. Accordingly, there is no guarantee for suspects' indestructible freedom from torture and other forms of ill-treatment. Such unauthenticated dependency on intelligence and security information has also in effect neglected the suspects' right to a fair trial and the right to the presumption of innocence as painted both in the pertinent international human rights instruments and the FDRE Constitution as the supreme law of the land.

References:

1. Assefa, S. K. (2012). *The Principle of Presumption of Innocence and Its Challenges in the Ethiopian Criminal Process*. Mizan Law Review, 6(2), 273-310.
2. Born, H, et al, (eds.) (2011). *International Intelligence Cooperation and Accountability*, Routledge, London.
3. Born, H. & Caparin, M. (eds.) (2007) *Democratic Control of Intelligence Services: Containing Rogue Elephant*, Ashigate Publishing, USA & England.
4. Collins, D. (2002). *Spies like Them: The Canadian Security Intelligence Service and Its Place in World Intelligence*, Sydney Law Review 24 (4). 505- 528.
5. Dietrich, N. (2016). *South Africa and the Southern African Regional Police Chiefs Cooperation Organisation: The Dialectic Between "National" and "Regional" Safety and Security?* In: Palloti, A & Engel, U. (eds.), *South Africa After Apartheid: Policies and Challenges of the Democratic Transition*, Africa-Europe Group for Interdisciplinary Studies, Brill, Leiden/Boston, pp. 240-261.
6. Eijkman, Q. & Ginkel, B. V. (2011). *Compatible or Incompatible? Intelligence and Human Rights in Terrorist Trials*, International Security, Amsterdam Law Forum, 3 (4).
7. ESAT, Ethiopia: *Anti-Terrorism Head with spy Agency on Trial for Coordinating Assassination Attempt on PM*. ESAT News, 08 August 2018. Available at: https://ethsat.com/2018/08/ethiopia-anti-terrorism-head-with-spy-agency-on-trial-for-coordinating-assassination-attempt-on-pm/. [last accessed 10 August 18].
8. Ethiopian Human Rights Project, (2014). *Rule of Law, Political Space and Human rights in Ethiopia: A closer look at the Anti-Terrorism Law*, p.3 retrieved from http://ehrp.org/wp-

content/uploads/2015/03/Final-anti-terrorism-investigative-report.pdf [last accessed on 10 August 2018].

9. European network of National Intelligence Reviewers (ENNIR). *Intelligence Review in Germany*. Retrieved from http://www.ennir.be/germany/intelligence-review-germany. [last accessed on 20 August 2018].
10. FDRE Anti-Terrorism Proclamation No.652/2009, Federal Negarit Gazeta, 15th Year No. 57 Addis Ababa, 28th August 2009.
11. FDRE Constitution, *Proclamation No.1/1995,* Federal Negarit Gazette, 1'1Year No.1 ADDIS ABABA - 21sl August 1995; Art. 55 (13) and Art. 74 (2).
12. FDRE House of Peoples' Representatives, *the National Intelligence and Security Service Re-establishment Proclamation No. 804/2013*, Federal *Negarit Gazette*, 19th Year, No. 55, Addis Ababa, 23rd July 2013.
13. FDRE, the Office of Attorney General of the Federal Republic Ethiopia Establishment Proclamation No.943/2016, Federal *Negarit Gazette*, 22nd year, No. 62, Addis Ababa, 2nd May 2016.
14. FDRE, the Security, Immigration and Refugee Affairs Authority Establishment Proclamation No. 6/1995.
15. Federation of American Scientists [FAS], Pike, J. & Aftergood, S. (2018). *German Intelligence Agencies.* Retrieved from http://www.fas.org/irp/world/germany/. [last accessed on 10 June 208].
16. Federation of American Scientists Intelligence Resource Program (FAS), *South African Intelligence Agencies.* Retrieved from http://www.fas.org/irp/world/rsa/**.** **[**Last accessed on 10 June 2018].
17. Forcese, C. & Waldman, L. (2007). *Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of 'Special Advocates'* in*: National Security Proceedings*, Ottawa, The Canadian Centre for Intelligence and Security Studies.
18. Ford, C.A. (1997); *Symposium: Constitution-Making in South Africa: Symposium Article: Watching the Watchdog: Security Oversight Law in the New South Africa*, Michigan Journal of Race & law, vol.3 (59).
19. Gainor, R., & Bouthillier, F. (2014). *Competitive intelligence insights for intelligence measurement.* International Journal of Intelligence and Counter Intelligence, *27*(3), 590-603.

20. Germany, Act of 11 April 1978 (Federal Law Gazette I. p. 453), last amended by a law of 26 June 2001, Federal Law Gazette I. pp. 1254, 1260.
21. Giupponi, T & Fabbrini, F. (2010). *Intelligence Agencies and the State Secret privilege: The Italian Experience,* ICL Journal, Vol. 4(3), pp. 443-466.
22. Heyer, C. (2007). *Parliamentary Oversight of Intelligence: The German approach,* in: Tsang, S. (editor), *Intelligence and Human Rights in the era of Global Terrorism*, Praeger Security International, Westport, Connecticut, London, pp. 67-77.
23. House of Peoples Representatives [HPR] (2018). *Standing Committees of the Fifth Parliamentary Term: 2015-2020*. Retrieved from http://www.hopr.gov.et/web/guest/committee. [last accessed on 20 August 2018].
24. Hughbank, R.J. & Githens, D. (2010). *Intelligence and Its Role in Protecting Against Terrorism.* Journal of Strategic Security, Vol. 3(1), pp. 31-38.
25. Johnson, L.K, (2007). *Intelligence oversight in the United States*; in Tsang, S. (editor), *Intelligence Intelligence and Human Rights in the Era of Global Terrorism*, Praeger Security International, Westport, Connecticut • London, pp. 54-66.
26. Johnson, L.K. (edi.) (2010). *National Security Intelligence*, the Oxford Handbook of National Security Intelligence, Oxford University Press, Oxford.
27. Lonsdale, D. J. (2012). *Intelligence reform: adapting to the changing security environment.* Comparative Strategy, *31*(5), 430-442.
28. Morrison, J.N.L. (2007). *Political Supervision of Intelligence Services in the United Kingdom,* in: Tsang, S. (editor), *Intelligence and Human Rights in the era of Global Terrorism*, Praeger Security International, Westport, Connecticut, London, pp. 41-53.
29. Nathan, L. (2010), Intelligence Bound: *The South African Constitution and Intelligence Services*, International Affairs, 86(1), pp. 195-210.
30. Omand, D. (2010). *Securing the State (Intelligence and Security)*, Oxford University Press, New York.
31. Parliament of Australia. (2017). *Oversight of intelligence agencies: a comparison of the 'Five Eyes' nations.* Research Paper Series 2017/18, Parliamentary Library. Retrieved from http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/5689436/upload_binary/5689436.pdf. [last accessed on 15 August, 2018].

32. Rebugio, AB. (2013). *Bias and Perception: How it Affects Our Judgment in Decision Making and Analysis,* Small Wars Journal. Available at: http://smallwarsjournal.com/jrnl/art/bias-and-perception-how-it-affects-our-judgment-in-decision-making-and-analysis. [last accessed 11 June 2018].
33. Scheppele, K. L. (2010). *The International Standardization of National Security Law***,** Journal of National Security Law. & Policy, 4 (2).
34. Selth, A. (2009). *Known knowns and known unknowns: measuring Myanmar's military capabilities.* Contemporary Southeast Asia: A Journal of International and Strategic Affairs, *31*(2), 272-295.
35. Svendsen, Adam D. M. (2012). *Understanding the Globalisation of Intelligence,* Basingstoke, Palgrave Macmillan. Johnson, L. K. (2010). *National Security Intelligence*: In *The Oxford Handbook of National Security Intelligence*. Oxford University Press, Oxford.
36. The East African News, *Several deaths in blast at Ethiopian Prime Minister Rally*, Saturday, June 23. 2018. Retrieved from http://www.theeastafrican.co.ke/news/ea/Blast-Ethiopia-Prime-Minister-rally/4552908-4627022-26u2k7z/index.html. [last accessed 10 August 18].
37. The Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights. (2009). *Assessing Damage, Urging Action*, International Commission of Jurists, Geneva.
38. U.S. Office of the Director of National Intelligence [ODNI]. (n.d.). *Members of the Intelligence Community (IC).* Retrieved from https://www.dni.gov/index.php/what-we-do/members-of-the-ic. [last accessed on 11 June 2018].
39. UK Intelligence and Security Committee [ISC]. (2017). *Providing Parliamentary Oversight of the SIS, GCHQ, and the Security Service: Annual Report 2016/17*. Retrieved from https://fas.org/irp/world/uk/index.html. [last accessed 10 June 2018].
40. Vervaele, J. (2005) *Terrorism and Information Sharing Between Intelligence and Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law?*', *Utrecht Law Review,* Vol. 1 (1), pp. 1-27.
41. Voorhout, V. J.E.B.C. (2005). *Intelligence as Legal Evidence, Comparative Criminal Research into the viability of the proposed Dutch Scheme of Shielded Intelligence Witnesses in England and Wales, and legislative compliance with Article 6(3) ECHR, Utrecht Law Review*, Vol. 2 (2), pp. 119-144.

42. Wetzling, T. (2016). *The Key to Intelligence Reform in Germany: Strengthening the G 10-Commission's Role to Authorise Intelligence Surveillance*, Policy Brief, Stiftung Neue Verantwortung.
43. Wetzling, T. (2017). *Germany's Intelligence Reform: More Surveillance, Modest Restraints, and Inefficient Controls*, Policy Brief, Think Tank at the Intersection of Technology and Society, Stiftung Neue Verantwortung.
44. Wodage, W. Y. (2010). *Presumption of Innocence and the Requirement of Proof Beyond Reasonable Doubt: Reflections on Meaning, Scope and their Place under Ethiopian Law*. Ethiopian Human Rights Law Series, Volume 3.
45. Zaveršnik, A. (2013). *Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?* Journal of Contemporary European Research, 9 (1), pp. 181-202.
46. Zemichael, H. A. (2014). *The Standard of Proof in Criminal Proceedings: The Threshold to Prove Guilt under Ethiopian Law*, Mizan Law review, 8 (1), 84-116.