Intelligence-led Policing and Counterterrorism in Bangladesh
Understanding the Experience of Bangladesh Police

Niloy Ranjan Biswas and RM Faizur Rahman[1]

Abstract
This article examines the concepts of intelligence-led policing (ILP) and its applications in counterterrorism. Considering Bangladesh as a critical case, the paper discusses whether and how the police have adopted ILP in addressing the threats of terrorism and radicalization leading to violent extremism. The central research question for this study is—how Bangladesh Police has adopted and implemented intelligence-led policing in countering and preventing terrorist threats and violent extremism. What are the challenges and opportunities in this regard? The study adopts qualitative approaches by—(a) analyzing primary documents, such as global and domestic legal and institutional frameworks, and (b) conducting expert interviews with critical individuals from police and other concerned stakeholders. The article demonstrates that counter-terrorism agencies have launched successful operations to counter terrorist organizations and individuals; nevertheless, they often suffer from the deficiency of evidence-based knowledge to fight extremist views, ideas and narratives. It also suggests that CT agencies should sufficiently be equipped and coordinated to mobilize the approaches of ILP and, hence, contribute to the national P/CVE efforts. An effective use of ILP in an intelligence decision-making framework is critical.

1. Introduction

Intelligence and policing in the 21st century are two sides of the same coin in crime prevention, which initiate some forms of covert surveillance systems to gather critical information using various community-centric approaches. A standard definition and the execution of intelligence policing, or intelligence-led policing (ILP), is inconclusive. Furthermore, the functional meaning of ILP may indicate a collaborative enterprise based on improved intelligence operations and community-oriented policing and problem-solving, which some police departments in Western countries have adopted and implemented in recent decades. Intelligence-led Policing (ILP) is one of the new models adopted by many police departments worldwide (Ratcliffe, 2014, p. 2573).

Defining ILP is an evolving and innovative method of decision-making for police officers to fight crimes (James, 2013, p. 1). Studies on criminal intelligence highlight the decision-making part besides the collection of information (Burcher & Whelan, 2018, p. 1). Scholars have labeled ILP as a 'proactive' method of policing in preventing crimes rather than a conventional 'reactive' policing (Innes et al., 2005, p. 41; Innes & Sheptycki, 2004, p. 1, in Burcher & Whelan, 2018, p. 1). Moreover, 'data analysis' and 'information sharing' are core strategies of ILP in preventing serious crimes (Carter & Carter, 2009, p. 310-325, in Carter et al., 2014, p. 4). Therefore, contextualizing the idea of ILP is a critical task in its application.

[1] Niloy Ranjan Biswas (*Ph.D.*) is a Professor at the Department of International Relations, University of Dhaka. Email: niloy@du.ac.bd. RM Faizur Rahman (PPM) is the Superintendent of Police, Chuadanga district, Bangladesh. Email: prozzal@gmail.com. This paper is a shorter version of a comprehensive study report, commissioned by the Counterterrorism and Transnational Crime Unit (CTTC) of DMP, Bangladesh Police, in 2021. The full report was published in Imtiaz Ahmed and Monirul Islam (Eds.), *Preventing Terror Communication in Bangladesh*, Dhaka: Centre for Genocide Studies, DU, 2022. The authors acknowledge the CTTC for their generous support and anonymous reviewers for their comments, and interview participants for their contributions to complete the study.

Historically, Bangladesh Police has relied on the significance of intelligence in the planning process to address law and order issues, community problems, and public order. Information sharing between relevant departments within the police has been part of the core policy and not an *ad hoc* or informal practice. Police departments also increase their strength in translating information into data quality analysis. The political policymakers also exhausted the crux of intelligence significantly. Therefore, the state has invested in developing techniques, training, and expertise for the intelligence infrastructure of the security sector. How has it been implemented in countering contemporary threats of terrorism and radicalization?

The primary research problem of this study is two-fold—conceptual and practical implications of ILP in Bangladesh. In the post-9/11 world, counterterrorism policing across the regions highlighted the need for a coordinated and centralized data system and information sharing to address new forms of international terrorism. Risk identification to counter threats of terrorism is a central part of modern policing. ILP offers better ways to identify potential risks and sources of terrorism and radicalization through data, information gathering, and analysis. This also prepares law-enforcement agencies to assess a significant number of terrorism-related parameters, such as patterns of radicalization, perception of young people, and motives of various extremist factions of the society. Against that backdrop, this paper asks a central question—how does Bangladesh Police contextualize the adoption and implementation of intelligence-led policing to counter terrorist threats and violent extremism? It discusses the challenges and opportunities of adopting intelligence-led policing (ILP) by Bangladesh's state and law-enforcement organizations.

This paper adopted process tracing as a qualitative approach to examine scopes and challenges and how to adopt intelligence-led policing in Bangladesh Police. This is an underexplored area in the study of policing and counterterrorism in Bangladesh. The study has used checklists/guidelines among a purposive sample to conduct in-depth interviews of professionals/practitioners and academics. This study was administered in various departments of the Bangladesh Police covering the Police Headquarters, Special Branch, School of Intelligence, Detective Branch, CTTC, Anti-Terrorism Unit (ATU), Dhaka Metropolitan Police (DMP) and Rapid Action Battalion (RAB). The paper adopted detailed narratives—the story presented in identifying the relational factors of intelligence-led policing (in this case, strategy, training, orientation, and execution of policies) in the concerned sectors of terrorism, radicalization and religio-centric extremism. The discussion aims to produce analytical narratives on how intelligence in policing takes shape, is implemented, and under which conditions in Bangladesh. The process-tracing approach included a triangulation process using primary documents from Bangladesh Police and other CT security agencies and interviews of the key informants, and these were juxtaposed with secondary literature from selected global practices of ILP.

This paper has four sections: introduction, conclusion, and policy recommendations. The first section introduces the background, major research questions, justification, and methodology of this research. Section two presents conceptual debates on ILP and counterterrorism policing from global and local perspectives. Section three is the empirical contribution of this study. First, it conducts a comparative analysis of legal frameworks between Bangladesh and selective international practices. The discussion highlights strategy, technique & technologies, and institutional coordination in ILP. Interview findings from the participants of this study complement and strengthen this comparative analysis. Furthermore, the analysis highlights the decentralization framework of intelligence institutions in Bangladesh. Finally, in the

concluding section, the paper discusses a way forward highlighting a community-based and participatory ILP in Bangladesh.

2. ILP in Counterterrorism: Conceptual and Practical Implications

The concept of ILP can be described as an "underlying philosophy of how intelligence fits into the operations of a law enforcement organisation. ILP suggests strategic integration of intelligence in the organization's overall mission (Carter, 2004, p. 4, in Carter & Carter, 2009, p. 315)." Furthermore, intelligence-led policing is "a collaborative law enforcement approach combining problem-solving policing, information sharing, and police accountability, with enhanced intelligence operations (U.S. Department of Justice, 2009, p. 4)." A collaborative approach means ILP works with different agencies and communities, including local police, other law-enforcement agencies, and security agencies (LeCates, 2018).

Although ILP is a Western idea, intelligence is nothing new for other parts, especially in South Asia. The intelligence culture of South Asian states, such as India, Pakistan, and some East Asian countries, *e.g.,* China, has a deep-rooted connection with its endogenous resources of practice and knowledge on politics, strategy, and intelligence (Liebig, 2017). For example, Kautilya's *Arthashastra* is India's pioneering transcript of intelligence studies (Liebig, 2014, p. 27). In the *Arthashastra*, undercover operational activities, surveillance networks of spies, and intelligence services are addressed in detail (Liebig, 2014, p. 27-31). The *Arthashastra* and the Indian ancient epics Mahabharata and Ramayana address the pertinence of intelligence in their narratives (Liebig, 2017). However, the Eastern states significantly differ from Western intelligence cultures (Liebig, 2017).

Intelligence-led Policing (ILP) originated in the 1990s in the United Kingdom, but it received wide acceptance by law enforcement agencies after the 9/11 terrorist attack (Cichoracki, 2020, p. 2). As a concept or framework, ILP can analyze all forms of crimes. Still, traditionally, ILP is conceived as a customized approach to dealing with terrorism and national security threats (McGarrell et al., 2007, p. 143). In the post-9/11 era, the importance of utilizing intelligence by law-enforcement agencies in counterterrorism increased. For instance, intelligence was influential during investigations in successfully arresting the perpetrators following the London subway and the Madrid train bombings (McGarrell et al., 2007, p. 147).

In recent times, the credibility of ILP has increased by the effective use of intelligence in arresting terrorist suspects in the United States (Florida), Canada, Britain, and Israel (McGarrell et al., 2007, p. 147). However, the pertinence of intelligence in counterterrorism has its limitations reflected in the failure of intelligence in preventing the Madrid terrorist attack in 2004 and the London bombings in 2005 (Gregory, 2005, p. 2). The characteristic of ILP is not focusing on the crime that has occurred but instead focusing on threats (Carter & Phillips, 2013, p. 7). After the 9/11 terrorist attack, many countries felt the urge to form a different intelligence gathering and analysis unit. Due to the destructive costs of terrorist attacks, the prevention of such attacks is the best option. To prevent potential terrorist attacks, intelligence gathering and analysis of terrorist groups, activities, and plans are necessary.

There are different methods of using intelligence in counterterrorism, and ILP is the most comprehensive and accepted one in contemporary times. Since 9/11, ILP has influenced law enforcement agencies worldwide to bring significant changes to organizational structure in building capacity for collecting intelligence, sharing, analyzing, and decision-making (Schaible & Sheffield, 2012, p. 767). For example, after failing to detect the 9/11 terrorist attack in the

US, the Federal Bureau of Investigation (FBI) has gone through a drastic reform, which includes the insertion of more advanced communication information technology and the creation of separate career paths for intelligence analysts (Chalk & Rosenau, 2004, p. 1).

The US 9/11 Commission reported a lack of sharing information among law enforcement agencies and the intelligence communities, which eventually led to the terrorist attacks in the US in 2001 (National Commission on Terrorist Attacks Upon the United States, 2004). From the available data till 2017, after implementing ILP, the United States and the United Kingdom have decreased the number of terrorist attacks (Cichoracki, 2020, p. 42). However, in the same time frame of installing ILP, Canada, Australia, and New Zealand have observed a slight increase in terror attacks compared to the United States and the United Kingdom (Cichoracki, 2020, p. 42). In Germany, ILP is incorporated into the policy-making and strategic planning of the North Rhine-Westphalia State Police. In Sweden, the police department has taken extensive organizational changes to integrate and coordinate ILP at all national strategy and local operation levels. In Serbia, ILP is implemented by the Ministry of Interior to advance law enforcement and fight crime and security threats. Furthermore, a law was passed by Serbia in 2016 to define and instruct on the practice of applying ILP. Based on the Serious and Organized Crime Threat Assessment (SOCTA MNE) in Montenegro, a relevant law enforcement authority sets several national and inter-agency priorities to fight crimes (James, 2017, p. 72-77).

Global scholarship on intelligence-led policing and counterterrorism has highlighted some of the following issues as critical factors in observing the significance of intelligence data in thwarting terrorism and violent extremism threats. These are:

1. The collection of intelligence is a labor-intensive job. In policing, it is often known as a ‘gumshoe’ work to get on top of the threats of violent extremism.
2. Extremism in contemporary times has enormous potential for surprise. Counterintelligence may often pose challenges due to failures on various fronts as the best defense.
3. Terrorism is not a static threat and mainly creates several smokescreens while being applied by a specific group of people, full of fanaticism, deception, and disproportionate use of force.
4. The adaptability of the enemy is a tremendous capacity. They do not surrender permanently; therefore, the war on terror never ends.
5. There is always an ‘eschatological’ (holy grand cause) logic behind religio-centric extremism. This diverts and creates camouflage over the intentions of organized terrorist groups.
6. Over-militarization of intelligence through clandestine actions may often be proved to be wrong.

Furthermore, the scholarship may not have yet investigated various countries longitudinally and horizontally different country cases, particularly countries of the global South. One of the reasons could be the access to classified information in the intelligence and security sector. India and Indonesia are moderately covered. There is a dire need for research on other critical case studies that are susceptible to the threats of terrorism and radicalization leading to violent extremism.

3. Intelligence and Counterterrorism Policing: Bangladesh in Global Legal and Policy Frameworks

Bangladesh has experienced the presence of religio-centric militant groups since the 1990s (Riaz & Parvez, 2018, p. 1). The acts of violent extremism, mainly by the Islamic militants, are not a new phenomenon in Bangladesh (Mostofa, 2020). Since the 1990s, Bangladesh has experienced terrorist incidents intermittently with frequent gaps. However, recently, between 2013 and 2016, there had been a surprising rise in events related to violent extremism in Bangladesh (Parvez, 2019, p. 7). In 2016, the most shocking and brutal terrorist attack occurred in the history of Bangladesh when a group of armed militants attacked the Holey Artisan Bakery in Dhaka's Gulshan area and killed 22 people. Following the Holey Artisan attack, the government of Bangladesh has undertaken a zero-tolerance policy against terrorism and violent extremism. In Bangladesh, with the boosted anti-terrorist operations since the 2016 attack, law-enforcement agencies successfully cut down the number of terrorist incidents in recent years (Parvez, 2019, p. 7). For example, in 2017, law enforcers killed at least 35 suspected militants in around 15 major anti-militancy campaigns in nine districts of Bangladesh (Kalam, 2018).

Bangladesh Police is the flagship civilian law-enforcement agency. It is administered under the Ministry of Home Affairs, GoB. For most people in Bangladesh, the police represent the entry point to the criminal justice system. This has a headquarters based in Dhaka and several branches and units, including the Special Branch (SB), the Criminal Investigation Department (CID), the Armed Police Battalion, training institutions, and range and metropolitan police (including railway police). Bangladesh's intelligence community constitutes eight types of agencies. These are "national security and political control; counterterrorism; defense services; criminal investigation; border security; physical protection; signals intelligence; and financial intelligence (Ashraf, 2020, p. 31)." Although the working area and expertise separate the agencies from each other, however, their works and duties often overlap (Ashraf, 2020, p. 31).

The British colonial practices influenced the origin of intelligence frameworks in Bangladesh (Hussain, 2016, p. 60). For example, in section 23 of the Police Act of 1861, the duties of police officers include "to collect and communicate intelligence affecting the public peace (Government of the People's Republic of Bangladesh [GoB], 1861)." Section 24 of the Police Act says, "It shall be lawful for any police officer to lay any information before a Magistrate, and to apply for a summons, warrant, search-warrant or such other legal process as may by law issue against any person committing an offense (GoB, 1861)."

The significance of intelligence can also be found in the Police Regulations, Bengal, 1943. Article 40 (c) (iii) of the Police Regulations, Bengal, 1943 mentions "the work of the District Intelligence Branch." Article 69 (c) of the Police Regulations, Bengal, 1943 says:

> Superintendents must instruct their subordinates on how to make intelligent use of the Criminal Intelligence Gazette. It should be impressed upon all officers that they must not confine their interest to items concerning their police station, subdivision, or district; and they should be encouraged to send to their Superintendents for communication to the Criminal Investigation Department any information they may acquire on any subject mentioned in the gazette (GoB, 1943).

It further adds in Article 69(e) of PRB that "the Criminal Intelligence Gazette is a confidential document and is not for sale (GoB, 1943)." Article 205 (d) of PRB says, "Officer-in-charge of

Police-stations shall collect and communicate intelligence on all matters of public importance passing in their jurisdictions, even though such matters may have no connection with any criminal offence (GoB, 1943)." Article 295(a) of PRB mentions, "the services of the Criminal Intelligence Bureau of the Criminal Intelligence Criminal Investigation Department shall be utilized as far as possible Bureau for obtaining information regarding particular classes of crime and criminals (GoB, 1943)." Article 377(i) of PRB identifies:

> The collection and communication of intelligence on all matters of public importance is one of the principal duties of the police, and how this duty is performed by an officer in charge of a station will generally be manifested in his general diaries. Officers shall, therefore, endeavour to render their diaries as complete, but at the same time as concise, as possible (GoB, 1943).

Under article 612(a) of PRB, it is determined that "the functions of the Intelligence Branch are to collect and collate information of a political nature (GoB, 1943)." The success of the intelligence relies on sustainable trust between the police and the community members. On this imperative, one's attention may be drawn to the much-maligned colonial provisions incorporated in PRB 33(a) that says, "No police force can work successfully unless it wins the respect and goodwill of the public and secures its cooperation (GoB, 1943)."

Therefore, from the acts mentioned earlier, we can predict that the foundation of intelligence in the law-enforcement community in Bangladesh is deep-rooted in the laws from the colonial period. Additionally, the use of intelligence for counterterrorism purposes has been evolving through the newly enacted laws and established agencies.

The comparative discussion on Bangladesh's and selected countries' counterterrorism-related legal intelligence documents can be framed in three thematic areas: strategies, techniques, and coordination. Based on these four thematic areas, the comparative analysis of counterterrorism intelligence laws of major countries in the world and Bangladesh is discussed below –

3.1. Strategies of Intelligence Agencies in Counterterrorism

The United States has a comprehensive legal framework for counterterrorism intelligence. The significant laws on intelligence in counterterrorism came after the 9/11 terrorist attacks in the US, such as the US Patriot Act of 2001 and the Homeland Security Act of 2002. Another essential intelligence law, the Foreign Intelligence Surveillance Act (FISA), was passed in 1978. Section 201(1) of the Homeland Security Act, 2002 mentions "receiving and analyzing law enforcement information, intelligence, and other information to understand the nature and scope of the terrorist threat to the American homeland and to detect and identify potential threats of terrorism within the United States (United States, 2002)."

Similar to the legal framework of the US on counterterrorism intelligence, the UK has a robust legal framework addressing counterterrorism intelligence. The laws include the Intelligence Services Act of 1994, the Criminal Procedure and Investigations Act of 1996, the UK Terrorism Act of 2000, the UK Counter-Terrorism Act of 2008, and the Counter-Terrorism and Border Security Act of 2019. Section 1(1) of the Intelligence Services Act, 1994 says:

> There shall continue to be a Secret Intelligence Service (in this Act referred to as "the Intelligence Service") under the authority of the Secretary of State, and, subject to subsection (2) below, its functions shall be:
>
> (a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and

(b) to perform other tasks relating to the actions or preferences of such persons (United Kingdom, 1994).

The UK Terrorism Act of 2000 defines terrorist investigation and mentions the duties of police personnel through its articles. Moreover, the UK Counter-Terrorism Act of 2008 highlights information gathering and sharing provisions. Section 19 of the act is about the disclosure and the intelligence services. The recent law passed on counterterrorism in the UK is Counter-Terrorism and Border Security Act, 2019. This newly passed act contains several essential amendments to the previous terrorism acts.

The counterterrorism laws in India include the Terrorist and Disruptive Activities (Prevention) Act, 1987; Prevention of Terrorism Act (POTA), 2002; National Investigation Agency Act, 2008 (NIAA), etc. Terrorist and Disruptive Activities (Prevention) Act, 1987 is an earlier law that addresses the issue of punishment of terrorist offenses, the power of investigating officers and retaining confessions of the criminals. The Prevention of Terrorism Act (POTA), 2002 is another significant counterterrorism law in India. This act addresses terrorism-related issues, such as suggestions for punitive measures and action plans to deal with terrorist activities, organizations, special tribunals, and communication interception in some instances. Another Indian law not directly connected to counterterrorism or intelligence but relevant to the issue is the National Investigation Agency Act, 2008 (NIAA).

Major counterterrorism laws in Bangladesh are the Anti Terrorism Act of 2009 (amendment in 2013), and the Anti Terrorism Unit Act of 2019. Other than these laws, there are different laws like the Money Laundering Prevention Act, 2012; Digital Security Act, 2018; Explosive Substances Act, 1908; Arms Act, 1878; Bangladesh Telecommunication Act, 2001; and Dhaka Metropolitan Police Ordinance, 1976 to facilitate counterterrorism actions in Bangladesh. The Anti Terrorism Rules, 2013 highlight freezing accounts or suspending transactions by the Bangladesh Financial Intelligence Unit (BFIU), prescription, and enlistment of suspicious transactions. It advocates implementing United Nations Security Council Resolutions and proposes the freeze, seizure, attachment, or confiscation of proceeds of terrorism, investigation, and trial procedure (GoB, 2013).

Article 17(6) of Anti Terrorism Act of 2009 (amendment in 2013) states:

> The contact point of the law enforcing agency shall take reasonable measures to prohibit any individual or entities from making any funds, financial assets or economic resources or related services available for the benefit of the individual or entities engaged in or suspected to be engaged in terrorism. The contact point shall immediately bring such matters to the notice of the Focal Point of MOHA (GoB, 2013).

The Anti Terrorism Unit Act, 2019 addresses the issue of counterterrorism and intelligence more elaborately. The sole purpose of this act is to provide a legal framework for counterterrorism activities of the Anti Terrorism Unit. For example, Article 5(5) of the Anti Terrorism Unit Act, 2019 says, "The unit will be operated as an independent and self-sufficient specialized unit based on modern technology and intelligence information (GoB, 2019)." Furthermore, article 6(d) of the Anti Terrorism Unit Act, 2019, guides the activities of the unit, including "extremism and terrorist activity related intelligence information collection, the lawful interception on extremist and terrorist with the help of authority and agency under the existing law and regulations and taking effective initiatives to detect their position and preventing their activities through arresting identified criminals (GoB, 2019)." Additionally, on duties of the unit article 5(h) of the Anti Terrorism Unit Act, 2019 declares that the unit's task will be "to submit yearly terrorist threat assessment report and, if necessary, time to time,

special report to government through regular necessary information collection, analysis, and dissemination to counter terrorist activities (GoB, 2019)."

In comparing the above-mentioned counterterrorism strategies and laws, it can be identified that gaps exist in the domestic intelligence framework in Bangladesh. No single act offers a strategic framework for intelligence collection, processing, and use in decision-making regarding counterterrorism policing. In an interview with the authors, a senior officer of the Bangladesh Police's CT agency observed:

> Many countries adopted anti-terrorism laws in the last decade, and Bangladesh followed suit. The law also provides for other terrorism-related crimes with varying scale of punishment. The offences include membership in criminal organizations, supporting such organizations, conspiracy relating to acts of terrorism, attempts to commit and support such actions, instigating acts of terrorism, and harboring terrorists. However, it does not explicitly signify the role of intelligence in counterterrorism. Moreover, we do not have an internal strategy document for Bangladesh's security agencies to share intelligence on any criminal activities (BP002, personal communication, 2021).

The legal basis of surveillance over encrypted communication of unauthorized groups is absent. Furthermore, the usage of signal intelligence takes place in a grey legal zone without an approved authority of the executive or judiciary. It may weaken the overall procedure of intelligence-led proactive counterterrorism efforts. "The existing CT laws do not support any proactive intel-based operations that can deter any potential threats in the future. We cannot also use legal frameworks to justify using technologies for surveillance," mentioned a mid-level officer from CT agencies in Bangladesh (BP014, personal communication, 2021).

In conversation with the authors, a senior deputy commissioner of CTTC mentioned distinct types of intelligence that are valuable in intelligence-led policing, and these are:

> Human intelligence, signal /tech intelligence, prison-based intelligence, including phone calls, letters, interactions with relatives, foreign intelligence, police liaison officers at the embassies, and financial intelligence. We have to prepare a case-by-case approach to apprehend foreign nationals and gather any intelligence regarding their acts of terrorism that may affect Bangladesh. It is crucial to have explicit legal provisions or a strategy for foreign-based information on terrorism (BP002, personal communication, 2021).

A KII respondent in this study, a former senior decision-maker in the police administration observes that an oversight mechanism is essential in ensuring the transparency and effectiveness of intelligence organizations' activities. The civilian government should continue to exercise its control over the intelligence community. He also reiterated that the significant challenge of intelligence performance in Bangladesh depends on the political regimes' exhaustive use of intelligence for political vis-à-vis national interests (CSExp001, personal communication, 2021). It is noteworthy that the state's highest political office has declared zero tolerance to address the threats of terrorism. It must be reflected through oversight and democratic control over the national intelligence agencies. The Parliamentary Standing Committee on Home Affairs should play more active roles in this regard.

Finally, there is also a gap in retaining and securing information related to the investigation or criminal procedure in Bangladesh's counterterrorism legal framework. In an interview with the authors, a senior-level officer who had served in police headquarters' confidential cell in Dhaka and is now posted in a specialized CT agency mentioned, "Our intelligence practically runs more on a *de-facto* mechanism. We have an SB manual, which is a very comprehensive rulebook. It suggests how to retain and secure classified information. However, this is a

colonial text, requiring modification in various contexts (BP019, personal communication, 2021)." An intelligence strategy for counterterrorism or an overall intelligence strategy to counter organized criminal activities will be an essential requirement to thwart the threats of terrorism in Bangladesh.

3.2. Techniques and Technologies

With the surge of massive amounts of big data in security intelligence, artificial intelligence is dominated by SIGINT with the transformation of technological development and its utilization for multiple purposes. Nevertheless, the criticality of HUMINT is still perceived by Western and Eastern countries; subsequently, it created a hybrid model of intelligence to address the threats of significant crimes.

Bangladesh, however, significantly depends on manual collections through HUMINT. It has introduced SIGINT technologies to address contemporary challenges of transnational organized criminal activities. For example, in an interview for this study, a senior intelligence officer of a CT agency of Bangladesh Police mentioned the intelligence collection methods used by Bangladesh Police: "manual information gathering through direct surveillance, social media surveillance and open-source intelligence (BP001, personal communication, 2021)." He said further that the "suspect is the primary informant (BP001, personal communication, 2021)." Even though technologies are used to collect information, a capable officer needs to exploit the technology in gathering and analyzing the data. The officer also described how a group of skilled officers conducts social media surveillance for intelligence collection to create a complete profile of the suspects' activities. The officers regularly monitor the online movements of the suspect individual and group (BP001, personal communication, 2021).

An experienced officer in investigation and intelligence sectors in CT agencies in Bangladesh observed the hybridity of social media surveillance and said, "We conduct social media surveillance based on three pillars – a) reduced demand, b) reduced content, c) exploit the virtual data (BP002, personal communication, 2021)." He added that "reliability and validity of information are most important, and the intelligence collector and then analyst process the reliability and validity of the information (BP002, personal communication, 2021)."

In the context of Bangladesh, the pertaining question is whether and to what extent the existing framework allows legitimate use of SIGINT through legal discretion. Some of the international experience may help the readers to understand the necessity of legal-institutional support to establish the significance of hybridity in techniques and technologies used in ILP. For example, several sections of the US Patriot Act, 2001, directly indicate the method and technical support of utilizing intelligence for counterterrorism purposes. Section 103 of the Patriot Act, 2001 highlights "increased funding for the technical support centre at the Federal Bureau of Investigation (United States, 2001)." Section 201 of the Patriot Act provides "authority to intercept wire, oral, and electronic communications relating to terrorism (United States, 2001)." Foreign Intelligence Surveillance Act (FISA), 1978 defines and determines foreign intelligence and surveillance techniques and methods. Furthermore, it also describes the court proceeding regarding the authorization, collection, and use of intelligence for law enforcement purposes. Furthermore, section 1804 of FISA talks about the application for court orders for electronic surveillance, where the application submitted by the federal officer has to be approved by the attorney general (United States, 2001).

Section 3(1) of the UK's Intelligence Services Act, 1994, states the functions of the Government Communications Headquarters, "to monitor or interfere with electromagnetic, acoustic, and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and to provide advice and assistance on intelligence gathering (United Kingdom, 1994). To secure relevant information, article 4.1 of the Criminal Procedure and Investigations Act, 1996, suggests, "if material which may be relevant to the investigation consists of information which is not recorded in any form, the officer in charge of an investigation must ensure that it is recorded in a durable or retrievable form (whether in writing, on video or audiotape, or computer disk)."

In India, Section 36 of Chapter V of the Prevention of Terrorism Act (POTA) defines electronic, wire, and oral communication and interception of communication (Republic of India, 2002). Furthermore, section 38(1) of the POTA mentions the application for authorization of interception of wire, electronic or oral communication –

> A police officer not below the rank of Superintendent of Police supervising the investigation of any terrorist act under this Act may submit an application in writing to the Competent Authority for an order authorizing or approving the interception of wire, electronic, or oral communication by the investigating officer when he believes that such interception may provide, or has provided evidence of any offense involving a terrorist act (Republic of India, 2002).

In Bangladesh, the Anti Terrorism Unit Act, 2019 mentions archiving intelligence information by stating, "Police Commissioner or, in case, Police Super, will provide necessary assistance to the unit in collecting and archiving intelligence information (GoB, 2019)." Finally, article 16(2) of the Anti Terrorism Unit Act, 2019 says that "the unit will formulate its own database and archive works related to extremism and terrorist activity (GoB, 2019)."

The Bangladesh Telecommunication Act, 2001, and Telecommunication Amendment, 2006 give an idea about the authority of law enforcement and intelligence agencies to utilize the telecommunication and internet to collect relevant intelligence information on different issues. For example, section 6 of article 55 mentions that "no license under sub-section (1) shall be required in the following cases—(b) installation, operation or use of a radio apparatus by the Ministry of Foreign Affairs or an intelligence agency of the Government to meet its requirement (GoB, 2001; GoB, 2006)."

The legal provisions in Bangladesh advocate training and technical support to law enforcement officials in counterterrorism activities through legal acts.

> SB [Special Branch] headquarters in Dhaka collect intelligence from all over the country and operate by itself; however, at the field level, it has district wise designated offices, DSB. SB HQ receives weekly intelligence reports from these offices. Additionally, some intelligence information comes directly from the Police Headquarters in Dhaka (BP005, personal communication, 2021)."

As a technique, Bangladeshi counterterrorism practitioners collect information as a part of the investigation process. Using terror suspects is one of the techniques that is often used to collect information in the future. A mid-level officer talked about the process of intelligence collection, analysis, operation, and intervention in an interview with the authors. He observes, "finding one suspect and then using him/her in tracking others or gaining the trust of the radical groups online can lead to finding their location, networks, etc. (BP003, personal communication,

2021).” She further added that “devices seized from the suspects and social media accounts of the arrested terrorists are the good sources for gathering intelligence information of the groups and their activities linked with the terrorists (BP003, personal communication, 2021).”

Several respondents of this study highlighted the non-use of information from undisclosed intelligence sources as a piece of admissible evidence in the courts of justice in Bangladesh. The 1872 Evidence Act of Bangladesh deals with this issue. It is suggested that the government reconsider a reform in the Evidence Act or the relevant anti-terrorism laws to accept a credible intelligence source as admissible evidence in the court without compromising the identity. Such reform initiative would further enhance the extensive use of intelligence-led investigation in counterterrorism.

Does intelligence transform into policy? This is an essential perspective of intelligence-led policing. In discussion with the authors, an academic scholar described the importance of intelligence by saying, “intelligence is useful for any policy-making and has a role in every process of decision making. Furthermore, intelligence can be information about location, individual, plan, transnational connection, etc. However, there are differences between actionable intelligence and thwarting intelligence (AE001, personal communication, 2021).”

3.3. Intelligence Coordination

During an interview with the authors, a mid-level office with long work experience in CT agencies pointed out some of the significant challenges of the intelligence agencies in Bangladesh. He observes, “there is a lack of coordination among the intelligence agencies, and there is a credit hunting tendency among the officials at these agencies. Furthermore, wastage of human resources and absence of fusion centre intelligence information in Bangladesh makes it difficult for the intelligence agencies to work efficiently (BP006, personal communication, 2021).”

In the US, section 203 of the Patriot Act gives “authority to share criminal investigative information (United States, 2001).” Furthermore, section 701 of the Patriot Act mentions the “expansion of regional information sharing system to facilitate Federal State-local law enforcement response related to terrorist attacks (United States, 2001).” Finally, Section 908 of the Patriot Act indicates the importance of training for the officials by mentioning the “training of government officials regarding identification and use of foreign intelligence (United States, 2001).”

Section 203 of the Homeland Security Act, 2002 determines the accessibility of the secretary in terms of information and intelligence by saying:

> The Secretary shall have access to all reports, assessments, and analytical information relating to threats of terrorism in the United States and other areas of responsibility described in section 101(b), and to all information concerning infrastructure or other vulnerabilities of the United States to terrorism, whether or not such information has been, that may be collected, possessed, or prepared by an executive agency, except as otherwise directed by the President. The Secretary shall also have access to other information relating to the preceding matters that may be collected, possessed, or prepared by an executive agency, as the President may further provide (United States, 2002).

Other than the UK and the US, the European Union (EU), as a regional organization, also has a counterterrorism strategy that constitutes intelligence sharing among the member states. For example, Directive (EU) 2017/541 of the European Parliament and the Council of 15 March

2017 on combating terrorism. Furthermore, article 24 of the directive focuses on efficient ways of tackling terrorism and of sharing information regarding terrorism among the member states by saying that –

> To combat terrorism effectively, efficient exchange of information considered relevant by the competent authorities for the prevention, detection, investigation or prosecution of terrorist offences between competent authorities and Union agencies is crucial. Member States should ensure that information is exchanged in an effective and timely manner in accordance with national law and the existing Union legal framework, such as Decision 2005/671/JHA, Council Decision 2007/533/JHA (2) and Directive (EU) 2016/681 of the European Parliament and the Council (3). When considering whether to exchange relevant information, national competent authorities should consider the severe threat posed by terrorist offences (European Union, 2017).

In Bangladesh, article 29 of the Anti Terrorism Rules, 2013, focuses on sharing relevant operational information on movement, travel documents, communication, and technology used by the government by stating –

> The Government, under arrangements entered into by the Government of Bangladesh with the Office of the Ombudsperson or any other country or such other arrangements, shall share all relevant information including operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups (GoB, 2013).

On sharing terrorist-related information, article 6(f) of the Anti Terrorism Unit Act, 2019 offers "to tackle extremism and terrorist threat and to find a possible solution to that information has to be exchanged among the national and international agencies according to Inspector General's instruction (GoB, 2019)."

On terrorist financing, Article 24(3) of the Money Laundering Prevention Act, 2012, states, "the Bangladesh Financial Intelligence Unit may, if necessary, spontaneously provide other law enforcement agencies with the information relating to money laundering terrorist financing (GoB, 2012)."

Also, article 24(4) mentions –

> The Bangladesh Financial Intelligence Unit shall provide information relating to money laundering or terrorist financing or any suspicious transactions to the Financial Intelligence Unit of another country based on any contract or agreement entered into with that country under the provisions of this Act and may ask for any such information from any other country (GoB, 2012).

It is evident from the laws mentioned earlier that Bangladesh has some forms of legal guidance on sharing intelligence information among national and international agencies. However, those are limited in capacity. The practices of coordination and information sharing are case-specific and depend on the individual leadership of the particular organization. According to a senior CT practitioner of Dhaka Metropolitan Police (DMP), "Intelligence is shared on a need-to-know basis and sharing intelligence does not always guarantee success. Some intelligence sources are public and open-source; others are police agencies, senior police officials, victims, etc. (BP002, personal communication, 2021)." He added, "Inter and intra-agency conflicts of interest exist, and different agencies work on a similar issue in counterterrorism. When multiple working on a similar issue, there is a lack of proactive sharing; therefore, one hundred percent success is not achieved (BP002, personal communication, 2021)."

3.4. Decentralization of Intelligence Collection and National Policy-making

The decentralized structure of police administration is essential in understanding intelligence navigation from the field to the policymaking desks. The range and metropolitan police are structured into districts, circles, police stations (thanas), and outposts. The Inspector-General of Police (IGP) is the highest-ranking officer. At the district level, the police superintendents oversee the field operations of the police force and liaise with the deputy commissioner. The Ministry of Home Affairs (MoHA) controls police administration and appointments and transfers of all police officers above the rank of superintendent. An inspector in charge of each thana coordinates all kinds of work in the *thana* area.

The Special Branch has a separate headquarters (HQ), which an Additional Inspector General heads. The SB also has district-level offices widely known as DSB. The district Superintendent of Police (SP) has dual mandates – crime and intelligence. In effect, the DSB reports to the SP, who eventually disseminates confidential reports to three distinct customers – the Police HQ and the SB headquarters. A senior mid-level police officer from a district police office discussed SP and DSB in his interview with the authors. He said, "SP has two roles, one to oversee crime and another to deal with intelligence as the head of the DSB.

An important question is whether keeping the DSBs under the reporting authority of SPs in district police administration is a convenient and practical approach. Many respondents highlight that the current practice is the most effective channel to convey critical intelligence data to the policy-making authorities of Bangladesh Police—Police HQ and SB HQ. There is a different opinion from one of the interviews conducted in this study with a mid-level officer of an intelligence agency of the armed forces. In his response, he suggests intelligence collection should be straightforward and less time-consuming in its travel time from the field to the analysts' desk and then to the policy-makers. He means, "Inclusion of SP in the hierarchy may compromise the autonomy of the SB, and the DSB may apply a direct reporting mechanism to SB headquarters (DINT001, personal communication, 2021)."

Three separate interviews with the Superintendents of Police of three districts in this study highlight that keeping DSB under the purview of SPs would ensure seamless coordination between various district-level police and senior police policymakers in Dhaka (BP012, personal communication, 2021; BP015, personal communication, 2021). Moreover, it is complemented by a senior intelligence officer at Dhaka's Special Branch, Counterterrorism Section (CT). DSB, under the direct control of the SP office in a district, may add value to the counterterrorism intelligence community by effectively communicating between the SB CT branch and the Assistant Inspector General (AIG) Confidential office in the Police Headquarters in Dhaka (BP005, personal communication, 2021). Given the evolving dynamics of terrorism and radicalization in Bangladesh, the need for strengthening decentralized intelligence assets, especially at DSBs, and making them well-connected to CTTC agency/ies and CT Section at SB HQ, merits closer scrutiny.

In interviews, respondents have identified the lack of resources and skilled human resources at the district levels, which would be the essential assets to collect, process, analyze and convey intelligence to the decision-making level at the CT agency, SB and Police headquarters. The following table is derived from the interviews with DSB officials, District Intelligence Officers (DIOs) and SPs of the respective districts.

Table 1: Major issues, challenges and way forward from district-level administrations[2]

Topics on intelligence	Current status	Spot on the problem	What can be done?
1. Strategy	SB manual	Need an update on SIGINT & protection and counter-intelligence form	Bangladesh Police may form a committee to modernize the SB manual and propose a national intelligence strategy
2. Human resources	Inadequate	Need more persons, transfer, and posting need to be reconsidered to ensure sustained service in the DSB	A separate and internal HR policy for SB, DSB, and CT agencies' intelligence units
3. Training	Inadequate	Seniors (SPs) receive opportunities for training; it is not always trickled down to the juniors.	Localized opportunities for training need to be introduced.
4. Techniques	HUMINT	Majorly dependent on HUMINT and for technical support, districts depend on HQs	Hybrid models can enhance the capacity of districts' ability of intelligence administration.
5. Technology	N/A	Technological support is highly centralized and at the discretion of the HQs	Some SIGINT tech can be installed in the district headquarters.
6. Intra- Coordination	Good	DSB, DB, Range Police, local police stations, and Metropolitan police	Regular meetings and need-based sharing are required
7. Inter-force Coordination	Inadequate	NSI, DGFI, BGB, and other Intel agencies of security forces	Coordination may need to take place at the central level in Dhaka

In addition to empowering specialized CT agencies' intelligence units, respondents also highlighted the necessity of reforming the SB's CT Section, which can add value to bolstering the counterterrorism efforts of the Bangladesh Police. This would undoubtedly require putting human, electronic, and technical assets at the CT Section and posting well-trained officials at DSB offices. As it is a standard practice that intelligence agencies operate in a primarily compartmentalized culture, the DSB offices must maintain an autonomous reporting system that allows them to disseminate sensitive information only through proper channels to achieve two objectives. First, the intelligence data must reach the analysts' and decision-makers' desks in the shortest possible time and within the required deadline. Second, it must be accurate to the possible extent and should not be transformed into a different context and form while it is conveyed to the decision-makers. It is also essential that terrorism-related intelligence data and analysis be made accessible to any influence or persuasion of other irrelevant stakeholders.

[2] Authors summarized the findings from interviews of district-level respondents in this table.

The role of intelligence officers and analysts at the field level is also discussed in the interviews. The intelligence officers monitor the movement of a suspicious individual through sources and by themselves. They also keep in contact with the essential persons in the area, such as imams, chairmen, and others. They also maintain some community gatekeepers as the source of information. Furthermore, if a new person comes to the area and raises any alarms, they keep them under surveillance (BP009, personal communication, 2021). In another interview with the authors, another district intelligence officer shared the obstacles they faced while performing their duties by saying it is hard to balance crime duty and intelligence duty as there is a shortage of human resources. Then, there is the bare minimum of technological and safety equipment and assistance for doing their job efficiently.

Moreover, there is a lack of budgetary allocation to pay the sources to purchase information and insufficient training for them (BP018, personal communication, 2021). Intelligence is a resource-intensive and skillful activity. Another respondent complements it in an interview with the authors. He observes, "There is a lack of funding in intelligence work, lack of workforce as well as lack of skilled staffing, lack of training for the field level intelligence officers and analysts, lack of technological equipment and knowledge for intelligence officials (BP007, personal communication, 2021).

The discussion in this section elaborates on some critical issues—strategies, techniques, technologies and information sharing—of intelligence-led policing in Bangladesh. In addition, it has deliberated the patterns of decentralization framework of intelligence agencies in Bangladesh Police. An analysis of comparative legal frameworks of selected best country case studies and interview findings from crucial informants in Bangladesh showed. There may be a need for a strategy on intelligence-led counterterrorism. This would incorporate human resources, capacity development, finances, intelligence sharing and coordination, technology use, etc.

4. Concluding Remarks and Policy and Programmatic Recommendations

This paper has contributed to understanding strategy, techniques, and technologies used in a contextualized aspect of intelligence-led policing. The findings have considered the unique features of Bangladesh and its unique experience in countering and preventing violent extremism. Alternative to conventional counterterrorism forces and their approach to addressing threats of terrorism, ILP endorses a bottom-up approach and proactive people-friendly policing. This paper also discussed the experience of particular developed countries that had promoted intelligence-led policing in tackling severe crimes, including violent extremism.

The paper examined the need for an intelligence strategy paper that offers a strategic framework for intelligence collection, processing, and use in decision-making regarding counterterrorism policing. Second, continuous surveillance is a critical necessity for counter-terrorism. The paper finds that the legal basis of surveillance over encrypted communication of unauthorized groups is non-existent. It has hindered the usage of signals intelligence in a vacuum without following any standard approval mechanism of the judiciary. It may have influenced the legality and legitimacy of updated technologies in the intelligence-led proactive counterterrorism effort. Third, findings also expose a cavity in retaining and securing information storage in the existing framework of counterterrorism intelligence. Institutional and legal protection may need to be strengthened to ensure safety and prohibit acts of espionage that harm the intention of counterterrorism.

Based on the empirical observations and suggestions accumulated from the experts and primary and secondary literature analysis, this paper proposes ten-pillar policy recommendations for successfully deploying intelligence-led policing initiatives to counter and prevent violent extremism and radicalization threats.

1. Identify the intention and clarify the problems of terrorism and violent extremism.
   It is essential to know and learn one's community very well to understand the intentions of certain groups in the framework of radicalization and violent extremism and accumulate clear ideas of the problems. The security sector may experience a need to collect better data, with a more profound emphasis on analysis and sharing of information.

2. Adopt result-oriented strategies and tactics to combat threats of extremism.
   Once the problem is identified, the next step is to identify specific outcomes/results that the agencies want to achieve in counterterrorism. Most importantly, the ILP strategies and tailored tactics must effectively combat the threats of extremism. The result has clear indicators which are achievable and subject to evaluation.

3. Follow effective processes of intelligence collection and filtering the data from verified sources.
   A practical Intelligence provides substantive insights about the threats of the crimes, i.e., violent extremism. Big data does not always inherit critical information. Small data, such as information on a single target, often prove helpful and effective.

4. Engage an efficient data analysis process that will produce actionable intelligence.
   Intelligence analysis is a future-centric task. As part of predictive policing, forecasting potential threats with accuracy is required. The idea behind practical intelligence data assessment is to be forward-looking. Actionable intelligence' may be referred to as a set of factual information that will facilitate actionable response (i.e., military, political, or financial) to an identified current threat of violent extremism.

5. Promote collaboration between intelligence and law-and-order agencies.
   ILP depends on active and functional collaboration between intelligence and implementing agencies within the security sector. Addressing contemporary religio-centric extremism—prevention, and reduction—is prospective with a collaborative, coordinated effort. The partnership between agencies can leverage resources to employ joint counterterrorism operations and prevent violent extremism.

6. Train and build the capacity of the police and intelligence officers on ILP.
   Police authorities must employ resources for the continuous capacity building of CT practitioners and concerned intelligence officers. The capacity-building programs can be based on generic and specific issues of violent extremism.

7. Bridge between community and the counterterrorist forces in P/CVE efforts.
   ILP suggests a bridge between community and police organizations. Community policing is an idea that advocates for overt intelligence collection. Utilizing community support will be an essential strategy and a technique here.

8. Ensure long-term commitment of the police leadership in using ILP to counter and prevent terrorism.
   Actionable intelligence must be translated into the decision-making framework to counter and prevent violent extremism. A sustainable ILP initiative is dependent on the support of the police leadership. It must be an inherent part of the holistic strategy document of the Bangladesh Police.

9. Continuous assessment and ensure adaptability with the changes in ILP-based CT policing. The CT practitioners should be able to accommodate adaptability with the changes proposed by the continuous evaluation of the strategies and techniques in ILP for counterterrorism. It is essential for the ILP programs not to become stagnant; the constantly evolving ILP approach must appreciate new measures.

10. Legal review of counterterrorism laws to facilitate ILP.
    The government and security agencies in Bangladesh shall generate a consensus to reform necessary changes in the counterterrorism and criminal justice legal frameworks to facilitate an adequate functioning of ILP.

References

Books and Journals

Ashraf, A. S. M. A. (2020). Bangladesh. In B. de Graaff (Ed.), *Intelligence Communities & Cultures in Asia & the Middle East: A Comprehensive Reference* (pp. 25-48). Colorado, USA: Lynne Rienner Publishers, Inc.

Burcher, M., & Whelan, C. (2018). Intelligence-Led Policing in Practice: Reflections from Intelligence Analysts. *Police Quarterly* 22(2), 1. https://doi.org/10.1177%2F1098611118796890.

Carter, D. L., & Carter, J. G. (2014). Intelligence-led policing: Conceptual considerations for public policy. *Criminal Justice Policy Review* 20(3), 310-325. Quoted in J. G. Carter, S. W. Phillips, & S. M. Gayadeen, Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory. *Journal of Criminal Justice* 42(6), 4. https://doi.org/10.1016/j.jcrimjus.2014.08.002.

Carter, D. L. (2004). *Law enforcement intelligence: A guide for state, local and tribal law enforcement agencies.* Michigan: Michigan State University. http://www.intellprogram.msu.edu.

Carter, J. G., & Phillips, S. W. (2013). Intelligence-Led Policing and Forces of Organizational Change in the United States. *Policing and Society* 25(4), 7. https://doi.org/10.1080/10439463.2013.865738.

Chalk, P., & Rosenau, W. (Eds.). (2004). *Confronting the "Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies.* Santa Monica, CA: RAND Corporation.

Gregory, F. (2005). *Intelligence-led Counter-terrorism: A Brief Analysis of the UK Domestic Intelligence System's Response to 9/11 and the Implications of the London Bombings of 7 July 2005.* Madrid: Real Instituto Elcano. https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/lectures/gchq/2002june/gregory781-v.pdf.

Hussain, M. S. (2016). Role of Intelligence in National Security: A Bangladesh Perspective. In A. S. M. A. Ashraf (Ed.), *Intelligence, National Security, and Foreign Policy: A South Asian Narrative* (pp. 55-64). Dhaka: Bangladesh Institute of Law and International Affairs (BILIA).

Innes, M., Fielding, N., & Cope, N. (2005). The appliance of science? The theory and practice of crime intelligence analysis. *British Journal of Criminology* 45(1), 41.

Innes, M., & Sheptycki, J. W. E. (2004). From detection to disruption: Intelligence and the changing logic of police crime control in the United Kingdom. *International Criminal Justice Review* 14(1), 1. Quoted in M. Burcher, & C. Whelan, Intelligence-Led Policing in Practice: Reflections From Intelligence Analysts. *Police Quarterly* 22(2), 1. https://doi.org/10.1177%2F1098611118796890.

James, A. (2013). *Examining Intelligence-Led Policing*. London: Palgrave Macmillan.

James, A. (2017). *Guidebook on Intelligence-Led Policing.* Vienna: OSCE. https://www.researchgate.net/publication/318661364_Guidebook_on_Intelligence_Led_Policing.

LeCates, R. (2018, October 17). Intelligence-led Policing: Changing the Face of Crime Prevention. *Police Chief Magazine*. https://www.policechiefmagazine.org/changing-the-face-crime-prevention/.

Liebig, M. (2014). Statecraft and Intelligence Analysis in the Kautilya-Arthashastra. *Journal of Defence Studies* 8(4), 27. http://idsa.in/jds/8_4_2014_StatecraftandIntelligenceAnalysis.html.

McGarrell, E. F., Freilich, J. D., & Chermak, S. (2007). Intelligence-Led Policing as a Framework for Responding to Terrorism. *Journal of Contemporary Criminal Justice* 23(2), 142–58. https://doi.org/10.1177/1043986207301363.

Parvez, S. (2019). Recent Trends and Patterns of Violent Extremism in Bangladesh: Variations and Responses. CGS-UNDP Papers: 1. Centre for Genocide Studies (CGS), University of Dhaka, Dhaka.

Ratcliffe, J. (2014). *Intelligence-Led Policing*. Philadephia: Academia. https://www.academia.edu/26606549/Intelligence_Led_Policing.

Riaz, A., & Parvez, S. (2018). Bangladeshi Militants: What Do We Know? *Terrorism and Political Violence* 30(6), 01-02. https://doi.org/10.1080/09546553.2018.1481312.

Schaible, L. M., & Sheffield, J. (2012). Intelligence-led policing and change in state law enforcement agencies. *Policing: An International Journal of Police Strategies & Management* 35(4), 767. https://doi.org/10.1108/13639511211275643.

Primary Documents

Cichoracki, C. (2020). *The Effectiveness of Intelligence Led Policing in Countering Terrorism on Global, National, Local, & Cyber Fronts* [Master's Thesis, Johns Hopkins University].

European Union. (2017). *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.*

Government of the People's Republic of Bangladesh, Bangladesh Parliament. (2001). *The Bangladesh Telecommunication Act, 2001* (Act No. 18 of 2001).

Government of the People's Republic of Bangladesh, Bangladesh Parliament. (2006). *Telecommunication Amendment, 2006* (Act No. 7 of 2006).

Government of the People's Republic of Bangladesh, Bangladesh Parliament. (2018). *Digital Security Act, 2018* (Act No. 46 of 2018).

Government of the People's Republic of Bangladesh, Bangladesh Police. (2019). *Anti Terrorism Unit Act, 2019.*

Government of the People's Republic of Bangladesh, Law, Justice and Parliamentary Affairs. (2012). *Money Laundering Prevention Act, 2012* (Act No. 5 of 2012).

Government of the People's Republic of Bangladesh, Ministry of Home Affairs. (2009). *Anti Terrorism Act, 2013* (Act No. XVI of 2009).

Government of the People's Republic of Bangladesh. (1861). *The Police Act, 1861* (Act No. V of 1861).

Government of the People's Republic of Bangladesh. (1943). *Police Regulations, Bengal, 1943* (Act No. V of 1861).

Liebig, M. (2017). Intelligence Culture in South Asia. MA Seminar: SS 2017. Department of Political Science, South Asia Institute, Heidelberg University, Heidelberg.

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission Report*. Washington, D. C.: The National Commission on Terrorist Attacks Upon the United States. https://govinfo.library.unt.edu/911/report/index.htm.

Republic of India. (2002). *Prevention of Terrorism Act (POTA), 2002* (Act No. 15 of 2002).
U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance. (2009). *Navigating Your Agency's Path to Intelligence-Led Policing.* Washington, DC: Global Justice Information Sharing Initiative.

https://it.ojp.gov/documents/d/Navigating%20Your%20Agency%27s%20Path%20to%20Intelligence-Led%20Policing.pdf.

United Kingdom of Great Britain and Northern Ireland. (1994). *Intelligence Services Act, 1994.*

United Kingdom of Great Britain and Northern Ireland, Ministry of Justice. (1996). *Criminal Procedure and Investigations Act, 1996* (section 23(1)).

United Kingdom of Great Britain and Northern Ireland. (2008). *UK Counter-Terrorism Act, 2008* (Chapter 28).

United States, United States Code. (1978). *Foreign Intelligence Surveillance Act (FISA), 1978.*

United States, United States Congress. (2001). *The US Patriot Act, 2001* (Public Law 107–56, 107th Congress).

United States, United States Congress. (2002). *Homeland Security Act, 2002.*

Newspaper/Media

Kalam, Z. (2018, January 3). Interactive: Bangladesh's fight against militancy gained new grounds in 2017. *The Daily Star*. https://www.thedailystar.net/onlinespecial/bangladesh-fight-against-militancy-terrorism-new-grounds-islamic-state-dhaka-attack-2017-1514293.html.

Mostofa, S. M. (2020, June 4). What Does COVID-19 Mean for Terrorism in Bangladesh? How the pandemic intersects with challenges of Islamist radicalisation for Bangladesh. *The Diplomat*. https://thediplomat.com/2020/06/what-does-covid-19-mean-for-terrorism-in-bangladesh/.

Interviews

AE001, an academic scholar on intelligence & security affairs from University of Dhaka, in an interview with the authors, Dhaka, February 14, 2021.

BP001, a senior intelligence officer (deputy commissioner) of a CT agency of Bangladesh Police, in discussion with the author, Dhaka, February 4, 2021.

BP002, a deputy commissioner of investigation of a CT agency of Bangladesh Police, in an interview with the authors, Dhaka, February 4, 2021.

BP003, a mid-level additional deputy commissioner on intelligence and investigation of a CT agency of Bangladesh Police) in an interview with the authors, Dhaka, February 8, 2021.

BP005, a special superintendent of Special Branch, Bangladesh Police, in an interview with the authors, Dhaka, February 10, 2021.

BP006, a mid-level officer from a CT agency of Bangladesh Police, in an interview with the authors, Dhaka, February 15, 2021.

BP007, a mid-level officer (additional police superintendent), in charge of district special branch-DSB, Rajshahi District Police, Bangladesh Police, in an interview with the authors, Rajshahi, March 6, 2021.

BP009, interview with a Sub-inspector intelligence officer, Rajshahi, March 6, 2021.

BP014, a mid-level officer of a CT agency of Bangladesh Police, in an interview with the authors, Dhaka, April 7, 2021.

BP012, BP015, key decision-making police officials in Sylhet and Cox's Bazar districts, in an interview with the authors, Sylhet, April 9, 2021, and Cox, Bazar, February 27, 2021.

BP018, Interview with a Sub-inspector intelligence officer, Cox's Bazar, February 27, 2021.

BP019, a senior deputy inspector general of a CT agency of Bangladesh Police, in discussion with the author, Dhaka, April 26, 2021.

CSExp001, a member of the civil society and a former IGP of Bangladesh Police, in an interview with the authors, Dhaka, July 26, 2021.

DINT001, a Defense Forces Intelligence Official [Analyst and Investigator], in an interview with the authors, Dhaka, April 11, 2021.