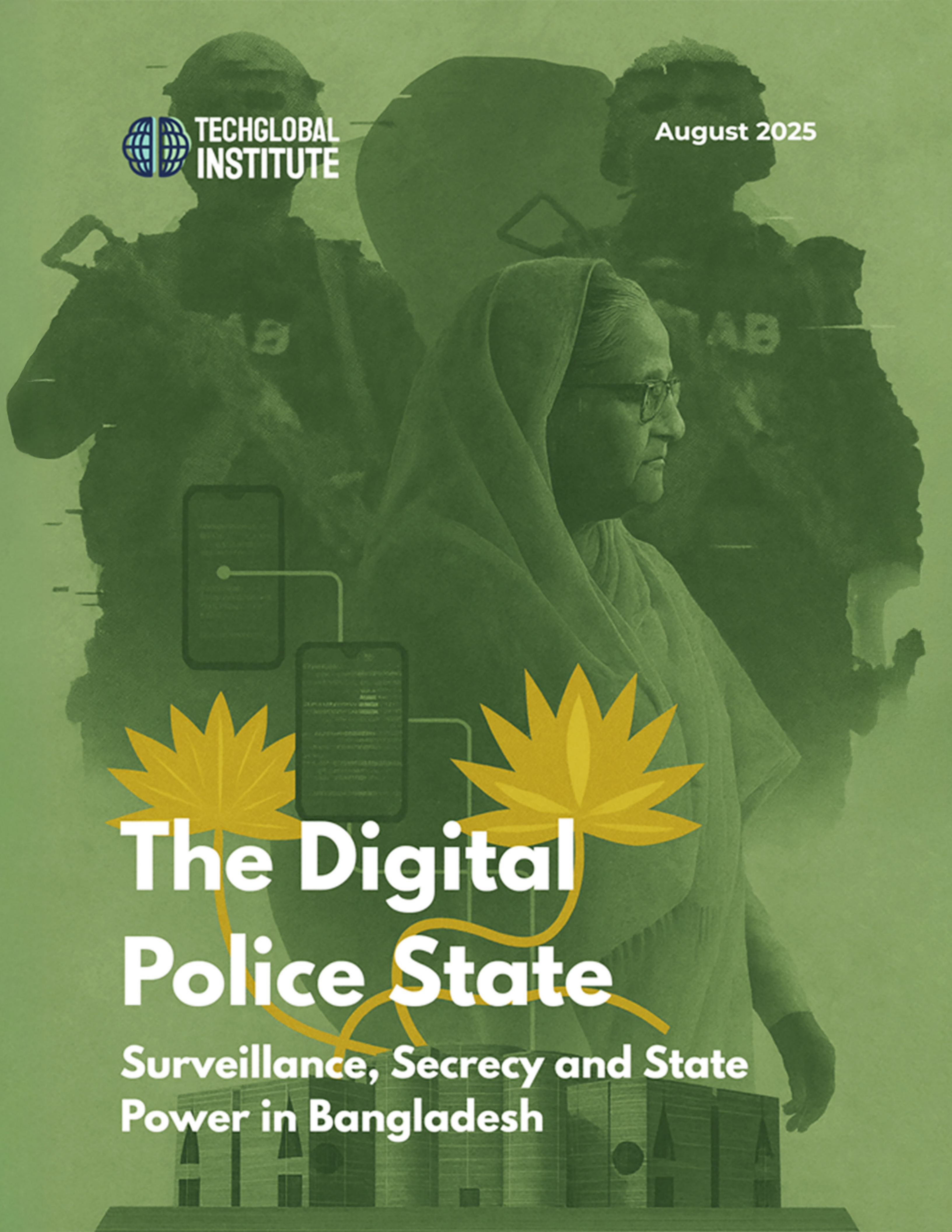


TECHGLOBAL
INSTITUTE

August 2025

The Digital Police State

Surveillance, Secrecy and State Power in Bangladesh

ACKNOWLEDGEMENT

This research publication is the result of over a year of dedicated investigations by a global team of researchers, human rights lawyers, and open-source analysts. Despite significant personal and professional risks, they worked tirelessly to collect, verify, and analyze publicly available records. While the list of findings may not be exhaustive, the team made every effort to ensure accuracy and integrity. For security reasons, their identities have been withheld. Tech Global Institute expresses deep gratitude for their courage, commitment, and vital contributions to advancing the understanding of the development and use of surveillance and spyware in Bangladesh and across the Global Majority.

The Digital Police State

Surveillance, Secrecy and State Power in Bangladesh

TABLE OF CONTENT

SUMMARY

Bangladesh's surveillance system, rooted in colonial-era policing traditions and strengthened by post-independence military intelligence priorities, has transformed significantly over the past two decades. It has evolved from rudimentary physical monitoring to a sophisticated, cyber-enabled network capable of real-time interception, metadata analysis, remote eavesdropping, and content filtering. This transition accelerated under the pretext of counterterrorism, especially following the 9/11 terrorist attack in the United States and 2016 Holey Artisan Bakery attack in Bangladesh. However, the report finds that cyber surveillance has increasingly been used to target political opposition, journalists, activists, and ordinary citizens, particularly during electoral cycles and mass protests.

In this report, we investigate the evolution, architecture and implications of Bangladesh's surveillance apparatus, revealing a system that has expanded over the years with limited transparency, oversight, or accountability. Drawing on public records, investigative reports, procurement and trade documents, and semi-structured interviews on background, the study traces the historical, political, technological, and legal contours of its expanding cyber monitoring regime, and maps how invasive surveillance technologies—often acquired from foreign vendors operating in legal grey zones—have been systematically embedded into the country's security, political, and governance frameworks.

A central finding of this investigation is that at least 160 surveillance technologies and other spyware systems were imported into and/or deployed in Bangladesh between 2015 and 2025, often via opaque procurement processes and third-country intermediaries. These tools range from IMSI catchers and Wi-Fi interceptors to spyware like Pegasus, FinFisher and Predator, enabling expansive, often warrantless state-sanctioned surveillance. The investigation identifies the origin countries of known suppliers and finds that companies registered in France, Germany, the United States, Canada, the United Kingdom, and others, sold surveillance technologies and spyware to the former Bangladeshi government, despite its record of serious human rights abuses. Critically, the report documents how Israeli-origin technologies, such as Cellebrite UFED and spyware from NSO Group and Intellexa, were routed through Cyprus, Singapore, and Hungary to circumvent formal trade restrictions, raising ethical and legal concerns about global surveillance exports.

Between 2015 and 2025, it is estimated that Bangladesh spent nearly USD 190 million on surveillance and spyware, including at least USD 40 million on Israeli-origin technologies, majority of which have reportedly been used in other authoritarian regimes worldwide. Purchases rose sharply before or just after national elections in 2018 and 2024, indicating these technologies were likely used to suppress political and civic opposition, and maintain regime continuity.

The investigation finds the National Telecommunications Monitoring Center (NTMC) alone appears to have spent over USD 100 million on surveillance technologies, including deep packet inspection (DPI) and decryption platforms to intercept internet traffic, and spyware to filter content and extract data. Meanwhile, the Information and Communication Technology Division's BGD e-GOV CIRT, has invested heavily on spyware for social media, messaging and web content interception and analyses. These figures are likely underestimated due to the absence of comprehensive public records and documentation on surveillance procurement. Nonetheless, together, these investments point to a coordinated expansion of the state's capacity to monitor and control digital communications.

The analysis further identifies a web of domestic laws that either explicitly authorize or indirectly facilitate surveillance. It also demonstrates how law enforcement and intelligence agencies—many of which are established and empowered through non-public executive orders and operate within opaque, black-box structures—carry out extensive surveillance in the absence of explicit legal mandates and in violation of constitutional safeguards. Despite the breadth of these practices, there is no specialized parliamentary committee to oversee intelligence operations, minimal judicial engagement with surveillance-related constitutional questions, and an absence of meaningful procedural guardrails. These gaps are further compounded by official secrecy laws and broad national security exemptions embedded across multiple legal frameworks, which collectively shield surveillance practices from both public scrutiny and institutional accountability.

The report also details the political and institutional drivers behind the expansion of surveillance, linking its use to regime preservation, the suppression of dissent, and control over civic and digital spaces. Surveillance tools have been widely adopted across policing, intelligence, government, and military institutions—ostensibly under the mandates of counterterrorism, cybersecurity, or public order—but are frequently deployed to monitor dissent and journalism.

Although elements of these findings have been previously reported by media and research groups, there has been little effort to systematically or specifically address the purchase and deployment of surveillance and spyware in Bangladesh. Despite a change in government, it is unclear whether, and to what extent, surveillance and spyware continue to be purchased and used in Bangladesh. Contrarily, government records show that the Rapid Action Battalion (RAB) acquired vehicular mobile interception devices, and its officers were authorized for training in mobile and Wi-Fi interception, including use during large gatherings and protests as recently as February 2025.

To address these systemic concerns, the report presents a series of legal and institutional recommendations aimed at establishing constitutional limits on surveillance, enhancing transparency, ensuring independent oversight, and aligning Bangladesh's practices with international human rights standards. With elections approaching, and given the precedent of using surveillance technologies to suppress political opposition or intimidate voters, urgent action is needed to prevent their disproportionate use against citizens.

Without such meaningful reform, the country risks further entrenching a model of digital authoritarianism, where surveillance operates not in service of public interest or security, but as a tool of unchecked state power and political control.

INTRODUCTION

Over the past few decades, cyberspace has drastically transformed the modalities of state surveillance, enabling more pervasive and opaque forms of data collection, interception, and monitoring. Bangladesh, amid rapid technological modernization and expanding security infrastructure, has increasingly integrated cyber surveillance into its systems of governance. This evolution reflects not only domestic priorities of counterterrorism and regime stability, but also the influence of transnational security agendas, international intelligence cooperation, and the global surveillance trade.

Cyber surveillance—defined as the systematic monitoring, interception, collection, and retention of digital communications and data across communication networks—raises profound concerns for privacy, civil liberties, and democratic accountability.[1] In the Bangladeshi context, these concerns are magnified by the deployment of surveillance tools and known spyware beyond conventional security contexts, including their use for political control, suppression of dissent, and curtailment of fundamental rights.

While surveillance and spyware both involve monitoring and intercepting communication, they differ in their intent. Surveillance, in itself, can be a legitimate act of monitoring specific targets, often for security and law enforcement purposes. On the other hand, spyware is malicious software installed on an individual's device without their consent or knowledge for the purpose of stealing their information. The boundary between surveillance and spyware is increasingly blurred, as surveillance today often extends beyond narrowly defined targets. Instead of focusing on individuals under specific suspicion, modern surveillance systems now rely on spyware to enhance broad monitoring and interception capabilities.[2] For clarity, this report uses the term cyber surveillance to encompass both spyware and other forms of malicious surveillance technologies.

While theoretical frameworks such as Foucault's panopticism offer useful insights into the underlying power structures enabled by cyber surveillance,[3] international human rights law—particularly the International veillance architecture operates largely beyond these legal boundaries, entrenched in executive secrecy, colonial-era laws, and institutional opacity.[4]

Analyses of public procurement records, international trade data, legal texts, and journalistic and open-source investigations reveal that Bangladesh's cyber surveillance capabilities have significantly expanded through the acquisition of advanced technologies by an intricate network of state and corporate actors. These systems are often procured from international vendors via opaque or indirect channels. Many of these acquisitions originate from countries with

[1] United Nations Human Rights Council. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (UN Doc. A/HRC/23/40). <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf>; Watt, E. (2017). Cyberspace, surveillance, law and privacy [Doctoral Dissertation, University of Westminster]. WestminsterResearch. <https://westminsterresearch.wmin.ac.uk/>.

[2] Klang, M. (2009). Spyware. In Handbook of Research on Technoethics (pp. 593-608). IGI Global.

[3] Sheikh, N., & Askari, M. U. (2021). Foucauldian Panopticon: A model for U.S. cyber surveillance. Journal of Political Studies, 28(1), 193–211. <https://doi.org/10.46568/jps.v28i1.44>.

[4] Mahapatra, S. (2021). Digital surveillance and the threat to civil liberties in India (GIGA Focus Asien, 3). German Institute for Global and Area Studies. <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-73130-3>; att, E. (2017). Cyberspace, surveillance, law and privacy [Doctoral Dissertation, University of Westminster]. WestminsterResearch. <https://westminsterresearch.wmin.ac.uk/>.

troubling human rights records, raising urgent questions about the ethics and accountability of the global surveillance and spyware trade.

Against this backdrop, this report critically examines Bangladesh's cyber surveillance landscape by mapping the historical and political contexts, identifying the actors involved, tracking the technologies procured and their uses, and assessing the human rights implications of these practices. It demonstrates how surveillance has become a central instrument of statecraft, often at the expense of constitutional safeguards, democratic oversight, and individual freedoms. Finally, the report offers policy recommendations for aligning Bangladesh's surveillance practices with its domestic constitutional framework and international human rights obligations. These include proposals for legal reform, institutional accountability, and enhanced transparency in surveillance-related procurement and deployment. By foregrounding the tension between national security and civil liberties, this report aims to contribute to broader debates around digital authoritarianism and the regulation of surveillance technologies and spyware in Bangladesh.

This research is guided by the following questions:

What cyber surveillance tools and technologies have been deployed by the Bangladeshi government?

To what extent do Bangladesh's existing legal and institutional frameworks regulate—or fail to regulate—the use of these surveillance capabilities?

How are these surveillance tools and technologies used for political purposes?

What are the implications of these surveillance tools and technologies on constitutional rights, especially the right to privacy and freedom of expression?

BACKGROUND

Surveillance in Bangladesh has evolved from colonial-era human-led intelligence gathering practices into a centralized cyber infrastructure shaped by authoritarian politics, internal security failures, and global counterterrorism agendas. Originally rooted in postcolonial statecraft and the securitization of militancy, cyber surveillance in recent decades has become a principal instrument of political control—reinforced by legislative reforms, classified budgets, and deepening cooperation with regional and international intelligence actors. Especially under successive Bangladesh Awami League (AL) governments, more advanced forms of surveillance tools and spyware have been deployed against dissenters, activists, and opposition parties, normalizing digital authoritarianism under the guise of national security and modernization.

Surveillance as a Tool of Statecraft

Surveillance in Bangladesh traces its origins to the colonial policing apparatus of British India, where intelligence was collected primarily for safeguarding imperial interests and suppressing dissent. Agencies like the Special Branch (SB), established in the late nineteenth century and currently the oldest intelligence unit in the country, continued after independence with a sustained focus on political intelligence.[5] Similarly, after the 1971 Liberation War, new agencies such as the Directorate General of Forces Intelligence (DGFI) and National Security Intelligence (NSI) were established, and over time, their mandates expanded to include domestic and foreign intelligence, political monitoring, counterintelligence, and counterterrorism. Today, the National Telecommunication Monitoring Centre (NTMC) represents the technological core of this apparatus. It operates sophisticated cyber surveillance equipment and software reportedly obtained from Israeli and other foreign companies, and integrates other security apparatuses including the DGFI, NSI, Bangladesh Police, and Rapid Action Battalion (RAB), granting them extensive and largely unchecked access to surveillance and spyware data.[6]

Despite popular resistance to British and later Pakistani authoritarian rule—both of which relied on invasive intelligence practices to subjugate citizens and suppress democratic movements—the intelligence culture of the postcolonial state retained its colonial logic. Rather than dismantle it, Bangladesh adapted and expanded it, institutionalizing surveillance into the very architecture of the new state. Surveillance remains a central instrument of statecraft, prioritizing regime stability and the consolidation of state power over public accountability, individual rights, public safety, the rule of law, and democratic oversight. In doing so, it reproduced the colonial logic that treated the population as a subject to be monitored and managed, rather than as a citizenry to be respected and represented. This continuity enabled the practices of domination once employed in service of the empire to be retooled in service of postcolonial Bangladesh.

Surveillance in Response to Security Failures and the Global Securitization of Militancy

Although Bangladesh's surveillance apparatus evolved incrementally in response to shifting ideological orientations, political imperatives, and technological change, its current emphasis on counterterrorism and crime prevention is shaped by two interrelated developments: recurring internal

[5] Ashraf ,A .A .(2022) .Bangladesh :Intelligence Culture and Reform Priorities .In R .Shaffer) Ed ,(.*The Handbook of Asian Intelligence Cultures* .Rowman & Littlefield Publishers.

[6] Office of the United Nations High Commissioner for Human Rights. (2025). Fact-Finding Report on Human Rights Violations and Abuses related to the Protests of July and August 2024 in Bangladesh. <https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/ohchr-fftb-hr-violations-bd.pdf>.

security failures and the global shift toward the securitization of militancy.

Bangladesh's internal security landscape was profoundly shaped by a series of intelligence failures in the 1970s and 1980s, including two presidential assassinations and multiple military coups and mutinies. Since the early 2000s, several high-profile terrorism incidents and insurrections under both AL and the Bangladesh Nationalist Party (BNP) stand out as some of the most consequential intelligence failures in the country's post-independence history. These crises not only exposed institutional vulnerabilities but also reoriented the state's priorities toward internal intelligence gathering and regime preservation, entrenching surveillance as a core instrument of statecraft to preempt instability, consolidate authority, and monitor perceived threats to regime continuity.

In parallel, the re-Islamization of Bangladesh's political landscape, especially after the assassination of Sheikh Mujibur Rahman, had lasting implications for state surveillance. Between 1975 and 1990, Ziaur Rahman and later Hussain Muhammad Ershad institutionalized political Islam within governance structures and restructured intelligence agencies to surveil political and civil society actors, including leftist groups, trade unions, and student organizations.[7] Subsequently, throughout the 1990s and in early 2000s, the alliance between BNP and the Bangladesh Jamaat-e-Islami (JIB) further entrenched the institutional legitimacy of the Islamization of Bangladesh's political order, reinforcing an intelligence culture oriented toward regime security and ideological control. As political Islam gained ground, intelligence priorities shifted toward monitoring ideological dissidence.

Khaleda Zia's second full term in office also coincided with the 9/11 attacks in the United States and a surge in domestic terrorist activity. Key incidents during this period included the 2001 bombings in Ramna Park and at a Communist Party of Bangladesh rally, and the 2004 grenade attack on an AL rally and attempted assassination of the British High Commissioner, each carried out by or linked to Harkat-ul-Jihad al-Islami.[8] In 2005, Jama'atul Mujahideen Bangladesh orchestrated two major attacks: the coordinated detonation of nearly 500 bombs across 63 of the country's 64 districts, and a suicide bombing campaign targeting members of the judiciary.[9]

The intensification of surveillance continued into the following decade under Sheikh Hasina's successive terms. Especially after the 2009 mutiny and the 2016 Holey Artisan Bakery attack,[10] both institutional and technological surveillance capabilities expanded rapidly. Specialized agencies like the Counter Terrorism and Transnational Crime (CTTC) division and the newly formed Anti-Terrorism Unit (ATU) procured advanced tools for cyber surveillance.[11] Framed within the broader banner of counterterrorism, these enhanced capabilities were often operationalized through new tools and technologies procured via partnerships with international agencies and private

[7] Ganguly, S. (2006). The Rise of Islamist Militancy in Bangladesh. United States Institute of Peace. <https://www.usip.org/publications/2006/08/rise-islamist-militancy-bangladesh>.

[8] The Daily Star. (2024). 2001 Ramna Batamul attack: Timeline. <https://www.thedailystar.net/news/bangladesh/crime-justice/news/2001-ramna-batamul-attack-timeline-3587116>; BBC News. (2004). Bangladesh rocked by deadly blast. <http://news.bbc.co.uk/2/hi/south_asia/3586384.stm>; Alam, J. (2020). Bangladesh opposition leader accuses government. Associated Press. <https://apnews.com/general-news-0c2c3080c91ad74705f543fb5defa082>; Reuters. (2016). Bangladesh upholds death sentences over 2004 attack on British envoy. <https://www.reuters.com/article/world/bangladesh-upholds-death-sentences-over-2004-attack-on-british-envoy-idUSKBN13W0KU/>.

[9] The Daily Star. (2016). Bomb attack on Laxmipur court: HC upholds death for JMB man. <https://www.thedailystar.net/country/news/bomb-attack-laxmipur-court-hc-upholds-death-jmb-man-1205167>; The Daily Star. (2016). Death of 6 JMB militants stays. <https://www.thedailystar.net/frontpage/death-6-jmb-militants-stays-1261018>; CNN. (2005). Bangladesh arrests top Islamic militants. <http://edition.cnn.com/2005/WORLD/asiapcf/12/03/bangladesh.arrests/index.html>.

[10] The Washington Post. (2016). Gunmen take hostages at Bangladesh restaurant; 2 dead. <https://web.archive.org/web/20160703121022/https://www.washingtonpost.com/world/asia_pacific/gunmen-take-hostages-at-bangladesh-restaurant-2-dead/2016/07/01/fd4a7a9a-3fe9-11e6-9e16-4cf01a41decb_story.html>; The Guardian. (2009). Dozens killed in Bangladesh mutiny by border guards. <https://www.theguardian.com/world/2009/feb/25/bangladesh-mutiny-soldiers>.

[11] Ashraf ,A .A .)2022(.Bangladesh :Intelligence Culture and Reform Priorities .In R .Shaffer(Ed ,).*The Handbook of Asian Intelligence Cultures* .Rowman & Littlefield Publishers.

vendors. While these measures strengthened the state's tactical response to extremist threats, their largely unchecked expansion significantly extended the reach of surveillance into everyday civic spaces. Operating beyond immediate security contexts, surveillance increasingly targeted not only suspected militants but also journalists, activists, and political opponents, blurring the line between national security and political control.[12]

Set against the backdrop of the Global War on Terror, these developments triggered a wave of legal and extralegal surveillance practices and catalyzed renewed interest in modernizing intelligence infrastructure. This period marked the beginning of a convergence between traditional intelligence and emerging cyber capabilities, enabled through international security cooperation and expanded public procurement of surveillance technologies. Nevertheless, the fundamental function of surveillance in Bangladesh—as a tool of political control rather than democratic accountability—remains largely unchanged.

Surveillance and Authoritarian Drift

The political backdrop of cyber surveillance in Bangladesh is inseparable from its authoritarian tendencies, deep-rooted mistrust between the state and its citizens, politicized security governance, and external influences.

While surveillance infrastructure was originally developed to counter national security threats and militancy, it has increasingly been deployed to consolidate political power and suppress dissent. Over the past three decades, successive governments have expanded these tools and technologies to reinforce executive authority. This politicization is amplified during electoral periods, as intelligence agencies are used to monitor and sometimes harass opposition figures. AL's use of surveillance played a key role in securing three consecutive election victories in 2014, 2018, and 2023, each marked by credible allegations of widespread electoral irregularities.[13] Its principal rivals, including BNP and JIB, along with dissidents, students, and activists, were subjected to intensive and invasive surveillance, often leading to arbitrary arrests, enforced disappearances, and extrajudicial killings.[14] Criticism and dissent have increasingly been conflated with national security threats, contributing to the shrinking of civic space.

These practices were accompanied by a broader set of online restrictions. For instance, ahead of the 2018 national elections, the government enforced localized internet shutdowns and blocked Skype to prevent opposition leaders from interviewing potential nominees.[15] Similarly, in 2022, mobile network services were deliberately degraded in areas hosting opposition rallies.[16] Cybersecurity laws have been routinely invoked to justify the arbitrary arrest and detention of journalists, activists, students, and opposition figures on vague or politically motivated charges. Within five years of its enactment, at least 7,000 cases were filed under the Digital Security Act, 2018. Amid these situations, opposition parties withdrew from the electoral race in 2014 and 2023.[17]

[12] Turner-Rahman, S. (2023). National and transnational digital repression in Bangladesh. University of Washington, Jackson School of International Studies. <https://jsis.washington.edu/news/national-and-transnational-digital-repression-in-bangladesh/>.

[13] Human Rights Watch. (2018). No place for criticism: Bangladesh crackdown on social media commentary. <https://www.hrw.org/report/2018/05/10/no-place-criticism/bangladesh-crackdown-social-media-commentary>.

[14] Human Rights Watch. (2018). Bangladesh: Crackdown as elections loom. <https://www.hrw.org/news/2018/12/13/bangladesh-crackdown-elections-loom>; Office of the United Nations High Commissioner for Human Rights. (2022). Situation of human rights in Bangladesh in the context of events surrounding the elections in 2018. <https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/ohchr-fftb-hr-violations-bd.pdf>; Department of Foreign Affairs and Trade. (2021). Country information report: Bangladesh. Australian Government. <https://www.dfat.gov.au/sites/default/files/country-information-report-bangladesh.pdf>.

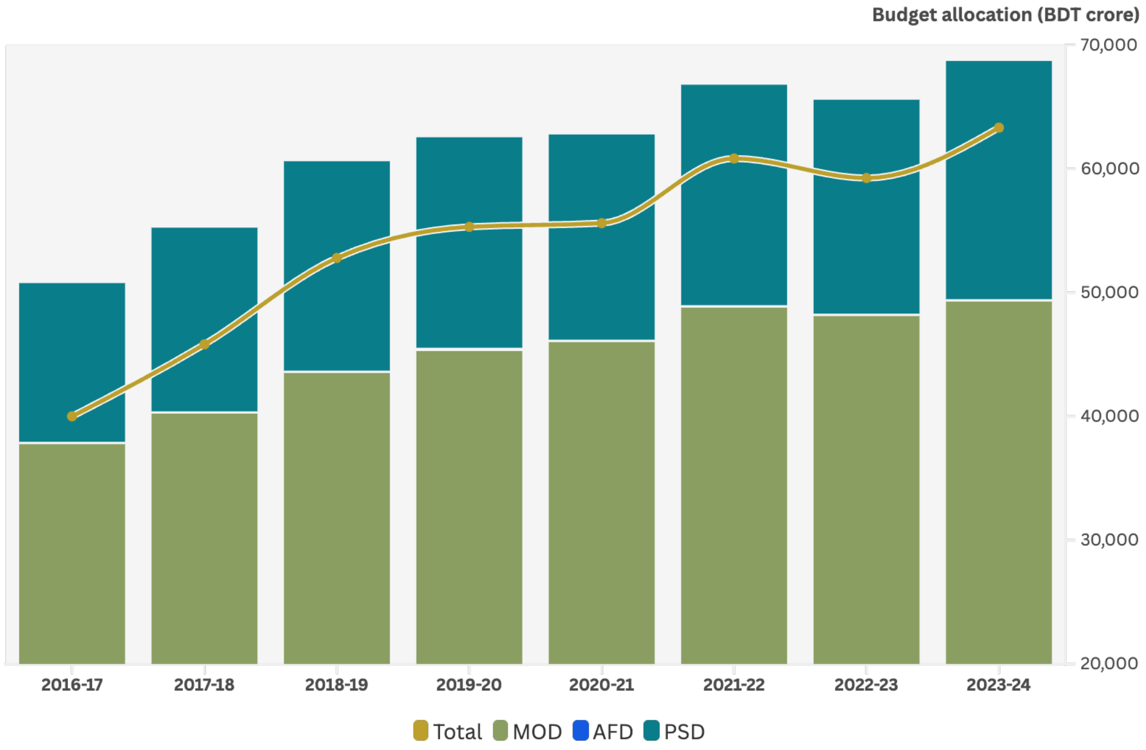
[15] The Daily Star. (2018). BTRC blocks Skype. <https://www.thedailystar.net/js-polls-2018/btrc-blocks-skype-1662676>.

[16] Afrin, S. (2022). Why internet speed slows down during BNP rallies. Prothom Alo. <https://en.prothomalo.com/bangladesh/politics/3yu4tyed3t>.

[17] The Daily Star. (2023). Over 7,000 cases under DSA: Law minister. <https://www.thedailystar.net/news/bangladesh/crime-justice/news/over-7000-cases-under-dsa-law-minister-3338511>; International Crisis Group. (2023). Beyond the election: Overcoming Bangladesh's political deadlock (Report No. 336). <https://www.crisisgroup.org/asia/south-asia/bangladesh/336-beyond-election-overcoming-bangla-

Defence budget has increased by 7% year-on-year

Aggregate budgets for defence and intelligence divisions increased by more than 58% between 2016 and 2023

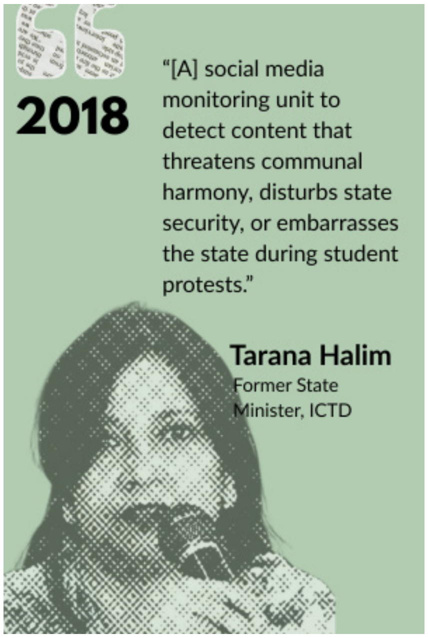


Source: Ministry of Finance, see Appendix

The average annual budget of three principal security and defence institutions—the Ministry of Defence, the Armed Forces Division, and the Public Security Division, under which all law enforcement and intelligence agencies (except NSI) operate—increased by nearly 7% year-on-year between the 2016-17 and 2023-24 financial years.

Since 2009, the AL government not only deployed surveillance technologies but also steadily expanded the state's capacity in this domain. It remains unclear whether this sustained investment reflects a calculated strategy by the government to consolidate political authority or a tacit bargain in which the security apparatus has instrumentalised political actors for its own ends. Although specific defence and intelligence budgets remain classified and are exempt from public disclosure, the average annual budget of three principal security and defence institutions—the Ministry of Defence, the Armed Forces Division, and the Public Security Division, under which all law enforcement and intelligence agencies (except NSI) operate—increased by nearly 7% year-on-year between the 2016-17 and 2023-24 financial years. Notably, the aggregate budgets for these ministries and divisions increased by more than 58% over an eight-year period, from BDT 40,008

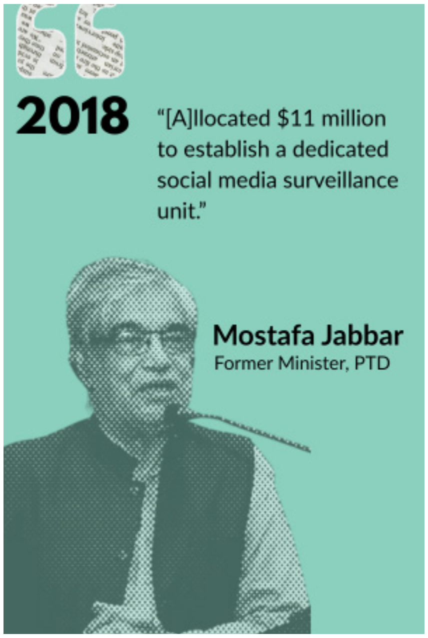
deshs-political-deadlock>.



2018

"[A] social media monitoring unit to detect content that threatens communal harmony, disturbs state security, or embarrasses the state during student protests."

Tarana Halim
Former State Minister, ICTD



2018

"[A]llocated $11 million to establish a dedicated social media surveillance unit."

Mostafa Jabbar
Former Minister, PTD

2019

"[NTMC] now has an advanced content blocking and filtering system."

Asaduzzaman Khan
Former Minister, Ministry of Home Affairs

crore in 2016 to BDT 63,333 crore in 2023. This upward trend appears to reflect broader investment priorities, including the possible expansion of surveillance-related infrastructure. Yet, mechanisms for democratic oversight remain virtually absent. Both legislative and constitutional safeguards, including parliamentary oversight mechanisms, remain largely dormant or symbolic in nature.[18] As a result, surveillance has remained largely unchecked, further exacerbating democratic backsliding in Bangladesh.

Alongside this budgetary growth, public statements from high-ranking government officials reflect an explicit policy commitment to strengthening internal security and digital monitoring capacities. For instance, in 2018, the cabinet approved a multimillion-dollar deal to procure surveillance technologies for the intelligence community.[19] Around this time, former State Minister Tarana Halim announced the formation of a social media monitoring unit tasked with detecting content that "threatens communal harmony, disturbs state security, or embarrasses the state" during student protests, while then Minister Mostafa Jabbar reported allocation of USD 11 million to establish a dedicated social media surveillance unit.[20] In 2019, NTMC reportedly implemented a "content blocking and filtering system." Amid ambiguity around state capability, former Home Minister Asaduzzaman Khan acknowledged the existence of more sophisticated social media surveillance tools in the agency's inventory.[21]

Even during the final months of its most recent term, the AL government appeared to have relied on these surveillance capabilities to quell mass uprising in July and August 2024. According to a fact-finding report by the Office of the United Nations High Commissioner for Human Rights, each of the aforementioned

[18] Office of the United Nations High Commissioner for Human Rights. (2025). Fact-Finding Report on Human Rights Violations and Abuses related to the Protests of July and August 2024 in Bangladesh. <https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/ohchr-fftb-hr-violations-bd.pdf>.

[19] New Age. (2018). Social media to come under telecom monitoring, surveillance. <https://www.newagebd.net/article/43598/social-media-to-come-telecom-monitoring-surveillance>.

[20] Mahmud, F. (2018). Bangladesh ramps up efforts to monitor social media after months of student-led agitations. Scroll.in. <https://scroll.in/article/891011/bangladesh-ramps-up-efforts-to-monitor-social-media-after-months-of-student-led-agitations>; Human Rights Watch. (2018). Bangladesh: Crackdown on social media ahead of elections. <https://www.hrw.org/news/2018/10/19/bangladesh-crackdown-social-media>; Human Rights Watch. (2018). No place for criticism: Bangladesh crackdown on social media commentary. <https://www.hrw.org/report/2018/05/10/no-place-criticism/bangladesh-crackdown-social-media-commentary>.

[21] The Daily Star. (2019). NTMC to filter online anti-govt propaganda. <https://www.thedailystar.net/city/online-anti-govt-propaganda-in-bangladesh-ntmc-filter-1704910>; Dhaka Tribune. (2023). ARTICLE 19 condemns surveillance through controversial technology.

intelligence agencies “shared intelligence, including information obtained through surveillance in violation of the right to privacy, to enable the campaign of mass arbitrary arrest,” as well as abduction and torture. Specifically, NTMC was found to have provided “surveillance and intelligence, including by monitoring people’s personal communications and supporting arrest and other police operations.”[22]

Taken together, these statements illustrate the political leadership’s sustained will to entrench surveillance as a central instrument of postcolonial statecraft, aimed at serving regime security. The normalization of cyber surveillance in Bangladesh, as documented in this report, reflects a broader transformation in the nature of state power. What ought to have been a defensive measure has now been reconfigured into a quiet but pervasive lever of governance to manage public discourse and suppress dissent. Unless counterbalanced by rights-based civil society oversight, legal reform, and transparency mechanisms, this trajectory threatens to entrench a form of digital authoritarianism under the guise of security modernization.

Surveillance, and Global and Regional Drivers

Bangladesh’s turn toward advanced cyber surveillance is also influenced by international and regional security dynamics. Among the most influential factors is the U.S.-led Global War on Terror, which played a pivotal role in redefining national security priorities worldwide, including in Bangladesh. Counterterrorism emerged as a dominant organizing principle for state security apparatuses.

Bangladesh expanded its surveillance and law enforcement capabilities through a combination of formal and informal partnerships, most notably with the Five Eyes countries, the European Union, and India.

Bangladesh expanded its surveillance and law enforcement capabilities through a combination of formal and informal partnerships, most notably with the Five Eyes countries, the European Union, and India. These partnerships facilitated access to technical assistance, funding, procurement opportunities, and intelligence-sharing, often with limited attention to democratic oversight or human rights safeguards. For example, the United States has reportedly worked closely with Bangladeshi agencies through the State Department’s Anti-Terrorism Assistance Program, providing institutional training to security agencies.[23] Core agencies like DGFI and NSI also transitioned from a reliance on human intelligence (HUMINT) to incorporating signals intelligence (SIGINT) and open-source intelligence (OSINT), laying the groundwork for systematic cyber surveillance. This shift was further supported by non-public procurement agreements involving foreign vendors.

Over the years, intelligence cooperation between Bangladesh and India appears to have increased. Counterterrorism responses in India—especially after the 2001 Indian Parliament attack and the 2008

<https://www.dhakatribune.com/bangladesh/302955/article-19-condemns-surveillance-through>.

[22] Office of the United Nations High Commissioner for Human Rights. (2025). Fact-Finding Report on Human Rights Violations and Abuses related to the Protests of July and August 2024 in Bangladesh. <https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/ohchr-fftb-hr-violations-bd.pdf>; United Nations. (2024). Bangladesh: UN report finds brutal, systematic repression of protests, calls for justice for serious rights violations. <https://bangladesh.un.org/en/289108-bangladesh-un-report-finds-brutal-systematic-repression-protests-calls-justice-serious>.

[23] The Daily Star. (2012). US experts provide anti-terrorism training. <https://www.thedailystar.net/news-detail-242432>; Bangladesh Public Service Commission. (2022). Annual Report 2022. <https://psc.gov.bd/storage/app/media/uploaded-files/Annual_Report_2022_PSC.pdf>.

Mumbai attacks—alongside the 2004 Chittagong arms haul case in Bangladesh,[24] appear to have had spillover effects across the border. Amid regional and international security pressures, Bangladeshi security agencies appeared to have adopted hardline approaches. Often, this extended to preemptive surveillance of suspected groups and the criminalization of ideological dissent. Furthermore, the securitization of Islam and the portrayal of cross-border militancy as an existential threat to both countries further reinforced policy alignment between the two countries.

While the cooperation has enhanced tactical counterterrorism capacity, it has also drawn criticism for bypassing democratic scrutiny and contributing to Bangladesh's increasingly centralized intelligence architecture. These trends have raised growing concerns about the consolidation of authoritarian practices under the pretext of global and regional security imperatives, with the Global War on Terror and shifting regional dynamics instrumentalized to provide cover for expanding the surveillance state and serve the narrow political interests of the country's leadership.

[24] Bhattacharyya, R. (2023). Chittagong Arms Haul in Bangladesh Remains a Riddle. The Diplomat. <https://thediplomat.com/2023/12/chittagong-arms-haul-in-bangladesh-remains-a-riddle/>; The Guardian. (2001). Twelve dead in attack on Indian parliament. <https://www.theguardian.com/world/2001/dec/13/india>; Riedel, B. (2012). Mumbai attacks: Four years later. Brookings. <https://www.brookings.edu/articles/mumbai-attacks-four-years-later/>.

LEGAL FRAMEWORK GOVERNING CYBER SURVEILLANCE

The legal architecture enabling cyber surveillance in Bangladesh is a complex framework comprising constitutional provisions, legislative enactments, executive directives, and regulatory guidelines. While Bangladesh's Constitution offers nominal protections for privacy and freedom of expression, these rights are frequently circumscribed by a suite of laws justified in the name of national security, public order, and counterterrorism. This section examines the principal legal instruments that authorize and shape cyber surveillance in Bangladesh.

> **Telegraph Act, 1885 and the Wireless Telegraphy Act, 1933, remain operational today and continue to inform contemporary surveillance practices.**

Key Legislations Authorizing Surveillance

Among the primary legal instruments relied upon by state authorities to conduct surveillance is the Bangladesh Telecommunication Regulation Act, 2001. Following amendments in 2006 and 2010, the statute effectively granted surveillance powers to law enforcement, intelligence, and regulatory agencies, enabling them to intercept, monitor, and collect information transmitted via telecommunication networks. Notably, this provision was not conceived in a vacuum; it builds on a long-standing legacy of expansive state control powers embedded in colonial-era legislations such as the Telegraph Act, 1885 and the Wireless Telegraphy Act, 1933, which remain operational today and continue to inform contemporary surveillance practices. Collectively, these provisions have been interpreted to confer sweeping authority to agencies such as NTMC, DGFI, NSI, ATU, SB, RAB, and Bangladesh Police to surveil internet traffic, encrypted communications, and voice and data transmissions.

Moreover, service providers are legally compelled to cooperate with government requests, under threat of criminal penalties, including fines, imprisonment, and potential non-renewal of operating licenses. At the same time, the law imposes no obligation on these agencies to conduct human rights due diligence in the procurement or deployment of cyber surveillance technologies, nor does it provide for institutional accountability or independent oversight mechanisms to ensure legal or constitutional compliance. Although the statute assigns the Bangladesh Telecommunication Regulatory Commission (BTRC) the responsibility to protect user privacy, this mandate remains largely unimplemented in practice, rendering privacy protections ineffective and largely symbolic.

Several other legislations provide direct and indirect authority for state agencies to conduct surveillance, including interception of digital communications. After gaining independence in 1971, Bangladesh saw successive autocratic and semi-autocratic governments with each regime relying on HUMINT, SIGINT, and OSINT for state surveillance, sanctioned by colonial-era or colonial-inspired statutes. These include the Code of Criminal Procedure, 1898, the Special Powers Act, 1974, the Official Secrets Act, 1923, the Anti-Terrorism Act, 2009, the Dhaka Metropolitan Police Ordinance, 1976, and the Special Security Force Ordinance, 1986. While these laws provide broad surveillance powers with minimal safeguards, certain specialised and sector-specific agencies—such as the Bangladesh Financial Intelligence Unit under the Bangladesh Bank, the Central Intelligence Cell under the National Board of Revenue, and the Market Surveillance and Intelligence Department of the Bangladesh Securities and Exchange Commission—possess more limited mandates focused on financial transactions, tax evasion, and market irregularities. However, even these bodies may have adopted digital monitoring tools, contributing to a broader, opaque surveillance ecosystem that lacks comprehensive oversight or privacy protections. Our research found that at least 22 different laws directly or indirectly enable invasive data collection activities by law enforcement, intelligence, and regulatory agencies.[25]

Licensing and Regulatory Guidelines

While the Bangladesh Telecommunication Regulation Act, 2001 provides general legal cover for privacy-infringing activities, the accompanying licensing framework imposes specific obligations on operators across the telecommunications value chain. These include enabling real-time access to user information, bulk data interception, and live database monitoring by designated security and intelligence agencies. Certain licensing guidelines also impose a positive obligation on operators to identify and report users flagged as national security threats. Although the exact modalities of compliance remain opaque, such obligations are likely fulfilled without meaningful user knowledge or informed consent. As a result, entities ranging from submarine and international terrestrial cable operators to mobile network providers and internet service providers are compelled to facilitate targeted and untargeted surveillance, without judicial warrants or any obligation to notify affected users.

Constitutional Underpinnings and Their Limitations

The Constitution of the People's Republic of Bangladesh guarantees several fundamental rights relevant to cyber surveillance. Article 39 affirms freedom of speech and the press, while Article 43 ensures the privacy of correspondence and "other means of communications" for every citizen. However, these rights are not absolute. Rather, they are subject to "reasonable restrictions imposed by law" in the interests of state security, public order, morality, and other specified grounds. While restrictions on fundamental rights are not inherently unconstitutional, their interpretation and application must conform to established constitutional standards of legality, necessity, and reasonableness. Existing constitutional jurisprudence mandates that any restriction on fundamental rights must be narrowly defined, procedurally safeguarded, and implemented in a non-arbitrary, non-discriminatory, fair, and proportionate manner.[26]

In practice, however, the current legal and institutional framework governing surveillance in Bangladesh fails to meet these constitutional benchmarks. For instance, section 97A of the Bangladesh Telecommunication Regulation Act, 2001—authorizing surveillance by any officer of an intelligence, national security, investigative, or law enforcement agency on vaguely defined grounds—grants sweeping discretionary powers that lack meaningful procedural safeguards. When applied by bodies like NTMC to enable expansive, warrantless, and opaque surveillance practices, this provision is likely to exceed the constitutional threshold of "reasonableness."[27]

Similar concerns arise with agencies like the DGFI and NSI, which operate without any statutory mandate or publicly accessible operational guidelines, thereby evading scrutiny and due process. Furthermore, the imposition of surveillance duties via licensing conditions without legislative oversight, and the establishment of core surveillance agencies through executive orders with overreaching statutory exemptions, all combine to create an accountability vacuum. As surveillance continues to function primarily as a tool of political control rather than democratic accountability, exceptions to fundamental rights have increasingly become institutionalized, while constitutional guarantees have been systematically eroded.

[25] Mahmood, S., & Diya, S. R. (2024). A new Digital Frontier: A Blueprint for Reforms towards Rights-Respecting Information and Technology Laws in Bangladesh [White Paper]. Tech Global Institute. <https://techglobalinstitute.com/wp-content/uploads/2024/12/Whitepaper-A-New-Digital-Frontier-Bangladesh.pdf>.

[26] Mahmood, S., & Diya, S. R. (2024). A new Digital Frontier: A Blueprint for Reforms towards Rights-Respecting Information and Technology Laws in Bangladesh [White Paper]. Tech Global Institute. <https://techglobalinstitute.com/wp-content/uploads/2024/12/Whitepaper-A-New-Digital-Frontier-Bangladesh.pdf>.

[27] Chowdhury, K. R. (2021). Bangladesh says it is buying mobile-phone interceptor to boost national security. BenarNews. <https://www.benarnews.org/english/news/bengali/bangladesh-monitoring-equipment-06102021154009.html>.

Executive Orders and Agency Formations

Ministry or Institution	Key Agencies
Ministry of Home Affairs	- Public Security Division (PSD) ● National Telecommunication Monitoring Centre (NTMC) ● Bangladesh Police ○ Metropolitan Police ○ Rapid Action Battalion (RAB) ○ Anti-Terrorism Unit (ATU) ○ Special Branch (SB) ○ Detective Branch (DB) ○ Counter Terrorism and Transnational Crime (CTTC) ○ Criminal Investigation Department (CID) ○ Police Bureau of Investigation (PBI)
Information & Communication Technology Division	- Department of Information and Communication Technology (DoICT) - Bangladesh Computer Council (BCC) ● Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT)
Posts and Telecommunications Division	- Bangladesh Telecommunication Regulatory Commission (BTRC) - Bangladesh Telecommunications Company Limited (BTCL) - Department of Telecommunications (DoT)
Prime Minister's Office	- National Security Intelligence (NSI) - Armed Forces Division (AFD) (with dotted line to Ministry of Defence) ● Directorate General of Forces Intelligence (DGFI)

A significant portion of Bangladesh's intelligence and surveillance architecture has been established and empowered through executive orders, rather than parliamentary legislations. Key agencies such as the DGFI and NSI were created in 1972 via non-public authorizing instruments, and no primary or secondary legislation has since brought these bodies under a statutory framework detailing their functions, powers, or limits.

Likewise, NTMC, originally set up in 2008 as a unit within the DGFI, now functions as an independent entity at the epicenter of Bangladesh's cyber intelligence ecosystem—tasked with both collecting citizens' data and interfacing with all major law enforcement and intelligence agencies. Similarly, specialized counterterrorism units such as the CTTC were established through executive authorizations from the Ministry of Home Affairs. Although formally constituted under the Armed Police Battalions Ordinance, 1979, RAB recruits personnel from the military and intelligence services and is tasked with conducting "intelligence in respect of crime and criminal activities" without effective procedural safeguards or regulatory oversight. None of these institutions have publicly accessible mandate documents substantively outlining their legal scope or inter-agency coordination protocols.

Many agencies are explicitly exempt from public scrutiny under the Right to Information Act, 2009, while the proposed Personal Data Protection Ordinance contains broad carve-outs for law enforcement and intelligence activities.

These agencies are further insulated from legal accountability and transparency mechanisms. For instance, many are explicitly exempt from public scrutiny under the Right to Information Act, 2009, while the proposed Personal Data Protection

Ordinance contains broad carve-outs for law enforcement and intelligence activities. Several laws also contain provisions that shield these agencies from legal challenge for any actions undertaken "in good faith," effectively eliminating avenues for redress.[1] Additionally, their operations are shielded by the Rules of Business, as well as colonial-era statutes such as the Official Secrets Act, 1923, which criminalizes—in vague and discretionary terms—the unauthorized possession, retention, or communication of information deemed prejudicial to state security or interests. Offenses under the statute, in particular, can be prosecuted as espionage and are punishable by life imprisonment or even death. Collectively, these provisions create a legal environment in which intelligence agencies function with impunity, operating beyond the reach of public accountability or democratic oversight.

Of note, the Ministry of Home Affairs is the primary authority responsible for overseeing Bangladesh's security architecture, including law enforcement, intelligence agencies, and paramilitary forces. Assisted by the Prime Minister's Office, the Information & Communication Technology Division, and other ministries, its mandate spans both routine policing and national intelligence coordination, with responsibilities extending to both internal and external security matters, cross-border cooperation, and enforcement of the official secrecy laws. As such, it plays a central role in procuring, deploying, and regulating surveillance technologies across multiple state agencies.

[1] Human Rights Watch. (2021). Where no sun can enter: A decade of enforced disappearances in Bangladesh. <https://www.hrw.org/report/2021/08/16/where-no-sun-can-enter/decade-enforced-disappearances-bangladesh>.

Lack of Robust Oversight and Judicial Recourse

A recurring theme in the analysis of Bangladesh's surveillance framework is the absence of robust independent oversight. Existing legal instruments fail to confer any meaningful mandate on the national parliament or its standing committees to scrutinize substantive issues related to security procurement and intelligence activities. As a result, the executive branch retains disproportionate control over the intelligence community.

Attempts to challenge the constitutionality of surveillance-enabling laws have encountered significant hurdles. For example, a judicial review petition filed in 2006 challenging the sweeping powers under section 97A of the Bangladesh Telecommunication Regulation Act, 2001—on the grounds that it constitutes an unreasonable restriction and violates the right to privacy under Article 43 of Bangladesh's Constitution—was dismissed, with the court reportedly ruling that the provision does not explicitly authorize violations of legal or constitutional standards.28 Similar constitutional challenges, such as the one against section 57 of the Information and Communication Technology Act, 2006 or against sections 25 and 31 of the Digital Security Act, 2018, have either been disregarded or dismissed.29 These precedents underscore the difficulties in obtaining judicial remedies against discretionary provisions or expansive state powers that carry significant risks of rights violations.

Our research found that at least 22 different laws directly or indirectly enable invasive data collection activities by law enforcement, intelligence, and regulatory agencies

[28] Rahman, M. R. (2016). South Asian Communication Surveillance and the Right to Privacy in the Digital Age (Master's thesis). Central European University.

[29] Shaon, A. I. (2015). HC rejects writ challenging Section 57 of ICT Act. Dhaka Tribune. <https://www.dhakatribune.com/bangladesh/bangladesh-others/108288/hc-rejects-writ-challenging-section-57-of-ict-act>; The Daily Star. (2020). Digital Security Act: HC questions two sections. The Daily Star. <https://www.thedailystar.net/frontpage/news/digital-security-act-hc-questions-two-sections-1872433>.

HOW BANGLADESH BECAME A SURVEILLANCE STATE

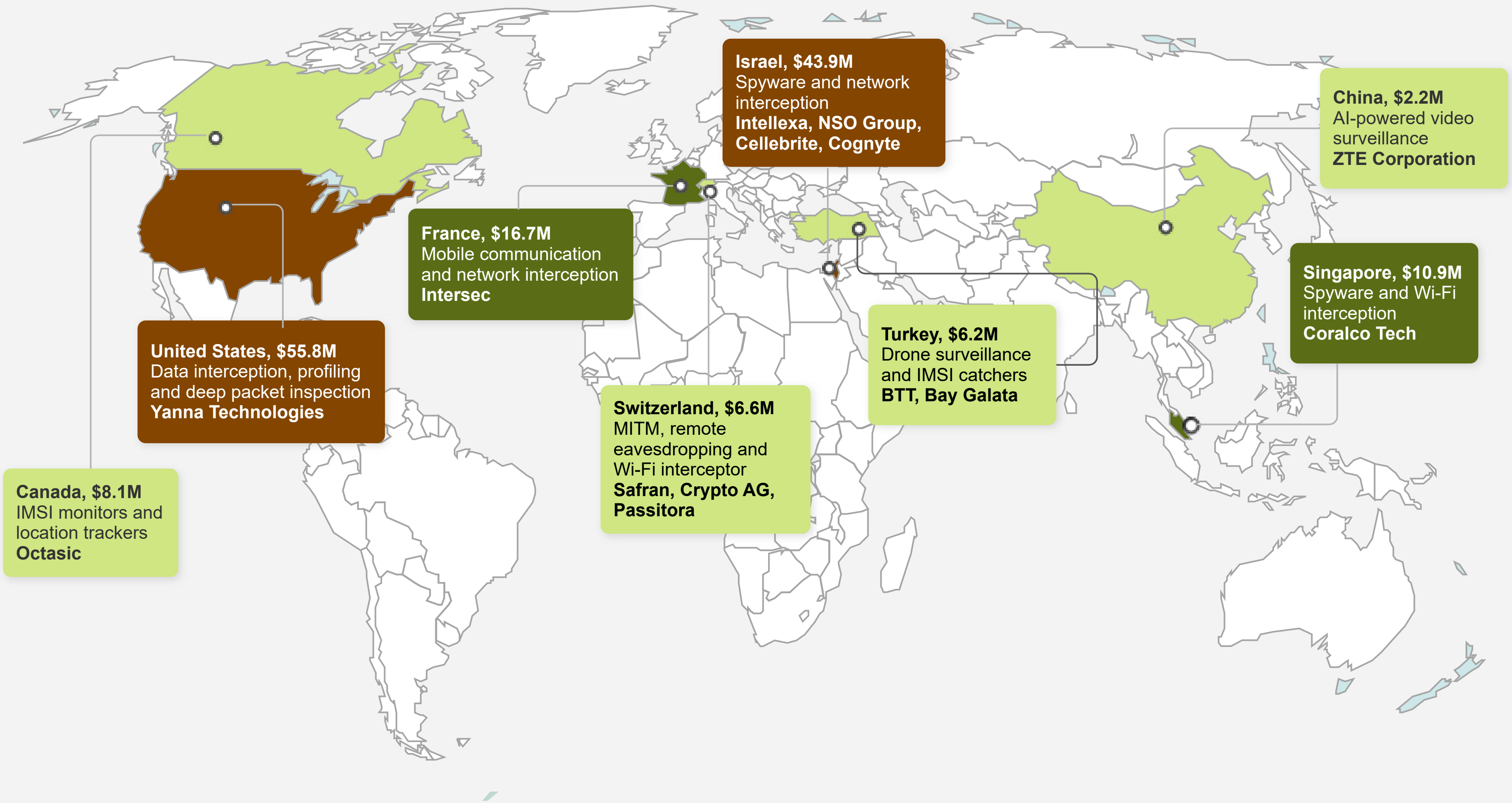
KEY FINDINGS AND PATTERNS

Bangladesh has, over the years, significantly expanded its surveillance apparatus through the acquisition of a wide range of cyber (software) and physical (hardware) monitoring technologies, often procured via opaque channels and sourced from foreign vendors. Often, the technologies are procured with the approval from the highest level of the government. For instance, the Executive Committee of the National Economic Council approved BDT 316.84 crore for acquisition of laser listening device, GSM/UMTS vehicular active support, IMSI catcher, Cellebrite UFED, Wi-Fi interceptors, and robot and drone surveillance devices by RAB between 2019 and 2021.[30]

Our findings are between 2015 and 2025, spanning a ten-year period in which various law enforcement, intelligence, and other government agencies have procured or deployed cyber surveillance technologies. Drawing on procurement records, tenders, import-export data, government orders, training logs, and open-source investigations, the following sections categorize the cyber surveillance tools in use, identifies key procuring agencies, and outlines their known or likely applications. Collectively, they offer a rare glimpse into the architecture of an increasingly sophisticated and secretive surveillance regime.

[30] See ,for example ,Executive Committee of the National Economic Council .)2020(.*Meeting Minutes* .Government of People’s Republic of Bangladesh< .

At least 20 countries have exported cyber surveillance technologies to Bangladesh worth US$ 184.5 million between 2015 and 2025



Israel, $43.9M
Spyware and network interception
Intellexa, NSO Group, Cellebrite, Cognyte

China, $2.2M
AI-powered video surveillance
ZTE Corporation

France, $16.7M
Mobile communication and network interception
Intersec

Singapore, $10.9M
Spyware and Wi-Fi interception
Coralco Tech

United States, $55.8M
Data interception, profiling and deep packet inspection
Yanna Technologies

Turkey, $6.2M
Drone surveillance and IMSI catchers
BTT, Bay Galata

Switzerland, $6.6M
MITM, remote eavesdropping and Wi-Fi interceptor
Safran, Crypto AG, Passitora

Canada, $8.1M
IMSI monitors and location trackers
Octasic

At least 160 surveillance technologies and spyware worth nearly USD 190 million likely procured

Our findings reveal that at least 160 surveillance technologies and spyware systems were likely imported into or deployed in Bangladesh between 2015 and 2025, at an estimated combined cost of USD 184.5 million. However, due to the lack of transparency and the challenges in accessing publicly available information on these technologies, it is difficult to assess the actual amount and may be higher. Multi-year vendor contracts made it additionally difficult to ascertain the exact expense in a given year.

These include audio surveillance devices like laser microphones, and spyware such as Pegasus, Predator, WiSpear, and FinFisher, AI-powered video surveillance systems with facial recognition, mobile and Wi-Fi interceptors like IMSI catchers, and software capable of full device access. Other tools include geolocation trackers, forensic extraction devices like Cellebrite UFED, deep packet inspection systems for monitoring internet traffic, and jamming devices have been used to disrupt wireless communications. At least nine known commercial spyware vendors have sold their technologies to Bangladesh, including sanctioned firms and/or their owners like those at NSO Group, Intellexa Consortium[31] and Cytrox. Others include British-German Gamma Group, Israel conglomerate Verint Systems and its subsidiaries Cognyte and UTX Technologies, and Israeli-owned Cellebrite, and Coralco Tech.

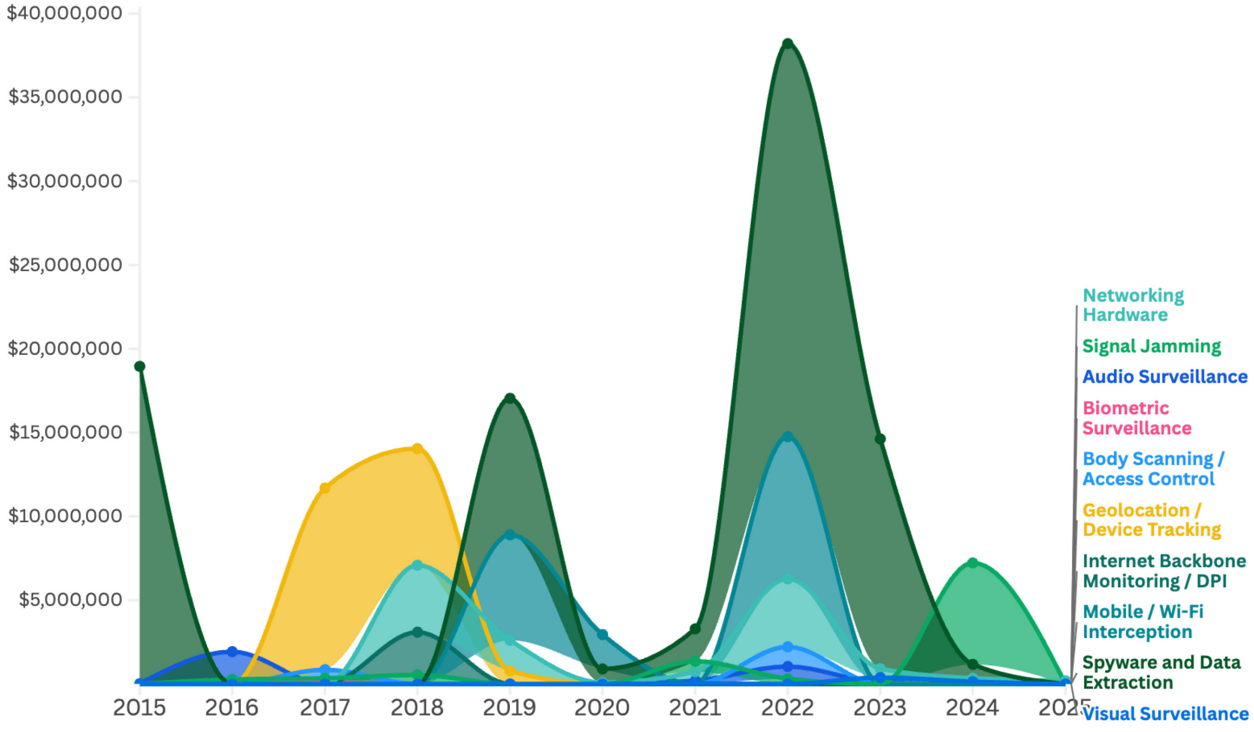
[31] U.S. Department of Treasury. (2024). Treasury sanctions enablers of Intellexa commercial spyware consortium <https://home.treasury.gov/news/press-releases/jy2581>

Purchases were higher just ahead of national elections

Ahead of national elections in 2017–18 and 2023–24, the government spent an estimated amount of at least USD 20 million over a 12–18 month period on surveillance technologies and spyware. Before the 2018 election, most spending focused on geolocation trackers and related software. By 2023, the emphasis had shifted to spyware capable of remote eavesdropping, full device access, and data extraction. Procurement records and training logs for law enforcement and intelligence officers between 2022 and 2024 show a strong focus on extracting social media, messaging, and web content, particularly Messenger, Telegram, WhatsApp, and Viber. Multiple purchases targeted equipment and software designed to break end-to-end encryption or deploy malware to remotely access devices, enabling direct retrieval of app-based communications.

Spikes in purchase coincide with national election years in 2018 and 2024

Increased spend on geolocation tracking ($10.8m) and spyware ($23.5m) ahead of national polls, indicating heightened surveillance on political rallies and candidates



2022 marked the highest annual spending on surveillance at USD 88 million

Based on available government records, in 2022, Bangladesh recorded its largest single-year expenditure on surveillance and spyware, totaling nearly USD 88.3 million. NTMC accounted for at least USD 78.3 million of this spending. That year, Major General Ziaul Ahsan assumed leadership of NTMC, overseeing its transformation from a modest intelligence processing unit within the Ministry of Home Affairs into a sophisticated spy agency embedded in the country's regulatory, political, and intelligence infrastructure.

In August 2022, French cybersecurity firm, Intersec, reportedly won a contract worth EUR 13 million (equivalent to USD 16.7 million at current conversion rate) to provide a geopositioning and complete network intelligence system to NTMC, coupled with five years of technical support and training.[32] Intersec's website indicates their "govtech" solution can analyze mobile network metadata and facilitate "less intrusive" content interception.[33] That same year, American firm, Yanna Technologies, won a contract worth USD 51.7 million to set up an "integrated lawful interception system" that can target individuals "threatening national security"[34]. Five months following the news, in January 2023, former Minister of Home Affairs Azaduzzaman Khan indicated that NTMC has now introduced an "integrated lawful interception system" that "possesses advanced capabilities for social media monitoring."[35]

[32] Intelligence Online. (2022). French firm Intersec bears U.S. giant SS8 for Bangladeshi geolocation contract. <https://www.intelligenceonline.com/surveillance--interception/2022/07/21/french-firm-intersec-beats-us-giant-ss8-for-bangladeshi-geolocation-contract,109800924-eve>.

[33] Intersec. Whitepaper. GovTec: Network Intelligence for Homeland Security. <https://insights.intersec.com/whitepaper-govtech-network-intelligence-for-homeland-security>

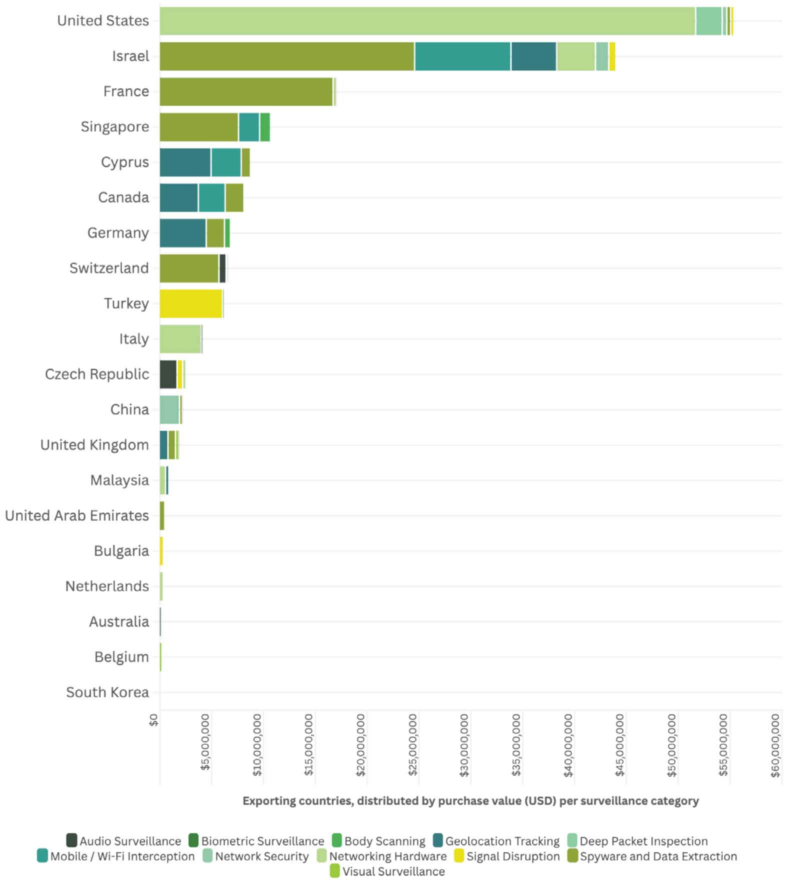
[34] The Daily Star. (2025). AL govt's secret surveillance state. <https://surveillancestate.thedailystar.net/>

[35] The Daily Star. (2023). Social media: Government introduces lawful interception. <https://www.thedailystar.net/news/bangladesh/news/social-media-government-launch-lawful-interception-3219566>

At least 30% of spyware procured appears to be Israeli-origin technologies, sold via third-country intermediaries

Although Bangladesh has no diplomatic engagements with Israel, public records show that Bangladeshi intelligence and government agencies have acquired several Israeli-origin surveillance and spyware systems for an estimated total of at least USD 43 million. This includes Cellebrite UFED and its Physical Analyzer (capable of extracting and analyzing data from mobile devices, including deleted files and app data) and Pegasus (enabling remote access to smartphones for covert monitoring), developed by Israel's NSO Group. Meanwhile, Prelysis, Cognyte, and Passitora—affiliated with Israel-owned commercial spyware firms like Intellexa and Verint—are registered in Cyprus, while Coralco Tech is registered in Singapore and PicSix is registered in Hungary. In 2022, Passitora sold its Wi-Fi interceptor for USD 5.7 million to NTMC through its Cyprus operations, evading diplomatic scrutiny and import controls. Collectively, these acquisitions deepen Bangladesh's integration of Israeli spyware, often linked globally to political repression and rights abuses including in Palestine, Egypt, Syria, and Armenia.

The United States takes the top spot as an exporting country at an estimated $55.6 million, while ISingapore follows Israel at at least USD 11 million, supplying technologies ranging from geolocation trackers and body scanners to spyware capable of remote device access and control. Many Singapore-registered firms may be linked to Israeli-origin consortiums known for exporting commercial spyware to repressive regimes, though this cannot be confirmed without greater transparency in company records. In contrast, public records show comparatively limited transactions with Chinese firms, totaling around USD 2.2 million, with ZTE Corporation's sales primarily involving video surveillance system.



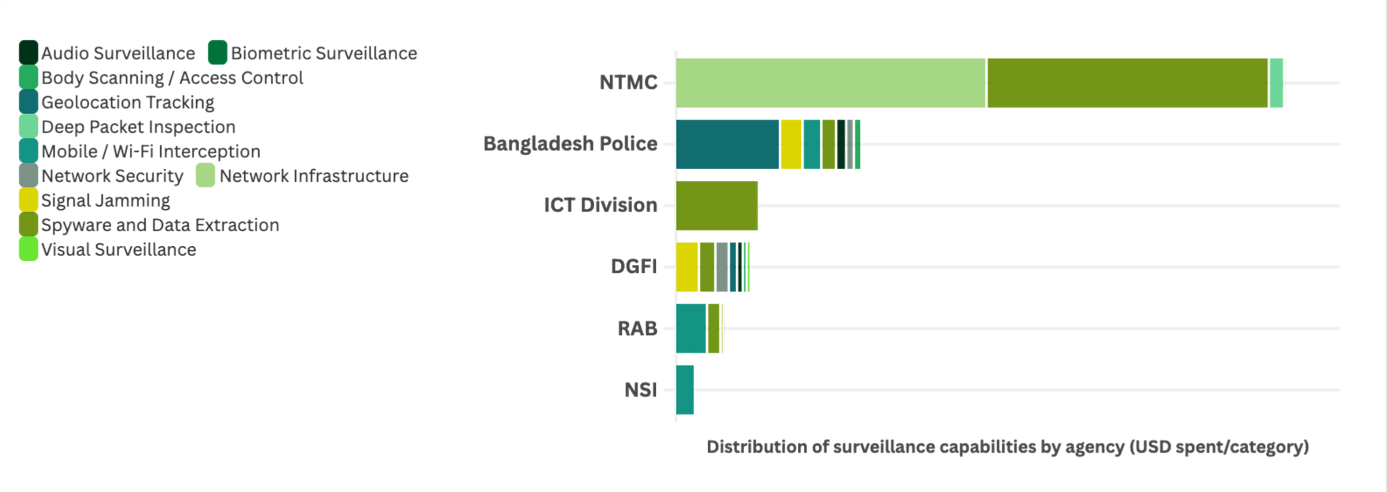
Device and app-level interception are central drivers for purchases, often achieved by installing malware in individual devices

Between 2018 and 2024, Bangladesh invested heavily in surveillance equipment, software, and spyware to block specific apps or content, break end-to-end encryption in messaging platforms like WhatsApp and Signal, and profile individuals through their social media and web activity. NTMC spent an estimated USD 46 million on equipment, spyware, and forensic tools to achieve the aforementioned, while the BGD e-GOV CIRT likely spent nearly USD 13 million. Authorities attempted to filter content at the app level, but when this proved difficult, they shifted to monitoring and filtering internet traffic at the provider level through deep packet inspection, and intercepting devices using spyware and malware.

Our investigations uncovered cases where malware was delivered through ordinary apps such as ridesharing, food delivery, e-commerce, games, and local content platforms. Once installed, this malware enabled intelligence and law enforcement agencies to fully access the device, monitor communications, and collect data without requiring app-level interception.

NTMC is the largest procurer, followed by Bangladesh Police and DGFI

While geolocation tracking and network interception are common across intelligence, law enforcement, and certain government agencies, our investigation identified clear patterns based on procurement records and training logs. NTMC is the single largest buyer, spending nearly USD 52 million between 2016 and 2025, with a focus on network interception, deep packet inspection, remote eavesdropping, and app- and device-level data extraction. Bangladesh Police and RAB have invested heavily in Wi-Fi and mobile network interception, as well as signal jamming through both vehicle-mounted and portable systems. Given their capabilities and specifications, these tools are primarily deployed for crowd control and the surveillance of protests. Meanwhile, DGFI has primarily invested in infrastructure for cell network monitoring and tapping, and signal jamming. Citizen Lab's investigations find that in 2015, DGFI purchased FinFisher, a computer spyware suite that can install malware on a target's device to gain access to their data and even take control of it.



Distribution of surveillance capabilities by agency (USD spent/category)

BREAKING DOWN SURVEILLANCE TECHNOLOGIES AND SPYWARE IN BANGLADESH

Against this backdrop, this report aims to identify, verify, and evaluate the use of surveillance technologies and spyware within the country. While source materials indicate certain surveillance technologies may have been acquired and/or deployed, there is absence of verifiable evidence conclusively establishing all the actors involved in and the timelines of their deployment, the command chain, and their actual uses. The absence of this information limits the ability to assess both the scale of surveillance capability and the manner in which it is applied in practice. Nevertheless, based on a reasonable assessment of the technical specifications and known functionalities of these systems, it is possible to make informed inferences about the surveillance capacity that exists in Bangladesh.

As a starting point, the table below provides a snapshot of the core categories of surveillance tools procured or used by Bangladeshi state agencies. As the documents reviewed do not list the intended use or technical specifications of these technologies, this table briefly outlines their potential uses based on a review of their known functionalities, which are addressed in greater detail in subsequent sections. This initial, indicative overview helps establish the breadth of technologies integrated into the country's surveillance architecture.

Category	Top Procuring Agency	Examples of Technologies Used in Bangladesh
Audio surveillance	DGFI, NTMC	Physical devices such as laser microphones, which detect vibrations on windows to capture sound from a distance, and GSM bugs hidden in everyday objects to transmit conversations via mobile networks. Other spywares, like Pegasus (NSO Group), FinFisher, and Predator (Intellexa / Cytrox), can remotely activate a smartphone's microphone to record audio and allow remote eavesdropping.
Video surveillance	Ministry of Home Affairs, DGFI, RAB	Advanced video surveillance systems enable real-time monitoring, facial recognition, vehicle tracking, and crowd analysis through AI-powered cameras and centralized command platforms, such as those supplied by ZTE Corporation. These include IP cameras and biometric surveillance kits that identify individuals using facial recognition, or iris scans, while under-door viewing kits use camera probes to covertly observe rooms without entry. Video surveillance can also be conducted using drones.
Mobile and Wi-Fi interceptors	Bangladesh Police, RAB	Surveillance devices, such as IMSI catchers, trackers, and monitors, that mimics a mobile cell tower to secretly intercept and track nearby mobile phones using the unique identifier number (IMSI) tied to SIM cards. Cell-site simulators, also known as Stingrays, manufactured and sold by Octasic, are devices capable of intercepting mobile phone signals and tracking user locations by masquerading as legitimate cell towers. They can be used to track location, monitor movement, and even intercept calls or text messages.
Geolocation and device tracking	NSI, Ministry of Home Affairs	Spyware targeting mobile devices can extract contacts, messages, multimedia files, browser data, and device information, as well as track GPS location, access the microphone and camera, record screen activity, execute shell commands, collect Wi-Fi data, and list running processes. Spyware like LightSpy employ dynamic plugins on macOS and Android devices to collect this information and access the device's internal systems.
Spyware	Bangladesh Police, DGFI, NTMC, RAB	Apollo (Merlinx) can intercept unsecured URL communications, extract email identifiers, and deploy cyber agents capable of infiltrating Android devices to access data, activate GPS tracking, and log keystrokes. Cellebrite's Universal Forensic Extraction Device (UFED) can bypass passwords and encryption to unlock mobile phones and other devices, extracting valuable data, and when used in conjunction with Cellebrite's Physical Analyzer, enabling operators to analyze data thoroughly and generate detailed reports. Oxygen Forensic Detective, similar to Cellebrite UFED, can access deep app- and cloud-level data, including chats, contacts and location.
Networking hardware and core infrastructure	DGFI, NTMC	Chinese firms like the ZTE Corporation provide telecommunication networks embedded in surveillance. Around the world, the firm has been directly involved in supplying and maintaining critical network equipment that enables real-time monitoring, filtering, and data interception. U.S. firm Yanna Technologies provides integrated platform infrastructure to intercept network traffic, remotely access devices, and extract data.
Deep packet inspection (DPI)	NTMC	DPI probes and other optical equipment allow monitoring and control of internet traffic, including accessing or modifying content of communications, such as emails, messages and browsing activity, inject scripts on webpages, and monitoring and filtering data packets as they travel across internet networks. Once embedded within national infrastructure, DPI can be used to block access to specific websites, throttle or prioritize certain services, and identify or target individuals based on their online behavior.
Signal disruptor	DGFI, RAB, Bangladesh Police	Jamming devices or RF jammers can intentionally block, interfere with, or disrupt wireless communications by emitting radio frequency (RF) signals on the same frequencies used by the target devices.

The following section identifies a number of tools and technologies that have been procured, and details, where possible, the entities responsible for their acquisition, operational deployment, or integration into broader security frameworks. It also sets out their likely uses based on known functionalities.

1. IMSI Monitors and Trackers

IMSI monitors and trackers are surveillance devices that mimic legitimate cell towers to capture unique mobile identifiers (also known as International Mobile Subscriber Identity (IMSI), which are linked to SIM cards) of nearby mobile devices. By collecting this identifier, such systems may be capable of locating, tracking, and monitoring targeted mobile devices in real time. Certain configurations are also reportedly able to intercept calls, messages, and other communications.

Documents from the Bangladesh Public Procurement Authority (BPPA) and Ministry of Home Affairs reveal several instances of procurement and related activities involving ***IMSI Monitors*** and ***Mobile Trackers*** by Bangladeshi law enforcement and intelligence agencies. They also list ***Backpack IMSI Monitors*** or ***Location Finders*** in procurement documents, which are easily concealable, portable versions likely designed for field operations requiring real-time location tracking.[36] Additionally, the documents refer to "Wide Terrain Searching Tools and Backpack Network Analyzers," which are likely intended for signal detection and network analysis across extensive areas, enhancing the state's capacity for covert surveillance. Their portability and broad scanning capacities allow surveillance to occur in both public and private spaces, without the knowledge of targeted individuals. However, the specific technical capabilities of these tools (e.g., range, interception capabilities, data storage) are not detailed in the official documents.

Between 2016 to 2022, RAB had sought or attended training for a range of catchers and tactical data interception units under a project titled "Capacity Building of RAB Forces in Technological Aspects."[37] Other official documents from the Ministry of Home Affairs show the involvement of the police forces in similar activities. Bangladeshi military intelligence officers also reportedly traveled to Hungary to receive technical training from Israeli experts.[38] Further evidence of imported mobile surveillance is found in trade records and investigative reporting from Cyprus, a known hub for surveillance technology re-export.[39] Another company, Coralco Tech—reportedly based in Singapore but linked to Israel—provided equipment for "active monitoring of mobile phones" to the Bangladeshi military in 2019 at an approximate cost of USD 1.6 million.[40] Agencies like the Bangladeshi Police and RAB, as well as the Ministry of Home Affairs, were

[36] Ministry of Home Affairs. (2017-2022). Government Order. Government of People's Republic of Bangladesh. <https://archive.org/details/back-pack-imsi-monitor-location-finder-tuning-antenna-canada-2019_202508>.

[37] See, for example, Ministry of Home Affairs. (2024). Annual Procurement Plan 2024/2025. Government of People's Republic of Bangladesh. <https://www.police.gov.bd/storage/upload/announcement/O2xt7F4nFl36ATnGX0vgaoD3dJXV6bHUhgMYn9Xj.pdf>; Ministry of Home Affairs. (2023). Annual Procurement Plan 2023/2024. Government of People's Republic of Bangladesh. <https://www.police.gov.bd/storage/upload/announcement/UG74eJMUBETeQrr0fHz2D5jAGDAfge1m7bCWtNWM.pdf>; Ministry of Home Affairs. (2022). Government Order. Government of People's Republic of Bangladesh. <https://mhapsd.gov.bd/sites/default/files/files/mhapsd.portal.gov.bd/notification_circular/39519a9e_9403_48b1_9f5b_c2c8f784b7b5/358.pdf>; Ministry of Home Affairs. (2023). Government Order. Government of People's Republic of Bangladesh. <https://mhapsd.gov.bd/sites/default/files/files/mhapsd.portal.gov.bd/divisional_noc/4c5a974d_6b1e_4943_86e8_2053a4d0335a/433.pdf>; Ministry of Home Affairs. (2025). Government Order. Government of People's Republic of Bangladesh. <https://mhapsd.gov.bd/sites/default/files/files/mhapsd.portal.gov.bd/divisional_noc/b648b9f7_03d6_42f6_b534_2b9443eee41c/96.pdf>.

[38] Al Jazeera Investigative Unit. (2021). Bangladesh bought hacking tools from Israel, documents show. <https://www.aljazeera.com/news/2021/3/8/bangladesh-bought-hacking-tools-from-israel-documents-show>; Al Jazeera Investigative Unit. (2021). Bangladesh bought Cellebrite phone-hacking tools from Israel. <https://www.ajiunit.com/article/bangladesh-cellebrite-phone-hacking-tools-israel/>.

[39] Yaron, O., & Khan, Z. S. (2023). Israeli spy tech sold to Bangladesh despite dismal human rights record. Haaretz. <https://www.haaretz.com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-bangladesh-despite-dismal-human-rights-record/00000185-9692-d16a-a987-f6b75dd00000>; The Jerusalem Post. (2023). Israeli spyware and surveillance tools sold to Bangladesh. <https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-728100>.

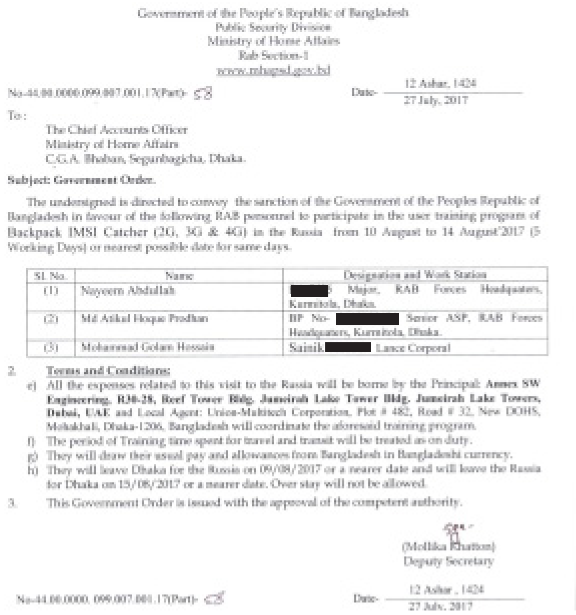
[40] Yaron, O., & Khan, Z. S. (2023). Israeli spy tech sold to Bangladesh despite dismal human rights record. Haaretz. <https://www.haaretz.

involved in most of these transactions.

The timeframe for these activities spans from 2017 to 2025, indicating ongoing procurement and training related to cyber surveillance tools in Bangladesh.

Procuring Entity	Year	Tender Details
Bangladesh Police	2018	An invitation for tender (reference no.: 44.01.0000.022.10.002.18.01, date: July 8, 2018) was issued for the procurement of IMSI Monitor/ Mobile Tracker and Back Pack IMSI Monitor/Location Finder. Tender was closed on November 30, 2018.
	2018-19	A re-tender (reference no.: 44.01.0000.022.10.002.18/22 (2018-19), date: December 5, 2018) was issued for the above items. Tender was closed on January 3, 2019.
	2019	A Factory Acceptance Test (FAT) for shipment of four pieces of Back Pack IMSI Monitor/Location Finder was scheduled in Canada from June 15 to 21, 2019. Another FAT for the shipment of two units of IMSI Monitor/Mobile Tracker was planned in Germany from 15 to 21 September, 2019.
	2025	An invitation for international tender (memo no.: 44.01.0000.453.07.442.24/329, date: January 30, 2025) was issued for the supply of Wide Terrain Searching Tool and Backpack Network Analyzer.
RAB	2017	A Government Order sanctioned the participation of RAB personnel in a user training program of Backpack IMSI Catcher (2G, 3G & 4G) in Russia from August 10 to 14, 2017.
	2019	A re-tender (tender package no.: G-10(T)/2018-2019, date: April 10, 2019) was issued for the procurement of Backpack IMSI Catcher. Tender was closed on May 12, 2019.
	2022	A tender for the procurement of Backpack IMSI Catcher (date: March 9, 2022) was issued with a closing date of April 21, 2022.
	2022	A Government Order approved officials to participate in foreign training on the Backpack IMSI Catcher System in the United Kingdom from October 24 to 29, 2022.
	2017-19	A number of training programs on IMSI catchers were conducted in Russia in 2017, in Canada and Germany in 2019, and the United Kingdom in 2022. These programs involved user training, pre-shipment inspections (PSI), and FATs.

com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-bangladesh-despite-dismal-human-rights-record/00000185-9692-d16a-a987-f6b75dd00000>; The Jerusalem Post. (2023). Israeli spyware and surveillance tools sold to Bangladesh. <https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-728100>; Times of Israel. (2023). Israeli-owned firms reportedly selling spyware to Bangladesh with no oversight. <https://www.timesofisrael.com/israeli-owned-firms-reportedly-selling-spyware-to-bangladesh-with-no-oversight/>; European Parliament. (2023). Draft results of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (Report A9-0189/2023). European Parliament. <https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html>



Government of the People's Republic of Bangladesh
Public Security Division
Ministry of Home Affairs
Rab Section-1
www.mhapsd.gov.bd

No-44.00.0000.099.007.001.17(Part)- 58　　　Date- 12 Ashar, 1424 / 27 July, 2017

To :

The Chief Accounts Officer
Ministry of Home Affairs
C.G.A. Bhaban, Segunbagicha, Dhaka.

Subject: Government Order.

The undersigned is directed to convey the sanction of the Government of the Peoples Republic of Bangladesh in favour of the following RAB personnel to participate in the user training program of Backpack IMSI Catcher (2G, 3G & 4G) in the Russia from 10 August to 14 August'2017 (5 Working Days) or nearest possible date for same days.

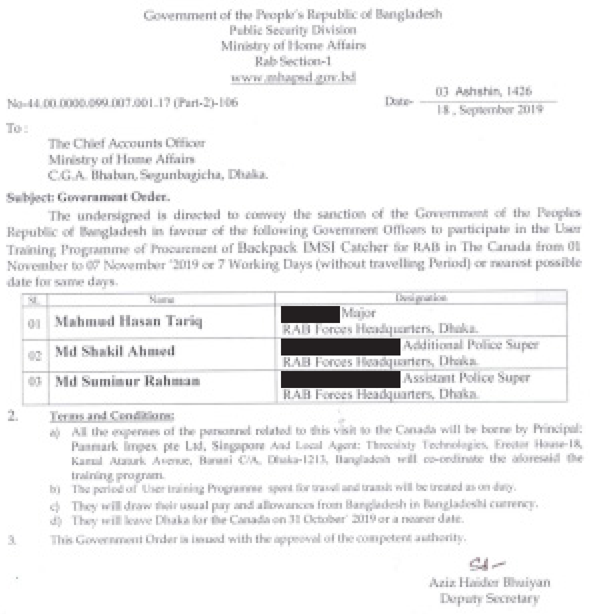
Sl. No.	Name	Designation and Work Station
(1)	Nayeem Abdullah	[redacted] Major, RAB Forces Headquaters, Kurmitola, Dhaka.
(2)	Md Atikul Hoque Prodhan	BP No- [redacted] Senior ASP, RAB Forces Headquaters, Kurmitola, Dhaka.
(3)	Mohammad Golam Hossain	Sainik [redacted] Lance Corporal

2. Terms and Conditions:
e) All the expenses related to this visit to the Russia will be borne by the Principal: **Annex SW Engineering, RJ0-28, Reef Tower Bldg. Jumeirah Lake Tower Bldg. Jumeirah Lake Towers, Dubai, UAE** and Local Agent: Union-Multitech Corporation, Plot # 482, Road # 32, New DOHS, Mohakhali, Dhaka-1206, Bangladesh will coordinate the aforesaid training program.
f) The period of Training time spent for travel and transit will be treated as on duty.
g) They will draw their usual pay and allowances from Bangladesh in Bangladeshi currency.
h) They will leave Dhaka for the Russia on 09/08/2017 or a nearer date and will leave the Russia for Dhaka on 15/08/2017 or a nearer date. Over stay will not be allowed.

3. This Government Order is issued with the approval of the competent authority.

(Mollika Khatun)
Deputy Secretary

No-44.00.0000. 099.007.001.17(Part)- 58　　　Date- 12 Ashar , 1424 / 27 July, 2017



Government of the People's Republic of Bangladesh
Public Security Division
Ministry of Home Affairs
Rab Section-1
www.mhapsd.gov.bd

No-44.00.0000.099.007.001.17 (Part-2)-106　　　Date- 03 Ashshin, 1426 / 18 , September 2019

To :

The Chief Accounts Officer
Ministry of Home Affairs
C.G.A. Bhaban, Segunbagicha, Dhaka.

Subject: Govrnament Order.

The undersigned is directed to convey the sanction of the Government of the Peoples Republic of Bangladesh in favour of the following Government Officers to participate in the User Training Programme of Procurement of Backpack IMSI Catcher for RAB in The Canada from 01 November to 07 November '2019 or 7 Working Days (without travelling Period) or nearest possible date for same days.

SL	Name	Designation
01	**Mahmud Hasan Tariq**	[redacted] Major RAB Forces Headquarters, Dhaka.
02	**Md Shakil Ahmed**	[redacted] Additional Police Super RAB Forces Headquarters, Dhaka.
03	**Md Suminur Rahman**	[redacted] Assistant Police Super RAB Forces Headquarters, Dhaka.

2. Terms and Conditions:
a) All the expenses of the personnel related to this visit to the Canada will be borne by Principal: Panmark Impex pte Ltd, Singapore And Local Agent: Threesixty Technologies, Erector House-18, Kamal Ataturk Avenue, Banani C/A, Dhaka-1213, Bangladesh will co-ordinate the aforesaid the training program.
b) The period of User training Programme spent for travel and transit will be treated as on duty.
c) They will draw their usual pay and allowances from Bangladesh in Bangladeshi currency.
d) They will leave Dhaka for the Canada on 31 October' 2019 or a nearer date.

3. This Government Order is issued with the approval of the competent authority.

Aziz Haider Bhuiyan
Deputy Secretary

2. Vehicle Mounted Mobile and Data Interceptor

Vehicle-mounted mobile and data interceptors can intercept communications and data from mobile devices within a targeted area. Deployed from a vehicle, these systems can mimic cell towers to capture calls, messages, and other digital communications, as well as track device locations. They may have the capabilities to track conversations, messages, photos and videos, including those on unencrypted services like Viber. Their mobility enables rapid deployment to different locations, supporting both targeted and wide-area monitoring without the need for fixed infrastructure. The system was reportedly acquired to enhance surveillance capabilities of NTMC.[41]

Various public procurement documents from BPPA and Ministry of Home Affairs, as well as investigative reports from Haaretz, show instances of procurement and related activities involving vehicle mounted mobile interceptors and vehicle mounted data interceptors equipment by NTMC.[42] The documents primarily reference the procurement and training related to "Vehicle Mounted Mobile Interceptors" and "Vehicle Mounted Data Interceptors" along with "Related Services," involving multiple entities. For instance, Mobileum, Inc. organized training on "Vehicle Mounted Data Interceptor and Related Services."[43] Another company, Toru Group, was involved in organizing proof of concept (POC) and admin training for vehicle mounted mobile interceptors in Greece.[44] One document from the Ministry of Home Affairs addresses the extension of visas for three Indian nationals working on the "Vehicle Mounted

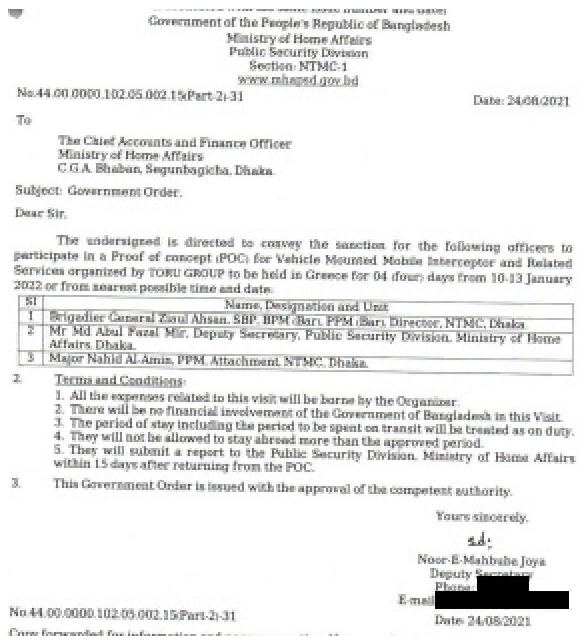
[41] Chowdhury, K. R. (2021). Bangladesh says it is buying mobile-phone interceptor to boost national security. BenarNews. <https://www.benarnews.org/english/news/bengali/bangladesh-monitoring-equipment-06102021154009.html>.

[42] Yaron, O., & Khan, Z. S. (2023). Israeli spy tech sold to Bangladesh despite dismal human rights record. Haaretz. <https://www.haaretz.com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-bangladesh-despite-dismal-human-rights-record/00000185-9692-d16a-a987-f6b75dd00000>; Yaron, O., & Khan, Z. S. (2023). In response to Haaretz investigation, Bangladesh says it made no 'direct' purchases of spytech from Israel. Haaretz. <https://www.haaretz.com/israel-news/security-aviation/2023-01-11/ty-article/.premium/bangladesh-says-it-made-no-direct-purchases-of-cybersecurity-from-israel/00000185-a153-d69c-abc5-b55b77070000>.

[43] Public Security Division, Ministry of Home Affairs. (2022). Government Order. Government of People's Republic of Bangladesh. <https://archive.org/details/vehicle-mounted-data-interceptor-copy/Vehicle%20Mounted%20Data%20Interceptor/>.

[44] Public Security Division, Ministry of Home Affairs. (2021). Government Order. Government of People's Republic of Bangladesh. <https://

Mobile Interceptor and Related Service Project," although the scope and timeline of their engagement remains unclear. Another letter dated January 11, 2021, details the visa extension process and requirements for further extensions. Activities included PSI, POC, and admin training, suggesting a comprehensive procurement process including evaluation, deployment, and user training. These documents indicate international collaboration and the presence of non-nationals in surveillance projects.



Government of the People's Republic of Bangladesh
Ministry of Home Affairs
Public Security Division
Section: NTMC-1
www.mhapsd.gov.bd

No.44.00.0000.102.05.002.15(Part-2)-31 Date: 24/08/2021

To

The Chief Accounts and Finance Officer
Ministry of Home Affairs
C.G.A. Bhaban, Segunbagicha, Dhaka.

Subject: Government Order.

Dear Sir,

The undersigned is directed to convey the sanction for the following officers to participate in a Proof of concept (POC) for Vehicle Mounted Mobile Interceptor and Related Services organized by TORU GROUP to be held in Greece for 04 (four) days from 10-13 January 2022 or from nearest possible time and date:

Sl	Name, Designation and Unit
1	Brigadier General Ziaul Ahsan, SBP, BPM (Bar), PPM (Bar), Director, NTMC, Dhaka.
2	Mr Md Abul Fazal Mir, Deputy Secretary, Public Security Division, Ministry of Home Affairs, Dhaka.
3	Major Nahid Al-Amin, PPM, Attachment, NTMC, Dhaka.

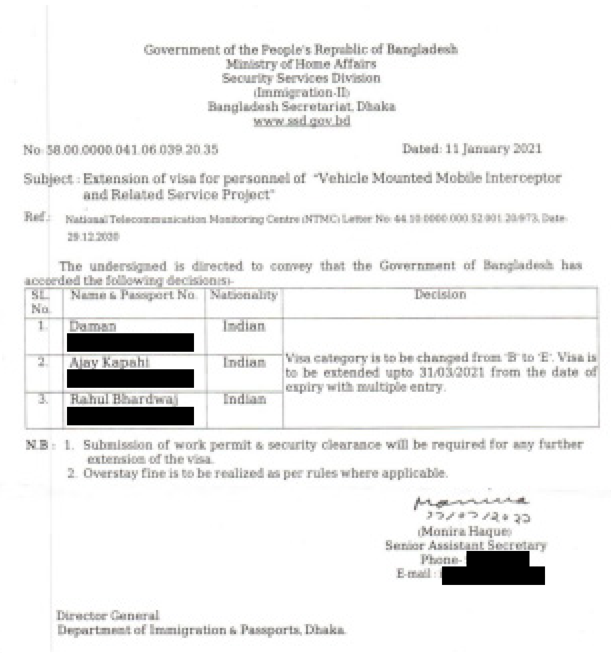
2. Terms and Conditions:
   1. All the expenses related to this visit will be borne by the Organizer.
   2. There will be no financial involvement of the Government of Bangladesh in this Visit.
   3. The period of stay including the period to be spent on transit will be treated as on duty.
   4. They will not be allowed to stay abroad more than the approved period.
   5. They will submit a report to the Public Security Division, Ministry of Home Affairs within 15 days after returning from the POC.

3. This Government Order is issued with the approval of the competent authority.

Yours sincerely,
s.d;
Noor-E-Mahbuba Joya
Deputy Secretary
Phone: [redacted]
E-mail [redacted]

No.44.00.0000.102.05.002.15(Part-2)-31 Date: 24/08/2021

Copy forwarded for information and



Government of the People's Republic of Bangladesh
Ministry of Home Affairs
Security Services Division
(Immigration-II)
Bangladesh Secretariat, Dhaka
www.ssd.gov.bd

No: 58.00.0000.041.06.039.20.35 Dated: 11 January 2021

Subject : Extension of visa for personnel of "Vehicle Mounted Mobile Interceptor and Related Service Project"

Ref.: National Telecommunication Monitoring Centre (NTMC) Letter No: 44.10.0000.000.52.001.20.973, Date: 29.12.2020

The undersigned is directed to convey that the Government of Bangladesh has accorded the following decision(s):-

SL. No.	Name & Passport No.	Nationality	Decision
1.	Daman [redacted]	Indian	Visa category is to be changed from 'B' to 'E'. Visa is to be extended upto 31/03/2021 from the date of expiry with multiple entry.
2.	Ajay Kapahi [redacted]	Indian	
3.	Rahul Bhardwaj [redacted]	Indian	

N.B : 1. Submission of work permit & security clearance will be required for any further extension of the visa.
2. Overstay fine is to be realized as per rules where applicable.

১১/০১/২০২১
(Monira Haque)
Senior Assistant Secretary
Phone- [redacted]
E-mail : [redacted]

Director General
Department of Immigration & Passports, Dhaka.

mhapsd.portal.gov.bd/sites/default/files/files/mhapsd.portal.gov.bd/notices/eff06988_f582_468d_8eef_d3ed0b49acda/31.pdf>; Public Security Division, Ministry of Home Affairs. (2021). Government Order. Government of People's Republic of Bangladesh. <https://mhapsd.gov.bd/sites/default/files/files/mhapsd.portal.gov.bd/notices/57335304_ebc5_4118_bcac_0136432c9e40/30.pdf>. See also Executive Committee of the National Economic Council. (2021). Meeting Minutes. Government of People's Republic of Bangladesh. <https://storage.googleapis.com/haaretz-cms-prod/ef/a0/3a8d481640c7b6156e04c6487a83/%D7%94%D7%97%D7%9C%D7%98%D7%AA-%D7%A7%D7%91%D7%99%D7%A0%D7%98-%D7%A8%D7%9B%D7%99%D7%A9%D7%AA-%D7%98%D7%95%D7%A8%D7%95-2021-%D7%91%D7%91%D7%A0%D7%92%D7%9C%D7%93%D7%A9%D7%99%D7%AA.pdf>.

Furthermore, NTMC appears to be the central agency involved in the acquisition and operation of these interceptors, with its personnel participating in training and inspection activities. The Public Security Division of the Ministry of Home Affairs oversaw the procurement and training activities, issuing government orders for participation in international training and inspections. According to records, the training and inspections occurred in Greece and Belgium, indicating engagement with international vendors, including Mobileum, Inc. and Toru Group. Toru Group was reportedly found to have ties with Israel,[45] acting as an intermediary to sell spyware to Bangladeshi clients.

Dates	Training
January 11, 2021	One document from the Ministry of Home Affairs addresses the extension of visas for three Indian personnel working on the Vehicle Mounted Mobile Interceptor and Related Service Project, signalling international collaboration for capacity building within Bangladesh.
August 24, 2021	Government Order issued for a POC in Greece scheduled for January 10-13, 2022.
September 8, 2021	Government Order issued for PSI in Greece scheduled for October 15-19, 2021.
February 3, 2022	Government Order issued for training in Greece scheduled for February 21-27, 2022.
April 11, 2022	Government Order issued for training in Belgium scheduled for May 23-31, 2022.

The training documents primarily focus on approvals and travel arrangements with little indication of technical specifications or operational capabilities of the tools. Even though the documents require attendees to submit a report to the Public Security Division, it remains unclear what training was conducted, as there is no publicly available record detailing their content, scope, or outcomes. Moreover, the term "Related Services" is not defined, making it difficult to understand the full scope of the surveillance activities

3. Voice and Data Interception System

Voice and data interception surveillance systems can monitor, capture, and record voice communications and digital data transmitted over telecommunication networks. Such systems may intercept phone calls, text messages, and internet traffic in real time, and can be used to track communication patterns, extract content, or analyze metadata.

Public documents reveal several procurement involving mobile voice and data intercept systems and related technologies primarily by NTMC. Most documents are official orders from the government, including the Ministry of Home Affairs. The documents outline the involved parties, training details, and financial responsibilities. For instance, in one set of documents, Yaana Technologies is identified as the entity providing training for the "Mobile Voice & Data Intercept system" and "Intelligence Platform & Target Profiling" supported by pre-

[45] Haaretz. (2023). Israeli spy tech sold to Bangladesh despite dismal human rights records. <https://www.haaretz.com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-bangladesh-despite-dismal-human-rights-record/00000185-9692-d16a-a987-f6b75dd00000>

shipment inspection (PSI). State actors, including the Ministry of Home Affairs and various associated agencies such as NTMC, Bangladesh Police, RAB, and NSI, are the recipients of the training, with officials from these agencies authorized to attend the training.[46] However, neither the specifics nor the technical capabilities of these tools (e.g., range, interception capabilities, data storage) are detailed in the official documents.

Dates	Training
August 5, 2019	Government Order for Mobile Voice & Data Intercept system training in Milpitas, California, USA, from September 16-20, 2019, or the nearest possible date.
November 20, 2019	Government Order for Intelligence Platform & Target Profiling training in Milpitas, California, USA, from December 16-20, 2019, or the nearest possible date.
May 13, 2018	Government Order for Pre-shipment Inspection training from May 28, 2018, or the nearest possible date.

[46] Public Security Division, Ministry of Home Affairs. (2018-2019). Government Order. Government of People's Republic of Bangladesh. <https://archive.org/details/b9e40ed9-5f63-4dcf-9f28-076eb9b19af3/yaana%20technologies.pdf>.

4. Wi-Fi Interceptors

Wi-Fi interceptors can detect, monitor, and capture data transmitted over wireless networks. It could, alone or in combination with other technologies, also identify connected devices, log browsing activity, collect unencrypted communications, and in some configurations, gain unauthorized access to networks or inject malicious code. RAB, NSI and Bangladesh Police are likely to have purchased these equipment.

The public procurement documents, including from websites of the Ministry of Home Affairs, the Prime Minister's Office, and BPPA, indicate that Wi-Fi interceptors and related systems have been a subject of procurement, import, and training activities for several law enforcement agencies in Bangladesh, including RAB and NSI, totalling around USD 16 million in purchases between 2015 and 2025. Several public procurement documents detail PSI for Wi-Fi interceptor systems. Officers from RAB conducted PSIs in the Netherlands in August 2018 and in Portugal in October 2018 for systems procured through EZY infotech Pte Ltd in Singapore and H.S Traders in Bangladesh. Separately, the Prime Minister's Office approved officers from NSI to conduct a PSI for a Wi-Fi interception system in Cyprus in April 2019, with expenses borne by Prelysis Communication & Information Systems Ltd.[47] The specific technical capabilities, such as range, detailed interception methods, or data analysis functionalities, are not elaborated upon in the official documents.

Additionally, the procurement documents contain records of training programs for the Wi-Fi interceptor systems. It notes that RAB personnel participated in user training programs in both the Netherlands in August and September 2018 and in Portugal in October 2018. These training programs, like the PSIs, were sponsored by the same vendors, who covered travel, accommodation, and food expenses.

These programs included user training and PSI, indicating a focus on ensuring proper functionality and operational readiness of the procured surveillance equipment.

Wi-Fi interceptors and related systems have been a subject of procurement, import, and training activities for several law enforcement agencies in Bangladesh, including RAB and NSI, totalling around USD 16 million in purchases between 2015 and 2025.

[47] Prime Minister's Office. (2019). Government Order. Government of People's Republic of Bangladesh. <https://archive.org/details/wi-fi-interception-system-by-prelysis-prime-ministers-office>; Public Security Division, Ministry of Home Affairs. (2018). Government Order. Government of People's Republic of Bangladesh. <https://archive.org/details/wi-fi-interceptor-in-the-netherlands/Wi-Fi%20Interceptor%20in%20The%20Netherlands>; Bangladesh Public Procurement Authority. (2023). Government of People's Republic of Bangladesh. <https://archive.org/details/wi-fi-interceptor-in-the-netherlands/Procurement%20of%20WI-FI%20INTERCEPTOR/>.

Procuring or Training Entity	Year	Tender and Training Details
RAB	2018	Government Order approved RAB personnel to participate in a PSI for the procurement of Wi-Fi Interceptor in Portugal from October 3 to 7, 2018.
	2018	Government Order approved RAB personnel for a PSI of the Wi-Fi Interceptor in the Netherlands from August 17 to 21, 2018.
	2018	Government Order approved RAB personnel to participate in a user training program for the Wi-Fi Interceptor in Portugal from October 10 to 22, 2018.
	2018	RAB personnel were approved for a user training program on the Wi-Fi Interceptor in the Netherlands from August 25 to September 6, 2018.
	2023	An invitation for tender (memo no.: RAB/INT/Project/2022-2023/4112316/104, date: April 26, 2023) was issued for the procurement of the Wi-fi Interceptor. The tender publication date was April 27, 2023, with a closing date of June 8, 2023. The tender document price was BDT 4,000, and the security amount was USD 43,000. The completion time was 120 months.
National Security Intelligence	2019	Government Order dated March 18, 2019, sanctioned NSI officers to participate in a PSI of the Wi-Fi Interception System in Cyprus from April 2 to April 8, 2019. The expenses for travel, accommodation, local transport, and meals for the officers were to be borne by the inviting institution, Prelysis Communication & Information Systems Ltd.
	2018-19	Other training and PSI were conducted in the Netherlands in 2018, in Portugal in 2018, and in Cyprus in 2019.

5. Spyware

Cellebrite UFED is understood to be capable of extracting, decoding, and analyzing data from a wide range of devices, including mobile phones, tablets, GPS units, and other storage media. It can reportedly bypass certain password protections and encryption to access stored information such as call logs, messages, contacts, application data, multimedia files, and location history. When used in conjunction with the UFED Physical Analyzer, the system can conduct more in-depth analysis, recover deleted content, and generate detailed forensic reports.

Public documents from the Ministry of Home Affairs and BPPA indicate that Bangladeshi state agencies have procured digital forensics tools, including Cellebrite UFED and associated Cellebrite UFED Physical Analyzer. The Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT) was involved in the planned procurement,[48] while Bangladesh Police were authorized by the Ministry of Home Affairs to undergo training for Cellebrite Certified Operator (CCO) and Cellebrite Certified Physical Analyst (CCPA) certifications, which relate to advanced data extraction and forensic analysis using the tools. Documents indicate that six police officers were authorized to participate in a training in Singapore in 2019.[49]

In 2018, a report by Citizen Lab revealed that Bangladesh was among 45 countries where Pegasus—the powerful spyware developed by Israeli cyber intelligence firm NSO Group—had been detected.[50] Pegasus is known for its ability to remotely access a target's smartphone, enabling covert surveillance of calls, messages, and even microphone and camera feeds. NSO Group has faced mounting international scrutiny and was sanctioned by the U.S. government in 2021 for enabling authoritarian regimes to "maliciously target" journalists, activists, and human rights defenders.[51]

Bangladesh's ties to Israeli-origin spyware run deeper. Our investigation found export documents from Cyprus—a known hub for intermediaries involved in surveillance tech transfers—show that another Israeli-owned firm, Coralco Tech, sold spyware worth an estimated USD 1.6 million to DGFI.[52] This technology reportedly allows for remote access and real-time eavesdropping on mobile phones, reinforcing state capacity for covert surveillance.

The same export records reveal that UTX Technologies, an Israeli surveillance company later acquired by Verint Systems, supplied multiple spyware systems to NTMC. In 2019, the firm sold a "web intelligence system" for USD 2 million, and in 2021, it provided a cellphone tracking system valued at USD 500,000.[53]

[48] Bangladesh Computer Council, Information & Communication Technology Division. (2023-2024). Annual Procurement Plan. Government of People's Republic of Bangladesh. <https://archive.org/details/ufed-cellibrite-annual-plan/page/n1/mode/2up>.

[49] Public Security Division, Ministry of Home Affairs. (2018). Government Order. Government of People's Republic of Bangladesh. <https://archive.org/details/ufed_20250810>.

[50] Citizen Lab. (2018). Tracking NSO Group's Pegasus Spyware Operations to 45 Countries. <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>

[51] U.S. Senate Foreign Relations Committee, Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy. (2024). Cyberspace under threat in the era of rising authoritarianism and global competition [Hearing Transcript]. U.S. Government Publishing Office. <https://www.congress.gov/118/chrg/CHRG-118shrg57143/CHRG-118shrg57143.pdf>; Marzocchi, O., & Mazzini, M. (2022). Pegasus and surveillance spyware. European Parliament. <https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA%282022%29732268_EN.pdf>; European Parliament. (2023). Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware. <https://www.europarl.europa.eu/doceo/document/PEGA-AM-742288_EN.pdf>.

[52] European Parliament. (2023). Draft results of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (Report A9-0189/2023). European Parliament. <https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html>; Yaron, O., & Khan, Z. S. (2023). Israeli spy tech sold to Bangladesh despite dismal human rights record. Haaretz. <https://www.haaretz.com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-bangladesh-despite-dismal-human-rights-record/00000185-9692-d16a-a987-f6b75dd00000>.

[53] European Parliament. (2023). Draft results of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (Report A9-0189/2023). European Parliament. <https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html>; Yaron, O., & Khan, Z. S. (2023). Israeli spy tech sold to Bangladesh despite dismal human rights record. Haaretz. <https://www.haaretz.com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-bangladesh-despite-dismal-human-rights-record/00000185-9692-d16a-a987-f6b75dd00000>.

These tools can monitor online behavior and geolocate mobile users.

Other Israeli firms, including Passitora, Prelysis, and Cognyte (a company also affiliated with Verint Systems),[54] have also been reportedly involved in selling spyware and surveillance technologies to Bangladesh, albeit through intermediary countries like Cyprus and Singapore.[55] These companies are part of a broader network of Israeli cyber intelligence exporters that have supplied spyware to dozens of authoritarian regimes worldwide,[56] contributing to the global expansion of invasive digital surveillance tools often used to suppress dissent, monitor civil society, and undermine press freedom.

Similarly, Turkish spyware firm, Bilgi Teknoloji Tasarım (BTT) used deceptive tactics to bypass export controls and sell surveillance tools like IMSI-catchers to Bangladesh. In the 2015 Hacking Team leaks, BTT was found selling spyware and other surveillance equipment to NTMC.[57] BTT was later acquired by a UAE firm in 2017 before shutting down.[58]

Separately, in 2019, BGD e-GOV CIRT was found to be actively using Oxygen Forensic Detective and BelkasoftX, which collectively have similar capabilities as Cellebrite, including accessing messaging apps data, cloud and system artifacts.[59] These highlight the state's broader efforts to institutionalize spyware within the broader surveillance architecture.

Procuring or Training entity	Year	Tender and Training Details
BCC	2023	BCC, under the Information and Communication Technology Division, planned the procurement of Computer Software Cellebrite UFED Physical Analyser & 4pc for BGD e-GOV CIRT in September 2023.
Ministry of Home Affairs	2019	The Ministry of Home Affairs approved police officers to attend CCO and CCPA courses in Singapore in February 2019, which was originally scheduled for December 2018.
		The documents show training programs related to Cellebrite tools in Singapore in 2019 for Bangladesh Police. Activities related to UFED Cellebrite includes training in 2019 and planned procurement in 2023-2024, indicating ongoing investment and use of these spyware.

[54] Atlantic Council. 2024. Mythical Beasts and where to find them: Mapping the global spyware market. <https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/>

[55] The Jerusalem Post. (2023). Ex-Israeli intel cyber experts tied to Bangladesh military spyware deals. <https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-728100>; European Parliament. (2023). Draft results of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (Report A9-0189/2023). European Parliament. <https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html>; Yaron, O., & Khan, Z. S. (2023). Israeli spy tech sold to Bangladesh despite dismal human rights record. Haaretz. <https://www.haaretz.com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-bangladesh-despite-dismal-human-rights-record/00000185-9692-d16a-a987-f6b75dd00000>.

[56] European Parliament. (2023). Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware.

[57] Burgess, M. (2023). A spy agency leaked people's data online—then the data was stolen. Wired. <https://www.wired.com/story/ntmc-bangladesh-database-leak/>; Intelligence Online. (2022). IKON: The new face of Turkish-Singaporean interception software specialist BTT. Intelligence Online. <https://www.intelligenceonline.com/surveillance--interception/2022/11/15/ikon-the-new-face-of-turkish-singaporean-interception-software-specialist-btt,109864719-gra>; Oliveira, F. (n.d.). Intelligence. Retrieved from <https://www.filipeoliveira.pt/intelligence>.

[58] Wired. (2015). Hacking Team leak shows how secretive zero-day exploit sales work. <https://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/>

[59] BGD e-Gov CIRT. (2019). Extracting and analyzing Messenger data with Oxygen Forensics. <https://archive.md/ptRHf>.

6. Web Analytics Tools

Web analytics tools are software applications used to collect, measure, and analyze data on how users interact with websites and online platforms. They can track metrics such as visitor numbers, geographic location, device type, browsing behavior, and time spent on specific pages. While commonly used for improving website performance and user experience, these tools can also be leveraged for monitoring individuals' online activities, building detailed profiles, and identifying patterns of behavior. Documents from the Ministry of Home Affairs and BPPA show Bangladesh Police and BGD e-GOV CIRT have both invested in web intelligence, investigation systems, and web analytics tools.[60]

Procuring or Training entity	Year	Tender and Training Details
Bangladesh Police, CTTC	2024	The Bangladesh Police, specifically CTTC, is actively involved in procuring Web Intelligence & Investigation System-mid Level Capacity. This is evidenced by invitation for tender in February 2024 and a re-tender in May 2024 for the systems, with a security deposit of BDT 45,00,000. These procurements are funded by the Development Budget of the Government of Bangladesh.
Bangladesh e-GOV CIRT	2023	BGD e-GOV CIRT, under the Information and Communication Technology Division, has ongoing plans for the procurement of Computer Software Web Analytics Tools for BGD e-GOV CIRT. A corrigendum notice in April 2023 indicates adjustments to tender dates for such software. Additionally, the annual procurement plan for the Strengthening of BGD e-GOV CIRT project outlines a planned procurement for Supply & Installation of Computer Software Web Analytics Tools with an estimated cost of BDT 50,000,000 (or USD 410,000).
		BCC's annual procurement plan for 2022-23 for the Strengthening of BGD e-GOV CIRT project also includes various other computer software procurements. These include: • Threat Intelligence Solution • Access Data FTK • Guidance Encase Forensic • CIS CAT Pro • Digital Forensic Bundle • IXIA Breaking Point • AppScan • Acunetix for vulnerability assessment and penetration testing These procurements are generally for licensing, installation, and renewal of software necessary for digital forensics and cybersecurity infrastructure, however, can significantly strengthen remote eavesdropping, hacking and data extraction capabilities.

[60] Bangladesh Police, Ministry of Home Affairs. (2024). Invitation for Re-Tender. Government of People's Republic of Bangladesh. <https://archive.org/details/ministry-of-home-affairs>; Bangladesh Public Procurement Authority. (2024). Government of People's Republic of Bangladesh. <https://archive.org/details/procurement-of-web-intelligence-investigation-system-u-tx-tech>;

7. Location Based Social Network Monitoring System

A location-based social network monitoring system is capable of collecting and analyzing data from social media platforms to track user activity in connection with specific geographic locations. Such systems may aggregate geotagged posts, profile information, and network connections to identify individuals, map social interactions, and monitor events in real time. It functions more as an open-source intelligence surveillance system, but when paired with location data, it becomes a powerful mass surveillance tool capable of tracking individuals or groups based on their online speech, associations, and whereabouts.

Between 2015 and 2025, Bangladeshi intelligence and security agencies appeared to have cumulatively spent nearly USD 20 million on software and equipment that can collect, transfer, and retain location data. In late 2018, RAB initiated the procurement of a surveillance tool referred to as “Location-Based Social Network Monitoring System Software.” According to public procurement records, this process was formalized through an invitation for tender issued in November 2018. The procurement was funded through the Government of Bangladesh’s Development Budget for a total budget of BDT 300,000.[61] Further, a government order from April 2019 sanctioned two RAB officers to participate in a user training program in the United States from April 9 to 15, 2019.[62] The expenses for this training were to be borne by H.S Traders. This indicates a focus not only on acquiring the technology but also on ensuring that personnel are adequately trained in its operation.

8. GSM/UMTS Vehicular Active Support System

A GSM/UMTS vehicular active support system is a mobile surveillance platform, typically installed in a vehicle, capable of actively interacting with 2G and 3G mobile networks to intercept, monitor, and analyze communications within its range. Such systems may mimic legitimate cell towers to collect device identifiers (such as IMSI linked to a SIM card or the International Mobile Equipment Identity (IMEI) linked to the handset), track mobile phone locations, and, in some configurations, capture voice calls, text messages, and other data. Their mobility allows for flexible deployment across different geographic areas. RAB and Bangladesh Police have both invested substantially in vehicular active support systems, with RAB continuing purchases and sending officials for training as recently as February 2025.

Public procurement records reveal that RAB initiated the purchase of a GSM/UMTS Vehicular Active Support System to expand its surveillance and interception capabilities. The procurement followed an open tendering process, with RAB listed as both the procuring agency and end user. Notably, in February 2025, twelve officials from Public Security Division and RAB were authorized to travel to Turkey for a 10-day training program on operating mobile surveillance units with Threesixty Technologies covering all costs of training,[63] suggesting its involvement as a likely supplier or strategic partner in the deployment of the system. The procurement documents cover a timeframe from 2021 to 2025, detailing the progression from initial tender invitations to planned international training.

[61] Bangladesh Public Procurement Authority. (2018). Government of People’s Republic of Bangladesh. <https://archive.org/details/bppa-location-based-social-network-monitoring-system-software-by-rab>.

[62] Public Security Division, Ministry of Home Affairs. (2019). Government Order. Government of People’s Republic of Bangladesh. <https://archive.org/details/location-based-social-network-monitoring-system-software-for-rab>.

[63] Public Security Division, Ministry of Home Affairs. (2025). Government Order. Government of People’s Republic of Bangladesh. <https://archive.org/details/gsmtumts-vehicular-active-support-system-by-rab-2025>.

Procuring or Training Entity	Year	Tender and Training Details
RAB	2021	An invitation for tender was published on March 7, 2021, with a closing date of April 19, 2021. The tender package was named Procurement of GSM UMTS Vehicular Active Support System and had a security amount of USD 129,000. The procuring entity was RAB and the tender was managed by the Intelligence Wing of RAB Forces Headquarters.
	2023	A corrigendum issued on March 7, 2023, for the GSM/UMTS Vehicular Active Support System tender extended the bid deadline to April 25, with a total value of USD 34,000.
Ministry of Home Affairs, RAB	2025	Government Order dated February 26, 2025, approved the participation of 12 officials from the Public Security Division and RAB in a 10-day training program on the GSM/UMTS Vehicular Active Support System in Turkey. The training was scheduled from March 8 to 18, 2025. All expenses for this training was to be borne by Threesixty Technologies.

9. Drone Surveillance

Drone surveillance refers to the use of unmanned aerial vehicles (UAVs) equipped with cameras, sensors, or other monitoring equipment to conduct aerial observation and data collection. Such systems can capture high-resolution video and still imagery, track movements, monitor events or gatherings, and in some configurations, employ real-time facial recognition, thermal imaging, or signal interception tools. Their mobility and ability to access hard-to-reach areas make them highly adaptable for both targeted and wide-area monitoring, enabling authorities to observe public gatherings, track individuals, and conduct aerial reconnaissance.

Procurement documents from BPPA, including tender invitations and corrigenda from 2022 and 2023, reveal RAB's ongoing efforts to acquire drone surveillance technology. These documents detail the bidding process, eligibility requirements, security deposits, and training components, indicating a structured plan to integrate drones into RAB's operations.[64] The inclusion of training in the procurement process suggests RAB's intention not only to acquire the technology but to operationalize it effectively as part of its broader surveillance infrastructure.

Although confirmed records could not be found, Turkish firms like Bilgi Teknoloji Tasarım (BTT), could likely be linked with selling drones to Bangladesh.

[64] Bangladesh Public Procurement Authority. (2022-23). Government of People's Republic of Bangladesh. <https://archive.org/details/surveillance-by-drone-rab>. See also Public Security Division, Ministry of Home Affairs. (2023). Government Order. <https://archive.org/details/training-on-surveillance-by-drone-rab>.

Procuring or Training Entity	Year	Tender and Training Details
RAB	2023	Tenders highlight the government‘s approval for RAB officials to participate in international training programs focused on *Surveillance by Drone* .One specific instance details a-6 day training session in Dubai ,UAE ,in December ,2023 with expenses covered by the organizer.
RAB	2018-21	The procurement of drone surveillance tools is part of a larger project titled*" Enhancement of Technical and Technological Capability of RAB* ",approved by *ECNEC* in November.2018 With an estimated budget of BDT 3.17 billion ,the project aims to boost RAB‘s surveillance capacity through various advanced technologies ,including Wi-Fi interceptors ,backpack IMSI catchers ,robotic surveillance systems ,long-range laser audio devices ,and *Cellebrite* tools .A document from May 2020 confirms the project‘s implementation timeline from November 2019 ,1 to June.2021 ,30

10. Laser Listening Device

A laser listening device is a surveillance tool understood to be capable of capturing audio from a distance by detecting vibrations on surfaces such as windows. It works by directing a laser beam at the target surface, where sound waves cause microscopic vibrations; the reflected beam is then converted into an audio signal. In real time, such systems can enable covert monitoring of conversations taking place inside secured or private spaces without the need for physical entry, making it useful for covert operations. In environments where activists, human rights defenders, or journalists meet in safe spaces or at their homes, laser microphones enable listening from a distance of up to 300 meters without having to access any individual device. According to BPPA records, RAB issued an open tender on March 7, 2018, for the procurement of a Laser Listening Device.[65]

11. Electronic and Social Media Surveillance, and Dark Web Monitoring

Electronic and social media surveillance involves a suite of software platforms and analytical tools to monitor, collect, and analyze online communications and activities across websites, messaging applications, and social networking platforms. Such systems may track posts, monitor user interactions, identify emerging narratives, and flag specific keywords, images, or behavioral patterns. In some configurations, they are reportedly capable of real-time monitoring and mapping of social networks, allowing authorities to identify individuals or groups of interest.

Over the last few years, the government turned its attention to surveillance of social media and online content, given the growing importance of digital platforms in political discourse. In 2015, RAB reportedly paid Snaptrends, an analytics firm that sells stripped down Twitter data to law enforcement, approximately USD 115,000 for the software and associated training.[66] For years, Twitter has offered access to Firehose—where

[65] Bangladesh Public Procurement Authority. (2018). Government of People's Republic of Bangladesh. <https://archive.org/details/bppa-laser-listening-device-by-rab-2018>.

[66] Bloomberg. (2015). How despots use Twitter to hunt dissidents. <https://www.bloomberg.com/news/articles/2016-10-27/twitter-s-fire-

a sample of half a billion tweets per day is available and accompanied with roughly 30 or so data points—accessible to select social media analytics firms. While most firms offer this information to marketers, some, like Snaptrends, sell to governments and law enforcement, usually during moments of social unrest.

Subsequently in 2018, NTMC announced plans to procure a Social Media Monitoring System (Open Source Intelligence) and related services, reportedly at a cost of BDT 236 crore.[67] This system was intended to scan and analyze public content on Facebook, X (formerly Twitter), YouTube and other platforms to identify "rumors" or "subversive" content. By late 2019, under a project named Cyber Threat Detection and Response, the Department of Telecommunications had reportedly initiated trials for a nationwide system enabling real-time filtering of online content.[68] Details of the chosen solution are scarce, and it remains unclear whether the technology was acquired or used.

In 2019, UAE-based cybersecurity firm, Spider Digital, sold SSL Decryption Platform to NTMC for just over USD 200,000. An SSL decryption platform is a system or tool that intercepts and decrypts SSL/TLS-encrypted internet traffic so that it can be inspected, monitored, or analyzed before being re-encrypted and sent on its way.

Since most modern web traffic is encrypted (HTTPS), normal network monitoring tools cannot see the actual content being transmitted. An SSL decryption platform solves that by temporarily breaking the encryption, allowing surveillance agencies to examine the data. It is often installed at an ISP- or provider level. By 2023, Spider Digital announced they now are supplying "data monitoring tools" to government agencies across Asia that can be deployed without the user's knowledge.[69]

Various public documents and government orders also approved the participation of Bangladeshi security officials in international seminars focused on electronic surveillance, social media and dark web monitoring, and cybercrime investigations. It shows officials, particularly from NTMC, the Ministry of Home Affairs, and various police units, attending ISS World seminars. These seminars have taken place in locations such as Washington D.C., USA in 2019 and Dubai, UAE in 2021 and 2024.[70]

Training documents attributed to a number of agencies indicate a government-wide focus on enhancing capabilities related to monitoring digital communications and investigating cyber-related offenses. In some instances, the expenses for training are borne by the seminar organizer or a system and service provider (e.g., Spider Digital). The government orders also outline terms and conditions, such as the attendees being "on duty" during the travel and seminar period, and the requirement to submit a report upon their return. This indicates that the government officially sanctioned the training or seminar, treating it as part of the officials' formal responsibilities.

hose-of-tweets-is-incredibly-valuable-and-just-as-dangerous>

[67] Acharjee, D. (2018). Social media to come under surveillance. The Independent. <https://web.archive.org/web/20180613180511/https://www.theindependentbd.com/post/153852>.

[68] Islam, M. Z. (2019). Govt can now filter online contents. The Daily Star. <https://www.thedailystar.net/frontpage/bangladesh-govt-can-now-monitor-block-filter-online-facebook-contents-1802497>; Human Rights Watch. (2020). Bangladesh: Online surveillance, control <https://www.hrw.org/news/2020/01/08/bangladesh-online-surveillance-control>.

[69] Newsfile. (2023). Spider Digital announces the launch of its data monitoring platform 'Sasha' for government institutions across Asia. <https://www.newsfilecorp.com/release/151741/Spider-Digital-Announces-the-Launch-of-Its-Data-Monitoring-Platform-Sasha-for-Government-Institutions-Across-Asia>.

[70] Public Security Division, Ministry of Home Affairs. (2019-2024). Government Order. Government of People's Republic of Bangladesh. <https://archive.org/details/electronic-surveillance-social-media-monitoring/Electronic%20Surveillance%2C%20Social%20Media%20monitoring.pdf>.

12. Integrated Lawful Interception System

An integrated lawful interception system (ILIS) is a centralized platform that enables law enforcement and intelligence agencies to monitor, collect, and analyze communications and data from telecommunications networks in real time. Such systems may integrate multiple interception capabilities—such as voice, text, internet traffic, and metadata collection—into a single operational interface, often linked directly to service providers' infrastructure. Multiple public statements by government officials, including the former Minister of Home Affairs, confirm that the NTMC has procured and deployed ILIS. Import and procurement records, in addition to media reporting,[71] show at least USD 51.734 million spent on ILIS, sourced from several companies, most prominently Yanna Technologies, Intersec and Verint Systems.

Government procurement documents show that NTMC officials have traveled abroad to procure and train on interception systems multiple times. For example, five officers from NTMC received approval to travel to San Francisco, USA, to participate in the integrated lawful interception system procurement related training in November 2017. Other documents detail three officers from NTMC receiving approval to travel to California, USA to attend a "technical discussion regarding the procurement of an integrated lawful interception system" in October 2018.[72]

Ahead of the 2024 election, the government was reportedly set to deploy a mobile phone surveillance system that empowers law enforcement and intelligence agencies to track users' exact locations and access sensitive personal information. According to reports, this surveillance system, Integrated Lawful Interception System, has the capacity to link all internet service providers, international internet gateways, national internet exchange service providers, and mobile operators to a system of the government agencies.[73] President Abdul Hamid, in his addresses to the nation in 2018 and 2023 ahead of the national elections, acknowledged NTMC's active engagement in digital surveillance, noting its implementation of the Integrated Lawful Interception System to enable data and voice interception, as well as the use of OSINT to monitor internet and social media activities.[74] These efforts suggest that, alongside NTMC, specialized interception gear was being acquired to allow field-level surveillance by law enforcement units.

[71] The Daily Star. (2025). AL govt's secret surveillance state. <https://surveillancestate.thedailystar.net/>

[72] Public Security Division, Ministry of Home Affairs. (2017-2018). Government Order. Government of People's Republic of Bangladesh. <https://archive.org/details/integrated-lawful-interception-system-121210121>.

[73] Ahmed, R. (2023). Govt to launch advanced surveillance system before elections. Prothom Alo. <https://archive.md/sbE2f>.

[74] Hamid, M. A. (2023). Address of the President to the National Parliament of Bangladesh [Speech]. Bangladesh National Parliament. <https://www.parliament.gov.bd/uploads/pdf/President_address/address-2023_054837_.pdf>; Hamid, M. A. (2018). Address of the President to the National Parliament of Bangladesh [Speech]. Bangladesh National Parliament. <https://www.parliament.gov.bd/uploads/pdf/President_address/address-2018_060356_.pdf>.

Bangladesh's procurement of cyber surveillance tools has often involved transnational transactions, given that most such technology is produced abroad. Publicly available trade information and investigative reporting shed light on how these tools are imported.

Direct Imports and Tenders

The table below demonstrates how surveillance trade is conducted through complex logistics to bypass political barriers, raising transparency concerns. Of note is the presence of Israel in export routes—both as the origin of surveillance tools, but also as a pit-stop or intermediary in trade between foreign companies and Bangladeshi state agencies.

Some imports have been more straightforward. The installation of the DPI-based content filtering system was reportedly done by a local tech integrator, Tech Valley Solutions, importing hardware from the United States.[75] Details of the purchase, such as the manufacturer or model, were not disclosed in public sources. Another report indicates that Swiss authorities once intervened "just before shipment" to stop the sale of an IMSI catcher to RAB on human rights grounds.[76] Here, transparency practices of Swiss export controls allowed the deal to become public.

Below is a curated list of exporters and the surveillance technologies they have supplied to Bangladesh. Several are repeat vendors, including firms from Canada and the United States—countries that have recently taken steps to restric the export of commercial spyware and surveillance tools. Despite such measures and public reporting on misuse, companies like Octastic and Yanna Technologies continue to provide stingrays and deep packet inspection systems to law enforcement and intelligence agencies worldwide, including in Bangladesh, where serious human rights concerns persist.

[75] Islam, M. Z. (2019). Govt can now filter online contents. The Daily Star. <https://www.thedailystar.net/frontpage/bangladesh-govt-can-now-monitor-block-filter-online-facebook-contents-1802497>.

[76] Privacy International. (2018). Updated: Amid crackdown, Bangladesh government forces continue spytech shopping spree. <https://privacyinternational.org/long-read/2226/updated-amid-crackdown-bangladesh-government-forces-continue-spytech-shopping-spree>.

TRADE DATA AND PATTERN

Company	Country of Origin	Procuring Entity	Export and/or Procurement Details
Octasic	Canada (with offices in India and Japan)	Bangladesh Police	Octasic primarily supplies Stingrays; it sold IMSI catchers to RAB in 2019, and its CEO Sebastien Leblanc confirmed that the Canadian government approved the export of surveillance technologies to Bangladesh.[77]
ZTE Corporation	China	Bangladesh Police	ZTE deploys video surveillance systems integrated into national telecommunication networks, enabling governments to monitor communications and public spaces.[78]
Neosoft AG	Switzerland	RAB	Produces advanced cellular network interception, IMSI catchers, and other tools capable of identifying users and tracking their locations. It also includes tools for extracting intelligence from 2G, 3G, 4G and 5G networks. Experts have identified its role in training and selling surveillance tools to entities like RAB.
Gamma Group	Germany; United Kingdom	DGFI	FinFisher (or FinSpy) is a surveillance software used to monitor and intercept communications, gather intelligence, and track individuals' activities. Gamma Group dissolved its FinFisher unit in 2014; the spyware is sold through other entities.
Yaana Technologies	United States	NTMC	Yaana appeared as a contractor for DPIs and mobile interception systems between 2018-19 with NTMC and has organized trainings for its officials on surveillance technologies. In 2022, they received a contract to set up an integrated lawful interception system for the NTMC.

[77] Khan, S. S. (2022). The state's surveillance apparatus is out of control. The Daily Star. <https://www.thedailystar.net/views/opinion/news/the-states-surveillance-apparatus-out-control-2972721>.

[78] Surveillance Watch. (n.d.). ZTE – Bangladesh. <https://www.surveillancewatch.io/?menu=countries&country=Bangladesh&entity=ZTE>; AidData. (n.d.). China Eximbank provides RMB 1.547 billion government concessional loan for the Modernization of Telecommunication Network for Digital Connectivity Project (MOTN) (Linked to Project ID#52663). <https://china.aiddata.org/projects/52663/>; The Business Standard. (2024). Vision Technologies Limited becomes official ZTE distributor in Bangladesh. <https://www.tbsnews.net/economy/corporates/vision-technologies-limited-becomes-official-zte-distributor-bangladesh-1199356>; Mobile World Live. (2019). ZTE hosts global service partner conferences in 18 countries. <https://www.mobileworldlive.com/zte-updates-2019-20/zte-hosts-global-service-partner-conferences-in-18-countries/>.

Bay Galata Inc.	Turkey	Bangladesh Police	Bay Galata produces small arms, armed drones, anti-drone systems, and jammers for state use. It supplied Counter Unmanned Aerial Vehicles with jammers to the Bangladesh Police in 2024.
Aser Teknoloji Otomasyon	Turkey	DGFI	Aser contracts with defense ,telecommunications, and railways sector entities for surveillance tools .It supplied device and/or signal jammers to the DGFI in.2024
Mobileum Inc	United States	NTMC	Mobileum services the telecommunications sector with surveillance tools and solutions.
FinFisher	Germany; United Kingdom	-	FinFisher (or FinSpy) is a surveillance software used to monitor and intercept communications, gather intelligence, and track individuals' activities. Gamma Group dissolved its FinFisher unit in 2014; the spyware is sold through other entities.
Yaana Technologies	United States	NTMC	Yaana appeared as a contractor for DPIs and Mobile Voice and Data Intercept systems between 2018-19 with NTMC and has organized trainings for its officials on surveillance technologies.
Bay Galata Inc.	Turkey	Bangladesh Police	Bay Galata produces small arms, armed drones, anti-drone systems, and jammers for state use. It supplied Counter Unmanned Aerial Vehicles with jammers to the Bangladesh Police in 2024.
Aser Teknoloji Otomasyon	Turkey	DGFI	Aser contracts with defense, telecommunications, and railways sector entities for surveillance tools. It supplied Improvised Explosive Device Jammers to the DGFI in 2024.
Mobileum Inc	United States	NTMC	Mobileum services the telecommunications sector with surveillance tools and solutions.

Confidential Imports via Third Countries

Bangladesh's lack of formal relations with Israel means direct purchases from Israeli companies are officially prohibited. Despite this, multiple Israeli-origin systems reportedly ended up in Bangladesh, facilitated by third-party countries like Cyprus, Singapore, and Hungary. Several investigative reports and a draft report to the European Parliament documents shipments of surveillance systems to Bangladesh in 2019 and 2022.[79] For example, the Passitora SpearHead van manufactured by Passitora Ltd (formerly known as WiSpear, founded by now sanctioned former Israeli intelligence officer Tal Jonathan Dilian[80]) was exported from Cyprus to Bangladesh in June 2022.[81] Cyprus export data indicates that in 2019, several companies routed their sales through Cyprus to supply RAB, NTMC, DGFI and other agencies with surveillance tools. Another example is the PicSix case, where Hungary was reportedly the nominal source and the training location, even though the product was Israeli.[82] Through extensive investigations on company origins, technologies manufactured and/or sold, and procurement and export documentation, we have outlined a sample of Israeli-origin companies below to illustrate their interconnections and process of bypassing trade or diplomatic restrictions.

[79] Yaron, O., & Khan, Z. S. (2023). Israeli spy tech sold to Bangladesh despite dismal human rights record. Haaretz. <https://www.haaretz.com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-bangladesh-despite-dismal-human-rights-record/00000185-9692-d16a-a987-f6b75dd00000>; The Jerusalem Post. (2023). Israeli spyware and surveillance tools sold to Bangladesh. <https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-728100>; European Parliament. (2023). Draft results of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (Report A9-0189/2023). European Parliament. <https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html>.

[80] Marzocchi, O., & Gobet, E. A. H. (2022). Briefing for the PEGA mission to Cyprus and Greece. European Parliament. <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/738330/IPOL_STU(2022)738330_EN.pdf>; Hazou, E. (2022). Opposition calls for spying investigation. Cyprus Mail. <https://cyprus-mail.com/2022/08/09/opposition-calls-for-spying-investigation>.

[81] The Wire. (2023). Despite ban, Bangladesh bought spyware worth at least $12 million from Israeli firms: Report. The Wire. <https://www.thewire.in/south-asia/bangladesh-spyware-israel-ban>.

[82] Al Jazeera Investigative Unit. (2021). Bangladesh bought mass spying equipment from Israeli company. <https://www.aljazeera.com/news/2021/2/2/bangladesh-bought-surveillance-equipment-from-israeli-company>; Al Jazeera Investigative Unit. (2021). UN calls for Bangladesh army probe after Al Jazeera investigation. <https://www.ajiunit.com/article/un-calls-for-bangladesh-army-probe-after-al-jazeera-investigation/>; The Jerusalem Post. (2023). Ex-Israeli intel cyber experts tied to Bangladesh military spyware deals. <https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-728100>.

Company	Registered In	Associated Entities	Background	Tools Sold to Bangladesh
Prelysis	Cyprus; Israel	Kobi Naveh; Verint Systems	Prelysis largely supplies Wi-Fi interception systems to the NSI and is founded by a former employee of Verint, a large-sized surveillance tech firm.	Wi-Fi interception systems
Coralco Tech	Cyprus; Israel; Singapore	Founded by former UTX Technologies employee Eyal Almog	Coralco supplies OSINT tools and interception technologies for LTE, GSM, WiFi, and other communication platforms, and has allegedly developed tools with similarities to malware from Wolf Intelligence, such as the WolfRAT, which targets messaging platforms. It sells phone interception systems to the Bangladesh armed forces through its branch in Singapore, routing it through Cyprus.	OSINT, Wi-fi, LTE and GSM interception, malware
Passitora	British Virgin Islands; Switzerland	Intellexa Consortium, Wispear Systems Limited; founded by former Israeli intelligence personnel Tal Dilian	Passitora sold its SpearHead System—known in Cyprus for extracting private data from people's phones without their knowledge—to Bangladesh via Toru Group. Official government records show they won a bid in 2021 to vehicle-mounted interception systems.	Device / network interception targeting Wi-Fi signals, passwords and communication at long range
Merlinx	Israel; United States	OwnBackup, Bindency. Founded by former Israeli intelligence personnel Matan Markovics, Daniel Hanga, and Tal Tchwella.	Merlinx (formerly Equus Technologies) produces cyber infiltration tools, such as the Apollo platform, which enables Wifi interception and phishing-based data extraction. It has contracted with NSI through Prelysis. It is now owned by Bindecy, a firm with ties to Israeli cyber intelligence firm Toka.	Cyber infiltration tools; Wi-fi interception systems

Cellebrite	Israel	-	Cellebrite is an Israeli intelligence company known for developing UFED, a highly intrusive mobile device spyware.	Universal Forensic Extraction Device (UFED)
Pegasus	Israel	NSO Group	Pegasus is an infamous spyware created by the Israeli *NSO Group* and known for its sophisticated surveillance attacks ,through which it can infiltrate smartphones) iOS ,Android ,(extract sensitive data ,record conversations ,and monitor user activity without the user‘s knowledge .Multiple countries worldwide are hearing lawsuits against the use of Pegasus by State entities on their citizens, pointedly its misuse against journalists ,activists ,and political opposition.	Mobile device infiltration ,sensitive data extraction ,remote audio visual control

Toru Group	British Virgin Island ;Switzerland	Assaf Elias;
		Passitora;
		Intellexa
			Toru Group largely acts as a middleman in transactions linked to Passitora and Intellexa .It supplied *Vehicle Mounted Mobile Interceptors* spy vehicle to Bangladesh in June,2021 which is reportedly in use by Bangladeshi authorities. Toru Group‘s tools have allegedly been leading to the termination of police officials accused of criticizing the government in private WhatsApp groups.	Intermediary services for surveillance deals

UTX Technologies	Singapore;
	Lithuania;
	Cyprus
		Verint Systems	UTX Technologies have been linked with selling spyware and surveillance tools to multiple countries ,notably Mexico ,Nigeria ,Thailand and the UAE ,and likely affiliated with Russian-Israeli Anatoly Hurgin ,and linked with NSO Group and *Pegasus* .UTX was acquired by Israeli conglomerate Verint Systems in.2014	Web and location intelligence systems

Verint Systems	Netherlands; United States	Verint Systems ;Cognyte	Verint Systems is a large conglomerate with operations in the U.S .and Netherlands ,however ,with significant research and development presence in Israel .in ,2021 Amnesty International reported that its Israeli subsidiary supplied communications interception tools to South Sudan‘s National Security Service, which has been linked to surveillance and repression of political dissent	Spyware ,network interception ,ILIS

RECOMMENDATIONS

The practices of cyber surveillance in Bangladesh, often for political ends and without adequate legal safeguards, necessitates a multi-faceted approach to reform. Grounded in the principles of human rights, democratic accountability, and the rule of law, the following non-exhaustive recommendations are proposed to address the challenges identified in this report. These recommendations focus primarily on legal and institutional reforms, and are intended as a foundation for broader discussions on transparency, oversight, and the protection of fundamental rights in the digital age.

Comprehensive Legal and Policy Reforms

A robust legal framework is the bedrock of a rights-respecting surveillance regime. The current legal landscape in Bangladesh is inadequate and often repressive, necessitating urgent and comprehensive reforms.

Establish A Legislative Reform Commission On Surveillance Laws.

The Government of Bangladesh should establish an independent legislative reform commission tasked with conducting a comprehensive review of all existing laws and regulations that enable surveillance. This includes both core surveillance statutes, such as the Bangladesh Telecommunication Regulation Act, 2001, the Telegraph Act, 1885 and the Wireless Telegraphy Act, 1933, as well as the sectoral laws and regulatory instruments that enable surveillance through vague data access or cooperation provisions. This commission should evaluate whether such laws require amendment or repeal to bring them into compliance with constitutional safeguards, existing judicial pronouncements, and international human rights standards. In particular, the review must assess and narrow overly broad and vague terms such as “national security” and “public order,” which are frequently used to justify unchecked surveillance and the suppression of dissent. The commission’s work should draw from authoritative sources, including the recommendations outlined in paragraphs 81-99 of the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue.[83]

Surveillance activities must be governed by a clear, narrowly tailored, and publicly accessible legal framework that aligns with domestic constitutional standards and international human rights law. These frameworks should govern the entire lifecycle of surveillance technologies, from procurement and purchase to deployment, operational use, data handling, oversight, and redress. Each stage must be guided by the principles of legality, necessity, and proportionality, with transparency and accountability embedded by design.

Specifically, procurement processes should be subject to both parliamentary oversight and judicial scrutiny to prevent mission creep and abuse, and must include standalone human rights impact assessments, public disclosure of vendors and technical specifications, and the exclusion of technologies supplied by entities implicated in rights violations. Operational use of surveillance should be subject to prior judicial authorization and periodic audit by independent oversight bodies to ensure surveillance is “necessary and reasonable” to a legitimate security objective, and affected individuals should have access to effective remedies in cases of abuse. Moreover, secondary legislations, like rules, regulations, regulatory guidelines, and licensing frameworks must not be misused to introduce surveillance obligations or technical capabilities that go beyond what is explicitly permitted under statutory law. Overbroad legal immunities that shield public officials from accountability for surveillance-related abuses must be repealed to ensure individual and institutional responsibility.

[83] United Nations Human Rights Council. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (UN Doc. A/HRC/23/40). <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf>.

The Appellate Division's Clarification On Constitutional Boundaries On Surveillance Technologies

Given the frequent and expansive invocation of grounds such as national security, public order, and incitement to offence to justify surveillance practices in Bangladesh, and the growing body of evidence indicating their misuse by state agencies, there is an urgent need for constitutional clarification of what constitutes "reasonable restrictions" on fundamental rights. The Appellate Division of the Supreme Court of Bangladesh should issue a comprehensive ruling that sets out clear constitutional guidelines for law enforcement and intelligence agencies, and their governing ministries, addressing the entire lifecycle of surveillance technologies, including procurement, purchase, deployment, operational use, oversight, and redress. Such a ruling should explicitly mandate compliance with international standards, including the ICCPR, UN Guiding Principles on Business and Human Rights, UN Human Rights Committee General Comment No. 16, and reports such as A/HRC/23/40 (by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Frank La Rue). This guidance could arise through an appeal from a pending case from the High Court Division, a directive under Article 104 of the Constitution to ensure "complete justice," or a presidential reference under Article 106 of the Constitution seeking the court's opinion on the legality and limits of mass and targeted surveillance in light of its profound public importance.

Enact A Strong Personal Data Protection Law

Bangladesh should prioritize the drafting and enactment of a comprehensive personal data protection law that does not provide vague or overly broad exemptions for law enforcement and intelligence agencies. Specifically, the proposed statute should, similar to the Right to Information Act, 2009, extend its application to law enforcement and intelligence activities in cases involving corruption and human rights violation, rather than imposing blanket immunity. It should clarify, through explicit legal provisions or explanatory notes, that any restriction on transparency is an exception and not the norm, and must demonstrably be in the public interest, subject to human rights due diligence, and undergo regular audits by an independent oversight body composed of judicial and private sector experts. At all material times, both substance and application of the law must adhere to international human rights standards, such as the principles of legality, necessity, and reasonableness.

Strengthening Oversight and Accountability

The lack of effective oversight is a critical weakness in Bangladesh's intelligence and security architecture, leading to a culture of impunity. The following recommendations are aimed at ensuring more balanced and rights-respecting governance structures.

Establish An Independent Parliamentary Oversight Committee

Bangladesh currently lacks an effective parliamentary or institutional mechanism to scrutinize the operations of law enforcement and intelligence agencies engaged in surveillance. There is no specialized parliamentary committee with oversight powers, no independent data protection authority with the mandate or capacity to interrogate surveillance practices, and the judiciary has played a minimal role in defining the constitutional boundaries of privacy, free expression, and due process in this context. While legal challenges have been brought—such as those targeting provisions of the Digital Security Act, 2018, or the Bangladesh Telecommunication Regulation Act, 2001—they have largely failed to curtail surveillance powers or establish sustained institutional accountability. This legal and institutional vacuum has allowed surveillance practices to operate with near-total opacity and impunity.

To address this, an independent, well-resourced parliamentary oversight committee should be established by statute, with a clear mandate to monitor the full spectrum of surveillance activities carried out by law enforcement and intelligence bodies. This committee must be empowered to summon agency officials, compel the production of documents and contracts (subject to narrowly defined national security exceptions), conduct audits, and initiate independent investigations into potential rights violations. It should also be authorized to recommend legislative reform, refer matters to the judiciary, and publish periodic public reports to ensure transparency and democratic accountability. Its membership should reflect political diversity, and its work must be supported by a permanent, expert secretariat with technical, legal, and human rights expertise.

Empower Judicial Oversight

The judiciary must be empowered to play both a proactive and reactive role in regulating surveillance in order to uphold constitutional rights and ensure institutional accountability. Proactive oversight involves the prior authorization of all surveillance measures by a competent and independent judicial authority, based on probable cause, limited to serious criminal investigations, and subject to strict tests of legality, necessity, and proportionality. This process should be time-bound, require detailed justifications, and allow for adversarial review where appropriate. Reactive oversight, meanwhile, enables individuals to challenge unlawful or abusive surveillance after the fact through mechanisms such as judicial review, complaints procedures, and access to remedies, including the suppression of unlawfully obtained evidence, sanctions against responsible officials, and compensation for rights violations. To be effective in both roles, the judiciary must be granted an explicit legal mandate, supported by sufficient institutional autonomy, technical capacity, and access to independent expert advice to scrutinize complex surveillance technologies and ensure that their use remains consistent with constitutional and legal limits.

Promote Transparency And Public Reporting On Surveillance Activities

To foster public trust and ensure democratic oversight, law enforcement and intelligence agencies must publish regular transparency reports detailing the scope, frequency, and nature of their surveillance activities, as well as the technologies currently in use and under procurement. In line with international best practices—such as those outlined by the UN Special Rapporteur on the right to freedom of opinion and expression, Frank La Rue—these reports should, at a minimum, include aggregate data on the number and type of surveillance technologies procured; the number of surveillance requests made, approved, and rejected; and a disaggregation of requests by service provider, type of data sought, investigative purpose, legal basis invoked, and geographic scope. Agencies should also disclose the procedures followed when interacting with service providers, the legal safeguards designed to protect individuals' rights, and the oversight mechanisms in place. While operational secrecy may be justified in narrowly defined circumstances, blanket opacity erodes accountability, fosters impunity, and undermines public confidence in democratic institutions.

Export Controls For Surveillance Technologies and Spyware

Oversight and accountability are necessary not only within Bangladesh but also in the countries exporting surveillance technologies. Existing regional and international export control frameworks—such as the Wassenaar Arrangement, the Pall Mall Process, and the European Union's Dual-Use Regulation (Regulation (EU) 2021/821)—provide important reference points. These mechanisms articulate norms and responsible practices governing the cross-border sale, transfer, and use of surveillance and dual-use technologies. While the Wassenaar Arrangement and the Pall Mall Process are voluntary and depend on national implementation, the EU regulation is legally binding and directly enforceable within its member states.

Despite differing levels of enforceability, each framework establishes a normative baseline grounded in human rights principles and international accountability. Notably, they are either binding on or formally endorsed by a significant number of exporting or intermediary countries. As such, these frameworks offer critical leverage for civil society coalitions, digital rights organizations, and parliamentary bodies in exporting jurisdictions to advocate for more stringent oversight, and raise the question not only of how, but whether such technologies should be exported to governments with poor human rights records, such as Bangladesh. This form of external pressure can serve as a constructive mechanism for reform by incentivizing transparency, constraining opaque procurement practices, and encouraging alignment of surveillance practices in Bangladesh with internationally recognized human rights standards.

CONCLUSION

Bangladesh's surveillance apparatus has evolved into a complex and largely opaque ecosystem, sustained by a network of domestic legislation, transnational supply chains, and institutional practices that frequently bypass constitutional safeguards and international human rights standards. Across its entire lifecycle—from procurement and purchase to deployment and operational use—surveillance has been shaped by authoritarian political imperatives and deployed as a key instrument of political control. These activities often occur under vague legal mandates, with minimal parliamentary and judicial oversight. As a result, surveillance has become embedded in statecraft, serving to entrench regime stability and consolidate state power at the expense of individual rights, public accountability, democratic oversight, and the rule of law.

Yet this trajectory is not unique to Bangladesh. Across South Asia, the invocation of national security has increasingly been used to legitimize the expansion of state surveillance and the erosion of civil liberties. The result is the emergence of surveillance regimes that are structurally designed to prioritise regime security over fundamental freedoms. In these contexts, surveillance technologies are routinely used to preempt dissent, monitor political opposition, and suppress civic expression, transforming digital infrastructure into a mechanism of control. The danger lies not only in unchecked overreach, but in the quiet normalization of unaccountable governance in the digital sphere.

Addressing this crisis requires urgent, systemic reform. Clear constitutional limits on surveillance, comprehensive legal safeguards, independent oversight mechanisms, and genuine transparency are essential. Surveillance policy must be grounded not in the logic of political survival, but in the principles of human dignity, democratic accountability, and the rule of law. Without such a shift, the digital capabilities of the state will continue to serve as tools of repression rather than public service.

APPENDIX

METHODOLOGY

Research Design

This report adopts a qualitative, exploratory research design aimed at mapping the architecture, drivers, and implications of state surveillance in Bangladesh. Rather than testing a predefined hypothesis, it seeks to build a grounded understanding of how legal frameworks, institutional arrangements, political dynamics, and transnational supply chains interact to facilitate and normalize surveillance practices. Given the opaque nature of the subject matter, the limited availability of official data, and the absence of an effective disclosure process, a descriptive and interpretive approach was prioritized. This allowed for the identification of patterns, gaps, and emergent themes across a range of data sources. Such an approach is particularly well-suited to examining complex governance regimes like Bangladesh's, which often operate beyond formal legal accountability and in contexts marked by significant information asymmetry.

Data Collection and Source Triangulation

A triangulated data collection strategy was used to ensure analytical robustness and cross-verification of findings. Data were drawn from four primary source categories. First, academic literature on state surveillance, digital rights, and cyber governance provided the theoretical and conceptual foundation for the analysis. Second, investigative journalism and media reports were reviewed to trace the acquisition, deployment, and political context of surveillance technologies in Bangladesh, particularly in instances where official documentation was unavailable or inaccessible. Third, publicly available procurement records, trade databases, import-export data, e-tenders, training logs for specific technologies, and government documents were analyzed to identify surveillance tools, suppliers, procuring agencies, and usage patterns. Finally, semi-structured interviews were conducted with individuals familiar with surveillance procurement, deployment processes, and their broader implications, to supplement gaps in the documentary record and provide contextual insight into the operational, legal, and societal dimensions of surveillance practices in Bangladesh.

This triangulated approach served both to strengthen the reliability of the findings and to reveal the complex, layered nature of Bangladesh's surveillance ecosystem. Because no single source offered a complete picture, cross-verification was essential to identifying patterns, validating procurement timelines, and substantiating the presence and use of specific technologies. For example, interviews and media reports were corroborated with customs data, budget documents, procurement records, and government orders, which enabled the study to confirm details and uncover otherwise opaque dynamics, such as the role of intermediary suppliers, unofficial procurement routes, and informal uses of surveillance tools beyond legal mandates. Moreover, interviews not only filled documentary gaps but also offered critical insights into institutional logics, informal norms, and the human rights implications of surveillance practices, issues that are often invisible in written records. Together, this methodological approach enabled a more holistic and credible account of how surveillance is structured, deployed, and experienced in Bangladesh.

LIMITATIONS

This study faces several methodological limitations that are important to acknowledge.

First, there is a significant gap in existing academic literature and investigative reporting on cyber surveillance in Bangladesh. Unlike other jurisdictions where watchdog journalism, legal scrutiny, and public access to records provide a foundation for research, Bangladesh's surveillance ecosystem remains largely undocumented and opaque. As a result, reliance was placed on a range of fragmented and indirect sources, and inferences were often drawn from available public records, secondary documentation, and international investigative reports.

Second, no formal information disclosure requests were filed under the Right to Information Act, 2009, as nearly all agencies examined in this report fall within the exemptions granted to "organisations and institutions which are involved in state security and intelligence." These exemptions, coupled with the low rate of compliance and the potential for institutional retaliation, rendered the information disclosure mechanism unviable for the purposes of this inquiry.

In light of these constraints, the study instead relied on interviews with individuals familiar with surveillance procurement and deployment processes. Given the sensitivity of the subject matter, every effort was made to protect the identities of those consulted, and all information provided was cross-verified for credibility and accuracy wherever possible. However, a significant limitation was the inability to conduct interviews with serving agency officials or undertake on-site verification of surveillance infrastructure. As a result, the research could not be corroborated through direct institutional engagement or field-level observation.

Third, although the study triangulated information from a wide range of sources—including public procurement records, customs data, trade intelligence, and investigative journalism—the ability to verify specific claims was often constrained by the absence of access to primary evidence. This limitation is compounded by official secrecy laws and expansive national security exemptions, which continue to shield surveillance activities from public and judicial oversight.

Fourth, the study did not undertake a systematic review of technologies imported through local intermediaries. Many of these entities operate with little transparency and often serve only as conduits for foreign systems, limiting the granularity of the supply chain analysis.

Fifth, while every effort has been made to be as comprehensive as possible, this report is neither exhaustive nor definitive. Rather, it should be viewed as a non-exhaustive, evolving account of Bangladesh's surveillance ecosystem. As noted above, the lack of access to primary, verifiable information made it difficult to offer a fully comprehensive or conclusive mapping of surveillance infrastructure and practice.

Finally, the findings represent a snapshot of surveillance procurement and practices primarily covering the period from 2015 to 2025. Developments beyond this temporal scope fall outside the purview of this report.

DATA

1. Budget Figures

Budget allocation, FY 2016-2024

Source: Ministry of Finance, Government of Bangladesh

Financial Year (FY)	Ministry of Defense (MOD)	Armed Forces Division (AFD)	Public Security Division (PSD)	Total	YOY Growth
16/17	23,196	31	16,781	40,008	-
17/18	26,400	30	19,397	45,827	14.54%
18/19	30,670	34	22,099	52,803	15.21%
19/20	32,975	131	22,214	55,320	4.77%
20/21	33,916	39	21,659	55,614	0.53%
21/22	37,533	48	23,259	60,840	9.40%
22/23	36,650	37	22,575	59,262	-2.59%
23/24	38,174	36	25,123	63,333	6.87%
	259,514	386	173,107	433,007	6.96%

2. Exporting Countries

Australia

Bulgaria

Canada

China

Cyprus

Czech Republic

France

Germany

Hungary

India

Israel

Italy

Malaysia

Netherlands

Singapore

Switzerland

Turkey

United Arab Emirates

United Kingdom

United States

3. Suppliers and/or Vendors

Aser Teknoloji Otomasyon

Bay Galata

Belkasoft

Bilgi Teknologi Tasaram (BTT)

Cellebrite

Cognyte

Coralco Tech

Ezzy Group

Gamma Group

Intersec
LightSpy

MerlinX

Mobileum

Neosoft AG

NSO Group

Octastic

Oxygen

Passitora

PixSix

Prelysis

Raviraj Technologies

Snaptrends

Spider Digital

Toru Group

UTX Technologies

Verint Systems

WiSpear

Yanna Technologies

ZTE Corporation

4. Data Sources

Bangladesh Customs

Bangladesh Police

Bangladesh Public Procurement Authority

China Aid Data

Citizen Lab

Digital Forensics Research Lab, Atlantic Council

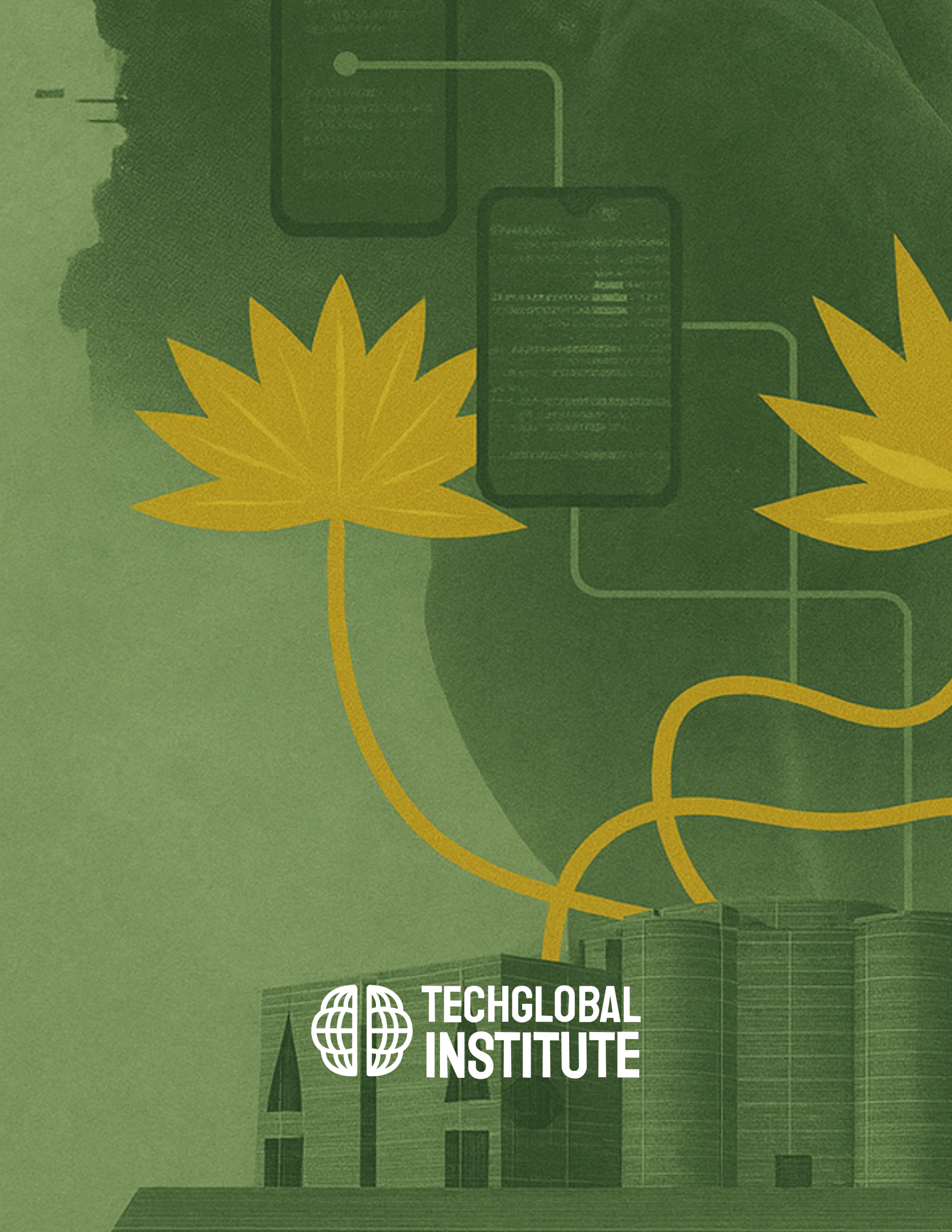
e-Government Procurement, Government of Bangladesh

Export records obtained from Cyprus, Canada, Switzerland and France

ITC Trade Map

Public Security Division, Ministry of Home Affairs

S&P Global Market Intelligence



TECHGLOBAL INSTITUTE