GSIC TOP SECRET - extracts from the Black List Dossier

This document is made up of intelligence gathered by different relevant agencies about potential future terror-related operations that might be implemented in the future by different malignant and criminal organisations. This list of operations is known in GSIC intelligence circles as **The Blacklist.** This list was found on the USB of a well known terrorist in the Colombian Jungles. It is yet unknown who is planning these operations. It is not clear which of these operations are actually serious and which are merely theoretical operations.

During the sessions of the GSIC, the chairs will declare to the committee that they have received confirmation that a specific operation from the list is a real plan that is about to be implemented. The committee will then need to pass plans to subvert the operation in question. Once an operation has been declared as a legitimate threat, further information will be handed to each delegate. We expect that throughout the whole duration of the sessions, 4 operations will be addressed.

You are required therefore to prepare for the sessions by studying all of the potential operations on the Blacklist and to set up a plan, involving your intelligence agency and others, to thwart these operations should they come to pass.

In your research you should consider these questions:

- What are your country's intelligence capacities?
- What are your country's interests (public or secret) when it comes to each operation. What is the outcome that they prefer?
- What should your intelligence agencies do to address each operation?

Item 1 Operation Fractured Barrel

Extract from the Dossier

Fragments recovered from the encrypted files reference a possible operation targeting a major international Energy Security Forum scheduled to take place in Dubai World Trade Centre (DWTC), Sheikh Zayed Road, Dubai, UAE. The event is the Global Energy Security Forum, which brings together ~1,200 delegates from more than 60 countries, including ministers of energy, national security advisors, executives from major oil corporations, and representatives of OPEC, the IEA, and global investment funds on the 24-25th of March. The documents suggest that several high-ranking energy officials from rival geopolitical blocs may be vulnerable during the event.

The files outline a scenario in which multiple "removal actions" could occur within a very short time window, potentially using different methods at separate locations connected to the forum. Notes in the dossier mention poisoning during a diplomatic dinner, a long-range precision attack during a public appearance, and an explosive device targeting a motorcade leaving the venue. The purpose of the operation is described cryptically as "fracturing market stability and forcing immediate energy panic."

Intelligence Assessment

Analysts within the Global Security Intelligence Council (GSIC) assess that the recovered files may outline a coordinated assassination plan targeting senior figures involved in global energy policy. Several passages indicate that the operation could aim to eliminate representatives from China, the United States, and Iran during the same diplomatic event. If authentic, executing such a plan would require multiple specialized teams operating simultaneously, each employing distinct methods to obscure attribution and create the appearance of unrelated incidents. One encrypted message references operatives potentially entering the United Arab Emirates using diplomatic passports issued by multiple countries, implying either exploitation of diplomatic immunity or insider cooperation within official delegations. While the organizing network's identity remains unknown, the language and operational sophistication suggest a transnational covert structure with access to advanced intelligence tradecraft and logistics capabilities.

Situation Analysis

The upcoming Global Energy Security Forum at DWTC is expected to gather ministers, advisors, and corporate leaders responsible for strategic petroleum reserves, energy transition planning, and global oil supply coordination. The geopolitical context surrounding the event is tense, with intensified competition among major powers over energy markets, supply routes, and strategic reserves. Any disruption affecting key decision-makers could generate immediate uncertainty in global markets. Dubai's position as a major diplomatic and commercial hub means that large numbers of foreign delegations, security personnel, and private contractors will be

present, potentially introducing vulnerabilities within the security environment. Intelligence agencies have also reported unusual encrypted communications between unidentified actors discussing travel arrangements and surveillance near international energy conferences, though their connection to the dossier remains unconfirmed.

Item 2 Operation Stateless Atom

Extract from the Dossier

Fragments recovered from encrypted communications reference a possible operation involving the abduction of nuclear scientists across multiple countries. Within 48 hours, a Pakistani uranium enrichment specialist disappears after leaving a conference in Vienna, a South Korean reactor safety engineer is kidnapped in Busan by masked individuals posing as customs officials, and an Indian missile guidance expert is abducted outside his residence in Bangalore. A video emerges online showing the captives in an undisclosed facility, with the kidnappers claiming they are assembling *"the world's first stateless nuclear program."* Intelligence indicates that the group may have operational connections to both North Korean black-market networks and Russian military contractors, suggesting a highly sophisticated transnational threat.

Intelligence Assessment

Analysts within the Global Security Intelligence Council (GSIC) assess that the recovered files outline a coordinated abduction plan targeting high-value nuclear experts. The simultaneity of the kidnappings suggests multiple specialized teams operating across different jurisdictions, with capabilities in surveillance, logistics, and covert extraction. Encrypted communications indicate the perpetrators may have access to advanced facilities and coercive technical expertise, potentially enabling the development of nuclear capabilities outside state oversight. While the organizing network remains unidentified, its operational sophistication implies a structured transnational entity with access to intelligence tradecraft and clandestine support networks.

Situation Analysis

The scientists who would be abducted as a consequence of this operation represent critical technical knowledge for nuclear enrichment, reactor safety, and missile guidance programs in Pakistan, South Korea, and India. The geopolitical environment is highly sensitive, with each country maintaining strategic oversight of its nuclear assets. Local security vulnerabilities, including conference security gaps, lax customs enforcement, and residential protection weaknesses, were exploited. Intelligence reports indicate coordinated movement and communication between unidentified actors across the affected regions, though their connection to state actors remains unconfirmed. The cross-border nature of the operation complicates recovery efforts and heightens the risk of uncontrolled proliferation.

Item 3 Operation Dead Hand Echo

Extract from the Dossier

Fragments recovered from intelligence sources reference a highly sophisticated cyber operation that aims to target the joint satellite early-warning systems used by both India and Pakistan. During a scheduled overnight software update, malicious code, later designated *"Dead Hand Echo,"* injected fabricated infrared satellite data into India's Strategic Forces Command, falsely indicating the launch of six Pakistani Shaheen-III missiles from sites near Bahawalpur. The operation would rely on India's automated retaliation protocols, causing the system to believe a nuclear strike is underway which would lead it to initiate the launch of two Agni-V ballistic missiles from Abdul Kalam Island toward pre-programmed targets in Pakistan. This is expected to also prompt Pakistan to initiate countermeasures as well.

Intelligence Assessment

Analysts within the Global Security Intelligence Council (GSIC) assess that *Dead Hand Echo* represents an unprecedented bold plan to make use of cyber capabilities capable of manipulating nuclear command-and-control systems. The operation would exploit supply-chain vulnerabilities in satellite communications infrastructure, demonstrating both technical sophistication and operational patience. The party behind this operation remains unclear.

Situation Analysis

The incident would occur during a routine software update, highlighting that even standard operational procedures within high-security satellite and missile systems may be exploited by a sufficiently skilled adversary. Both India and Pakistan maintain tightly integrated early-warning networks designed to detect missile launches, but the reliance on automated decision-making and satellite telemetry created a pathway for manipulation. The subcontracted supplier in South Korea represents a critical node in the supply chain whose compromise enabled remote injection of malicious code. The danger inherent to this possible operation demonstrates that vulnerabilities are not limited to national systems but extend across international supply chains and contractor dependencies.

Item 4 **Operation Crimson Plume**

Extract from the Dossier

Fragments recovered from intelligence sources reference a potential spread of an engineered pathogen deliberately released in multiple global cities. Within 48 hours, hospitals in Cairo, Mumbai, and Sao Paulo would report clusters of patients exhibiting a rapidly progressing respiratory illness. The disease in question begins with mild flu-like symptoms but quickly escalates to acute respiratory collapse and neurological seizures, resulting in multiple fatalities

among otherwise healthy adults. From the data retrieved in this file, the disease could be identified as a modified strain combining SARS-like coronaviruses and hemorrhagic fever viruses, engineered for rapid airborne transmission and unusually high mortality. Synthetic markers within the genome correspond to advanced biomedical research techniques, suggesting an origin linked to a classified biodefense program. The aim of the operation is to spread the pathogen in multiple major population centers by introducing it through airports. This would result in the spread of a deadly global pandemic.

Intelligence Assessment

Analysts within the Global Security Intelligence Council (GSIC) assess that the outbreak represents a deliberate biological attack using a genetically engineered pathogen. The simultaneous emergence of clusters across three continents indicates coordinated deployment, with precise timing suggesting involvement of actors with access to high-level biomedical research and global mobility networks. While direct attribution remains unclear, the genetic modifications point to capabilities consistent with classified laboratory programs. The operation demonstrates the potential for transnational actors to weaponize pathogens, bypassing conventional state oversight and detection mechanisms.

Situation Analysis

The outbreak exposes critical vulnerabilities in international public health infrastructure and biosecurity monitoring. Rapid airborne transmission and high mortality overwhelm local hospital capacities, while the disappearance of researchers suggests potential insider facilitation or direct operational involvement. Cross-border travel patterns and emerging infections in additional cities indicate the pathogen may already be spreading beyond initial containment zones. Intelligence agencies are monitoring flight and transport data to assess further distribution risks, though detection and response efforts are hindered by the engineered nature of the pathogen and the absence of acknowledged state responsibility.

Item 5 Operation shadow ledger

Extract from the dossier

Fragments recovered from the encrypted files reference what appears to be a large-scale financial network operating through numerous offshore shell companies and private banking channels across multiple countries. The documents describe a series of financial transactions that appear to be carefully structured to avoid detection, passing through the private financial institutions in Western Europe, and commercial banking channels in the Gulf region, before disappearing into anonymous accounts connected to the digital asset exchange. Financial intelligence analysts estimate that over 8$ billion may have been passed through this network over the past 18 months. The timing of these transfers is suspiciously aligned with large movements of funds occurring shortly before or after other activities mentioned in the Blacklist.

Intelligence assessments

Analysts within the Global Security Intelligence Council believe that the financial network may be operating as a central funding mechanism for multiple covert operations described in the Blacklist dossier. The transaction patterns reveal the use of sophisticated money-laundering techniques, including multi-layered shell corporations, fake commodity trade agreements, as well as the quick transfer of money into cryptocurrencies to hide the real owners of the funds.

Despite extensive monitoring efforts by financial intelligence units, investigators have so far been unable to identify the original source of the funds. The complexity and coordination of the network suggest that it may be controlled by a highly organized transnational structure with advanced financial expertise and access to major international banking systems.

Situation analysis

Over the past several months, financial regulators in the UAE, the UK, Germany, and Canada, have reported unusual activity involving inactive corporate entities that suddenly started transferring large amounts of money through international banking channels.

Investigators analyzing these transactions have identified multiple shell corporations registered in the Caribbean offshore financial centers, including companies linked to corporate registries in Cuba, which appear to function as intermediaries within the financial network.

Many of these companies appear to exist only as paper entities with no visible operational activities, and share the same directors, addresses, and legal representatives, suggesting a coordinated effort to hide the true owners of the funds.

Despite the increased oversight from financial authorities, the highly sophisticated structure of the networks makes it extremely difficult for investigators to trace the full movement of funds, or determine who controls the operation.

Item 6 Operation Northern Flame

Extract from the dossier

Fragments recovered from the encrypted files reference what appears to be a planned attack under the codename “Northern Flame”. The documents appear to describe an operation targeting a major North American international airport during busy morning travel hours.

According to the fragments, the operation involves an improvised explosive device hidden inside ordinary passenger luggage, inside a crowded airport departure terminal. The files stress the strategic importance of selecting a location with large amounts of international travelers to maximize disruption and social media attention. Additional notes indicate that the attackers may intend to take advantage of crowded check-in zones where baggage is often left unattended before screening.

Intelligence assessment

Analysts within the council believe that the document may indicate a planned attack targeting Toronto Pearson International Airport in Canada. Intelligence assessments suggest that the attackers may potentially use a compact improvised explosive device concealed inside a suitcase, placed near a crowded international check-in area. Intelligence analysts believe that if such an attack were to occur, a responsible organization might attempt to claim responsibility through encrypted online channels, potentially framing the incident as the opening phase of a wider campaign targeting major global airports. Security experts assess that the attack may have been intended both to expose weaknesses in airport security infrastructure, and to trigger widespread anxiety across global air travel.

Situation analysis

The documents suggest that the attackers may consider carrying out the operation during the morning departure rush, possibly at 8:15 AM, terminal 1 at Toronto Pearson International Airport, one of the largest international aviation hubs in North America. If carried out, the

explosion could cause damage across the check-in hall, and force immediate evacuation of the terminal as emergency services secure the area.

If credible intelligence emerges, Canadian authorities may raise the national threat level and begin coordination with international intelligence partners. Although investigators have not yet identified the organization responsible, intelligence agencies are concerned that the incident may be part of a broader campaign targeting global aviation systems.

Item 7 Operation Silent Conclave

Extract from the dossier

Fragments recovered from the encrypted files refer to a possible covert operation called the "Silent Conclave". The documents appear to describe a possible plan to compromise a confidential diplomatic summit scheduled to take place in London, UK, where several senior international officials are expected to participate in closed negotiations. The fragments suggest that the objective of the operation may not involve a physical attack, but rather the covert interception and manipulation of secure communications during the summit. The files mention possible efforts to penetrate hotel network systems, airport communications infrastructure, and municipal surveillance platforms connected to the event's security arrangements. Additional notes within the files suggest that the attackers may intend to collect real-time intelligence on leader travel schedules, aircraft arrival times, and secured convoy routes, as international delegations arrive in Frankfurt.

Intelligence assessment

Analysts within the GSIC believe that the operation may already be in its early stages. During routine cybersecurity monitoring, GSIC analysts have detected what appears to be an unusual concentration of encrypted satellite signals directed toward digital infrastructure associated with London's airport operations and nearby communication networks.

Further forensic investigation suggests that an unidentified cyber group may have attempted to access hotel network systems, municipal traffic camera systems, and portions of the airport's operational data infrastructure. Investigators suspect that the attackers may be attempting to intercept, monitor or possibly manipulate communications between participating delegations during the summit.

Situation analysis

The summit in London is expected to include high-level representatives from across the globe. Initial monitoring indicates that some encrypted communications connected to the summit may already be vulnerable to exposure. Analysts found digital indicators suggesting that external actors may be attempting to gain access to data regarding leader flight paths, arrival times, and planned ground convoy movements.

In addition, cybersecurity teams have also detected what seems to be attempts to simulate “man-in-the-middle” intrusions, a technique that would allow attackers to intercept or alter communications during secure video conferences between participating leaders. Such interference could result in the transmission of false messages or misleading information into sensitive diplomatic exchanges. While this operation does not seem to be ongoing, these signs have shown that the cyber security of the summit was already being tested.