

VARIOUS FORMS OF MONEY LAUNDERING IN DRUG TRAFFICKING

CEPOL Western Balkan Financial Investigation In-Service Training
'Financial Investigations in relation to Drug Trafficking'
08-12 October 2018 in Prishtina, KOSOVO



The market for illegal drugs is the largest criminal market in the European Union (EU). The drugs trade in the EU is conservatively estimated to generate around **EUR 24 billion** in revenue each year.



The market for cannabis remains by far the largest drugs market in the EU. There has been a further increase in the indoor and outdoor cultivation of herbal cannabis in and close to consumer markets.



Around 35% of the Organised Crime Groups (OCGs) active in the EU on an international level are involved in the production, trafficking or distribution of illegal drugs.



More OCGs are involved in cocaine trafficking than any other criminal activity in the EU. The significant increase in production in Colombia has resulted in intensified trafficking activity to the EU.

75% of the OCGs involved in the drugs trade in the EU deal in more than just one illegal drug.

The Balkan route remains the main entry route for the bulk of the heroin trafficked to the EU.

However, there has been a partial shift in the trafficking of heroin from the Balkan route to the Caucasus route.

Drugs are now widely traded online on various platforms.

The sale of drugs via **Darknet marketplaces** is a significant threat and continues to expand.



The scale of money laundering activities in the EU is significant reflecting the immense profits generated by the OCGs involved in the drugs trade and other serious and organised crime.

However, the global antimoney laundering framework implemented by law enforcement and other authorities in the EU has shown to have a poor success rate in identifying and seizing illegal funds generated by criminal organisations. Barely **1% of criminal proceeds are confiscated by relevant authorities at EU level.**

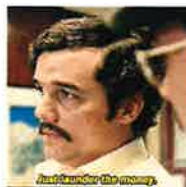




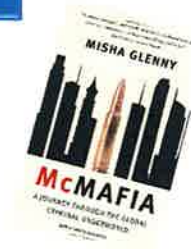
Money laundering allows OCGs to introduce the proceeds of crime into the legitimate economy. Almost all criminal groups need to launder profits generated from criminal activities. The trade in illegal drugs generates substantial profits for the OCGs involved.



In some cases, these OCGs launder these funds by themselves investing in businesses, real estate and other ventures across and outside the EU. However, the most successful drug trafficking networks also make use of money laundering syndicates, which have specialised in laundering the proceeds of other OCGs in exchange for a fee.



Robert Mazur (R) and a pilot stand in front of a private jet used during an undercover cartel operation



Between 0.71-2.0% of annual EU GDP is detected as being involved in suspect financial activity. In 2014, EU Financial Intelligence Units (FIUs) received almost 3 million reports. Although the overall number of suspicious transaction reports (STRs) continues to increase, only around 10% of these reports are further investigated – a figure that is largely unchanged since 2006. Rapid transaction processing and the proliferation of effective anonymisation tools are significant obstacles in the identification of the beneficial owners of criminal proceeds.

Even where further investigated, the likelihood of successful asset recovery is low, and barely 1% of criminal proceeds are confiscated by relevant authorities at EU level.

Money laundering is also increasingly a technical challenge for law enforcement authorities. Criminal networks continuously seek to exploit the latest technological developments such as cryptocurrencies and anonymous payment methods.

A growing number of online platforms and applications offer new ways of transferring money and are not always regulated to the same degree as traditional financial services.

Almost all organised criminal groups (OCGs) carry out their activities for one reason: **profit**. Criminal finances encompass both the crimes that generate vast sums and the methods used to launder these in order that they can be enjoyed and reinvested.

The widespread acknowledgement of the importance of tackling money laundering and criminal proceeds has led to a greater emphasis on conducting financial investigations and gathering financial intelligence. In response, a global anti-money laundering framework has developed over time, and one of its cornerstones is the reporting of suspected criminal financial flows (known as STRs) from the private sector, acting as gatekeepers to the financial system and legal economy, to Financial Intelligence Units (FIUs).

The reports sent by the private sector contain valuable information that can enhance ongoing investigations and often trigger entirely new ones. A number of cases have demonstrated the importance of this system: it would not be possible to effectively combat OCGs operating in the EU or affecting the EU from abroad without pursuing their finances, both for intelligence purposes and as a target.

WHAT ARE STRs?

There is no single name for, or definition of, a suspicious transaction report ((STR), often known as a suspicious activity report (SAR)). However, it is generally understood to mean a report compiled by the regulated private sector (most commonly banks and financial institutions, but also non-financial designated professions) about financial flows they have detected that could be related to money laundering or terrorist financing.



In 1989 the Financial Action Task Force (FATF) - an inter-governmental body - was created. Since then it has set international standards in the fight against money laundering, and their recommendations form a blueprint for the EU's anti-money laundering framework.

FATF's recommendations and the need for a more unified approach to anti-money laundering across the EU led to the First European anti-money laundering Directive in 1991. The Directive (updated three times in 2001, 2005 and most recently in 2015) underpins the EU anti-money laundering framework in place today, through minimum requirements to be implemented by the EU Member States. The Directive created the master design for the current EU anti-money laundering architecture. A cornerstone of this framework is the designation of entities obliged to report suspicious transactions to a central authority, known as a Financial Intelligence Unit (FIU).



The STR regime exists to prevent and detect the abuse of the financial system by criminal groups seeking to launder the profits of illegal activities.



SAR/STR - Process



Mr. Razi Makh Almad, CABLED, Country Anti Money Laundering Compliance Officer, BR Bank Ltd





Why are STRs useful?

A real case

In 2014 the Tax and Customs Authority in one MS conducted a key anti-money laundering operation that culminated in the provisional arrest of the **former Prime Minister**. The case was an investigation related to **tax fraud, corruption and money laundering**, involving sums in excess of 20 million euros.

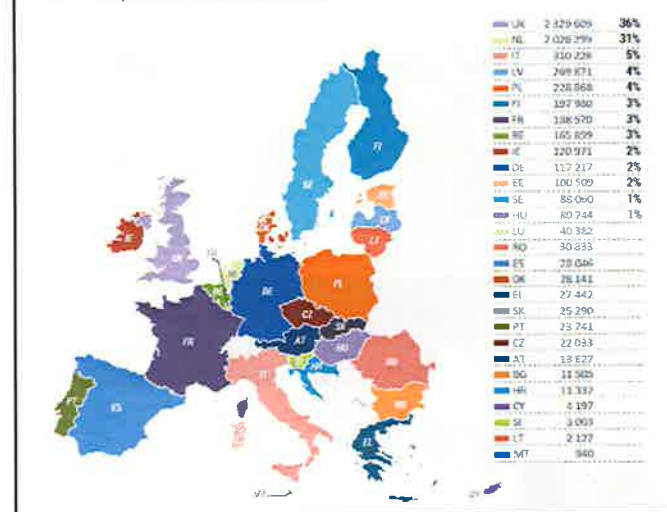
The role of STRs in the case was pivotal: the entire investigation was initiated because of a set of STRs filed by banking entities, informing that EUR 600 000 had been deposited by way of structuring into the bank account of a former Prime Minister. Sums were transferred from **his mother's bank account**, justified by way of the **sale of an apartment (which was over invoiced)** to the former politician's **close friend**.

On-going investigations indicated that this close friend was in fact a **front man**, used to manage an amount of EUR 20 million belonging to the former Prime Minister – sums incompatible with his declared income and corruption seen as the probable source of funds.

The reporting behind the case revealed the use of several money laundering methods including: the use of front men to manage bank accounts; **fake and over-invoiced** purchases to justify the integration and use of funds; false employment and service contracts; the use of cash couriers to transport money between the front men and the beneficial owner.



Chart 2 – Total reports across all Member States (2006 - 2014)



The Fourth anti-Money Laundering Directive sets out those sectors, both financial and non-financial, which have obligations to file reports around suspicious transactions or activities with their national FIUs. Some countries may also implement further categories of obliged entities through domestic legislation (for example, Spain includes NGOs and security and cash transport companies).



As regards the designated non-financial sector, three categories of obliged entities report most frequently to the FIUs – the gambling industry, public notaries and accountants.



Case example: Operation Gambling

A recent case reported across open sources deals with the **Italian Operation Gambling** in which Italian authorities arrested 41 persons and seized assets worth EUR 2 billion in a massive illegal gambling and money laundering operation.

Italian authorities took down a huge network of companies involved in online betting, headquartered in Malta and controlled by the 'Ndrangheta, the notorious Calabrian criminal organisation. Police believe the firms, including the six that were operating out of Malta, were used to launder vast sums of illicit cash.

The case has raised some concerns around the online gambling market and the potential for its abuse by criminal organisations. The implementation of the Fourth anti-Money Laundering Directive which extends scope beyond physical casinos to the gaming sector more generally, may have a significant effect on Malta given the size of its online gambling industry (with over 400 licences granted).



Italian police crack mafia's 2bn euro gambling empire as it seizes betting shops and companies belonging to notorious 'Ndrangheta' organised crime syndicate

- The gang imports cocaine from Latin America to Europe through Africa
- It then launders the incredible wealth through a huge gambling empire
- Police snatched assets including 1,500 betting shops and 60 companies
- Interior minister said it would be a 'serious blow' to the gang

By JAMES SPINNEY FOR Euronews
PUBLISHED: 16:51 OCT 17 2015 | UPDATED: 19:07 OCT 17 2015

On 24 January 2016, law enforcement and judicial authorities from France, the US, Germany, Belgium, Italy, the Netherlands and Spain, supported by Europol and Eurojust, took action against a prominent **OCG responsible for the laundering** of profits from **cocaine** sales throughout Europe.

Building on long-standing ties to South American drugs cartels, the OCG's **modus operandi** involved the use of **cash couriers travelling across Europe by car** to collect the proceeds of crime, followed by the **purchase of expensive cars, luxury watches and jewellery**. These high value goods were then **exported to Lebanon** where they were sold and the proceeds placed into the financial system for onward transfer to cartels in South America.

Moyens-Orient

hezbollah | Saad Hariri |

Opération Cedar : Saad Hariri et le Hezbollah cités dans une affaire de blanchiment d'argent

Parce qu'il s'agit



Jusqu'à présent, on ne sait pas si les membres du Hezbollah ont été impliqués dans l'affaire. Les autorités de la justice ont cependant annoncé que les membres du Hezbollah ont été impliqués dans l'affaire.

Financial investigations revealed that in 2014 alone, the group spent EUR 26 million in cash to purchase luxury watches, without triggering any STRs. The sums involved in 2015 are thought to have been even higher, by which time the group was laundering an estimated EUR 1 million per week. The targeted OCG was mainly composed of Lebanese nationals also suspected of being involved in financing terrorism through Hezbollah's military wing. In the wake of coordinated days of action, one of the main suspects of Operation Cedar was designated by US OFAC (Office for Foreign Asset Control) for his involvement in the financing of terrorist activities.



U.S. DEPARTMENT OF THE TREASURY

SECRETARY MNUCHIN ABOUT TREASURY POLICY ISSUES DATA SERVICES NEWS

Press Releases

Archived Press Releases

Weekly Public Schedule

Media Schedule and Advisories

Webcasts

Press Contacts

Press Center

Home > Press Center > Press Releases > Treasury Sanctions Key Hezbollah Members

Treasury Sanctions Key Hezbollah Money Laundering Network

1/28/2016

WASHINGTON — The U.S. Department of the Treasury today targeted Hezbollah's financial support network by designating Hezbollah-affiliated money launderers Mohamed Moukaddim and Hamid Zahir El Dine, as well as Trade Point International S.A.R.L., a company owned or controlled by Moukaddim. Moukaddim and El Dine were designated today under Executive Order (E.O.) 13224 for providing financial services to or in support of Hezbollah, which has long been designated by the U.S. as a terrorist organization. Trade Point International S.A.R.L. was designated today for being owned or controlled by Moukaddim. As a result of this action, all assets of those designated today that are located in the United States or in the possession or control of U.S. persons are frozen, and U.S. persons are generally prohibited from engaging in transactions with them.

Today's actions continue Treasury's campaign to target Hezbollah and its enablers pursuant to E.O. 13224. Recent Treasury actions have sanctioned heavily both individuals and entities associated with Hezbollah's terrorist, criminal, commercial, and procurement activities. Among those targeted have been financiers and companies in Lebanon, grant procurement providers, a business network in Africa, and numerous others. In total, Treasury has designated over 100 individuals and entities associated with Hezbollah.

"Hezbollah needs individuals like Mohamed Moukaddim and Hamid Zahir El Dine to fund its terrorist operations and political demagoguery," said Adam J. Szubin, Acting Under Secretary for Terrorism and Financial Intelligence. "We will continue to target this vulnerability, and impose and disrupt such enablers of terrorism wherever we find them."

Hezbollah was designated by the Department of State as a Specially Designated Global Terrorist pursuant to E.O. 13224 in October



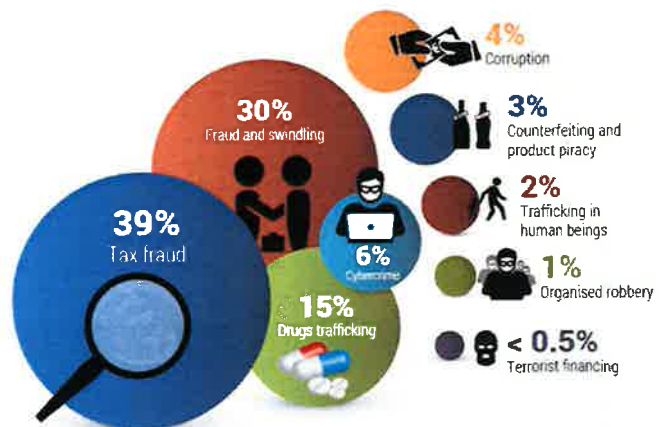
UNREGULATED SECTORS

Examples include virtual currency exchangers, NGOs, and security and cash transport companies (only Spain reported that the latter two categories are obliged entities under national AML legislation).



PREDICATE OFFENCES

Chart 11 (*) – Main predicate offences behind reporting as verified by FIU (2013/2014)



FIU types

Administrative: part of a structure (often the Ministry of Finance) separated from law enforcement or judicial authorities to create a buffer between reporting entities and those charged with investigation and prosecutions. The administrative FIU seeks to substantiate suspicion, and only then can a case be sent on to authorities in charge of criminal investigations.

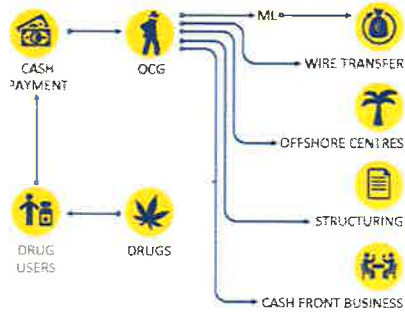
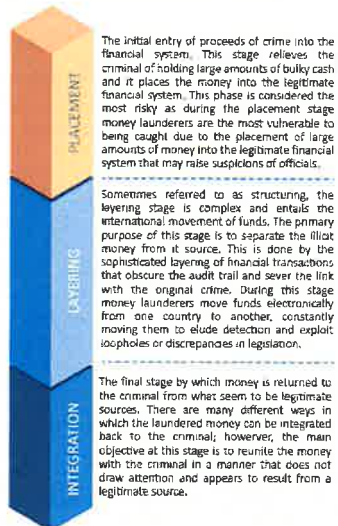
Law enforcement: part of a law enforcement agency, therefore fewer restrictions on FIU access to law enforcement information and vice-versa may apply, potentially resulting in greater operational cooperation and the use of reports in investigations. Such FIUs may also benefit from exchange of information using

national and international criminal information exchange networks.

Judicial: sits within the judiciary, commonly under the prosecutor's jurisdiction as in some legal systems, prosecutors are part of the judicial system and have authority over the investigatory bodies. Judicial FIUs are found in some countries with strong banking secrecy laws so actions such as freezing accounts can be swiftly undertaken.

Hybrid: have different characteristics from the other types of FIU. For example, it may sit within an administrative body but have staff from law enforcement agencies who continue to exercise criminal powers.

The money laundering cycle:



There are countless means of laundering the proceeds of crime, all of which have certain factors in common:

- the need to **conceal** the origin and true ownership of the proceeds;
- the need to directly or indirectly **maintain control** over the proceeds;
- the need to **change** the form of the proceeds in order to either shrink the huge volumes of cash generated by criminal activity or sever the link with underlying criminality.

CASE EXAMPLE: PROFITS AND PIZZA

One case investigated by Italian Authorities concerning the criminal activities of the Mafia Clan 'Fidanzati' led to the seizure of 14 businesses (restaurants, discos, bars etc.). These **cash-front businesses** were all owned and managed at arm's length by the Mafia, through family members, associates and strawmen.

Criminal profits from the groups' illegal activities were used to acquire the companies and finance business costs (payment for suppliers, labour, rents etc.). A discrepancy between the profits the businesses made and reported to tax authorities and their actual running costs alerted authorities to their possible use in the laundering of criminal proceeds.

Some of the businesses, such as **nightclubs**, offered an added advantage in that they provided an ideal market place for the group to conduct its illegal activities – **the sale of drugs**. Drug sellers received payment for their illegal activities through 'legitimate' wages paid to family members employed by the clubs as service staff (e.g. waitresses) which were in fact paid out of criminal funds.

In addition to their portfolio of criminal businesses, the clan also ran a **protection racket extorting up to 10%** of profits from local businesses and service providers (such as valets). The estimated value of the seized businesses amounted to some EUR 15 million which had been injected from criminal cash proceeds.



1983: The Year of the Blitz against the 'White Collar'

Nineteen eighty three was a pivotal year for the discovery of mafia infiltration into the economy and finance inside the square in Milan. The 'Silent Violence' on the night of February 14, led to the arrest of forty people, the notification of the mandate for another hundred already in prison, and seizure of assets for three hundred billion.

Borio Brothers, Ugo Martella, Antonino Esca, **Palizzari Brothers** and the entrepreneurs Antonio Vignola, Luigi Monti, and Carlo's Gatti were accused of **financing their money** through companies in Milan. The story of the case, however, ended with the cancellation of the charge of criminal conspiracy of the Mafia and a rental ordered by the Court of Cassation in 1991.

On November 11, 1983, the blitz of San Martino (forty arrests and raids in major casinos in Italy) failed to climb to the **Casino di Sanremo** for the control of which were nominated two strings, one backed by the **Mafioso from Catania Santapaola**, and the other by **Borio and Lora from Palermo**. The investigation revealed the **commingling of politics, business, and crime**, following the involvement of Antonio Natta, a former top representative of the PSI. Although the investigation of this case had a long history, it ended in June 1996, with the condemnation of all of the mafia-type criminal associations.

End of the Eighties: The Infiltration of the 'Ndrangheta

In the late eighties, Turatello and Epaminonda left the scene and illegal activities went back in the hands of traditional clans. Moreover, the Sicilians did not stop drug dealing and investment of their income in legal activities, as witnessed with the arrest in 1991 of Giuseppe Lottusa, nominee of the **Madrone clan**, who engaged in international transactions of money laundering.

Over the same years, the alarming level of penetration achieved by the 'Ndrangheta in Milan and its province emerged dramatically and openly for the first time. One of the North in previous decades, not for official choices, but following the families of migrants, the men of the Calabrian clan perfected successfully the control of the territory in large areas of the city and surrounding area, without gaining fame and suspicion. While neighborhoods of Milan, like **Intorciano, Corsiconio, and Quarto Oggiaro** or little towns like **Cesena, Bascimone, and Frazzato sul Naviglio**, to quote the most striking cases, fell under the domination of the Calabrian clan who speculate in marriages and kidnappings. The **bulky presence of the Calabrian unit** caused the **frenzied battle** with other organizations, which placed Milan in the third position among the cities in the ranking of the highest number of homicides.

After the surge of conflict, the leaders of the gangs operating in the city agreed to handle the traffic of drugs and the new business of arms smuggling.

1990: An Outbreak of 'Dome Connection'

WHAT'S NEXT?



Contis

Who we are | About Contis | How we work & Plan | News & media | Contact Us

Our alternative banking & payment services **make lives easier.**

Managing and moving money with ease. Providing accounts for everyone, in business and at life.

See our full range of award-winning products below.

For Credit Unions

For White Label
& Referral Partners

For Compliance

For Consumers

The 5th Anti-Money Laundering directive

The 5th Anti-Money Laundering directive will:

- **enhance** the powers of EU Financial Intelligence Units and facilitating their increasing transparency on who really owns companies and trusts by establishing beneficial ownership registers;
- **prevent** risks associated with the use of virtual currencies for terrorist financing and limiting the use of pre-paid cards;
- **improve** the safeguards for financial transactions to and from high-risk third countries;
- **enhance** the access of Financial Intelligence Units to information, including centralised bank account registers.
- **ensure** centralised national bank and payment account registers or central data retrieval systems in all Member States.

Strengthened EU rules to prevent money laundering and terrorism financing

11 July 2018

Vera Jansen
Director-General for External Relations

What does the 5th Anti-Money Laundering Directive bring?

- Improving transparency in the real estate of companies**
The Directive has been adopted together with the 4th Anti-Money Laundering Directive, which will be implemented by the Member States by 1 July 2020. It will require companies to disclose information on their beneficial owners to the competent authorities.
- Improving transparency in the real estate of individuals**
The Directive has been adopted together with the 4th Anti-Money Laundering Directive, which will be implemented by the Member States by 1 July 2020. It will require individuals to disclose information on their beneficial owners to the competent authorities.
- Improving transparency in the real estate of trusts**
The Directive has been adopted together with the 4th Anti-Money Laundering Directive, which will be implemented by the Member States by 1 July 2020. It will require trusts to disclose information on their beneficial owners to the competent authorities.
- Improving transparency in the real estate of other entities**
The Directive has been adopted together with the 4th Anti-Money Laundering Directive, which will be implemented by the Member States by 1 July 2020. It will require other entities to disclose information on their beneficial owners to the competent authorities.

- Lifting the anonymity on electronic money products (prepaid cards) in particular when used online**
Member States will have the possibility to allow the anonymous use of electronic money products only in the offline environment.
- Setting up centralised bank account registers or retrieval systems**
Member States will be required to set up centralised bank account registers or retrieval systems to identify holders of bank accounts in the EU. The Commission will work with the technical experts to ensure the interoperability of such registers or retrieval systems.
- Enhancing the powers of EU Financial Intelligence Units and facilitating their cooperation**
The Financial Intelligence Units will have access to financial data through international case and information exchange or data retrieval systems. The Financial Intelligence Units from the different EU countries will also be able to cooperate more easily, as well as with other competent authorities.
- Extending Anti-Money Laundering and Counter-Terrorism Financing rules to virtual currencies, tax related services, and traders in works of art**
The rules will be applied to the providers of virtual currencies, to persons who provide tax services or services to those provided by accountants, financial advisers and tax related services, and to persons who trade in works of art. These new rules will focus on the virtual currencies and on the virtual activity of the traders in works of art.
- Enhancing cooperation between financial supervisory authorities**
The Directive has been adopted together with the 4th Anti-Money Laundering Directive, which will be implemented by the Member States by 1 July 2020. It will require financial supervisory authorities to cooperate more easily, as well as with other competent authorities.
- Broadening the criteria for assessing high-risk third countries and improving checks on transactions involving such countries**
New criteria have been added under which to assess high-risk third countries, including the absence of an effective membership in addition. Member States will have to ensure that the checks carried out under the existing strategic measures in the new Money Laundering and Counter-Terrorism Financing Directive apply to the high-risk third countries identified by the European Commission. The Directive will also require the competent authorities to carry out enhanced due diligence checks on transactions involving high-risk third countries.



The EU Approach: EU Policy Cycle

- EU Policy Cycle for organised and serious international crime 2018/2021
- Multi Annual Strategic Plan for the Criminal Finances / Money Laundering / Asset Recovery Priority
- Priority: To combat criminal finances and money laundering and facilitate asset recovery in view of effectively confiscating the criminal profits of
- OCGs, especially targeting money laundering syndicates offering money laundering services to other OCGs and those OCGs making extensive use of emerging new payment methods to launder criminal proceeds

When are the new rules in force?

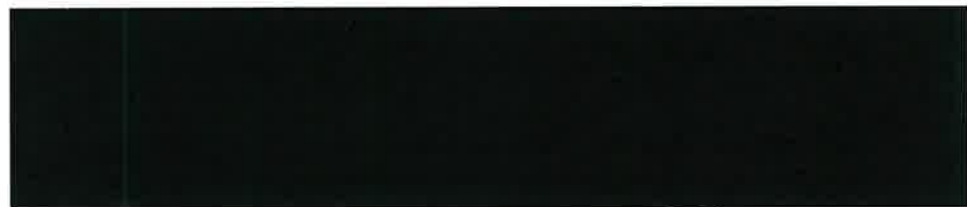
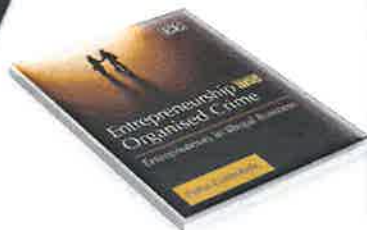
The 5th Anti-Money Laundering Directive has been adopted and entered into force on 5 July 2018. Member States will have to implement the Directive in their national legislation by 30 January 2020. These rules will be applicable to EU banks and other financial institutions starting from the year of 2020. The Commission will monitor Member States to check to what extent they have implemented the Directive and to what extent they have implemented the Directive in their national legislation.

Case Examples

Operation Kouri targeted a large criminal organization based in France, but operating in several other Member States (Belgium, The Netherlands and Spain) and beyond (Morocco and The United Arab Emirates), specialized in performing high end money laundering services to major international trafficking cartels (hashish and cocaine).

At the end of November 2016 a joint investigation team (JIT) consisting of investigators and judicial authorities from France, Belgium and the Netherlands, took action against the money laundering ring resulting in the arrest of 36 suspects and the seizure of 31 kg of cocaine, 2,5 kg of hashish, 2 submachine guns, 4 money counting machines, 7,350 kg of gold (worth over 800.000 EUR) and more than 7 million EUR in cash, making this operation the second biggest cash seizure in Europe during the year of 2016. Europol assisted the competent law enforcement agencies by organising and funding several operational meetings, provided a full scale analytical support and real-time intelligence analysis as well as forensic and technical support by deploying Mobile Offices to all involved Member States during the action days.

Operation Santa Lucia/Contini Blanca, led by Spain, Italy and Germany, focuses on an OCG involved in the transport of large amounts of drugs to Italy. The OCG is linked with the "Camorra" and uses infrastructures and companies to launder their proceeds by themselves. For that purpose, the OCG misuses the financial system, and by using middlemen operates multiple bank accounts, exploiting products such as loans and stock market trading. Moreover, trade-based money laundering is also a way of concealing their criminal funds by buying/selling companies, vehicles and jewellery that are controlled by the OCG.



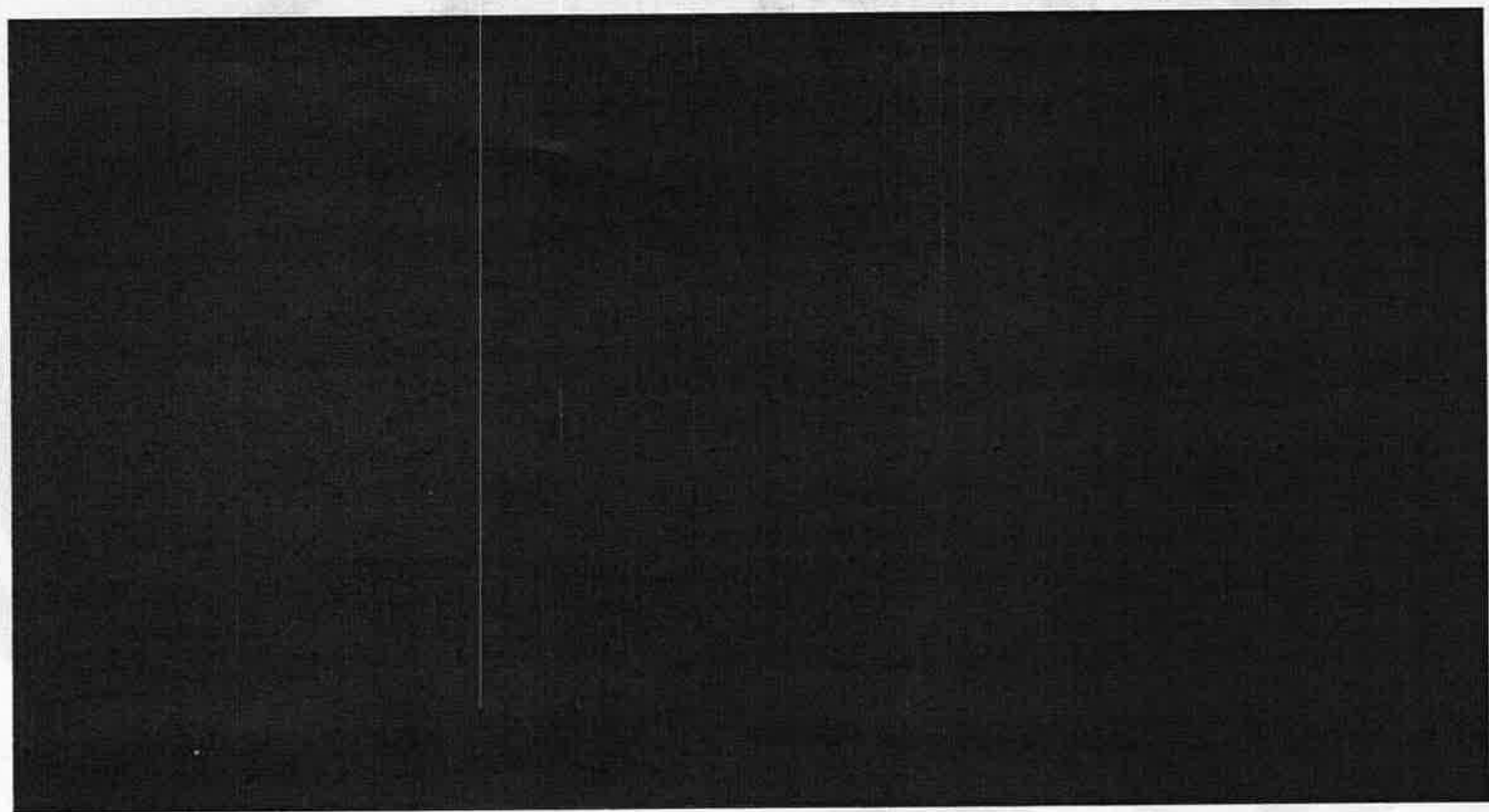


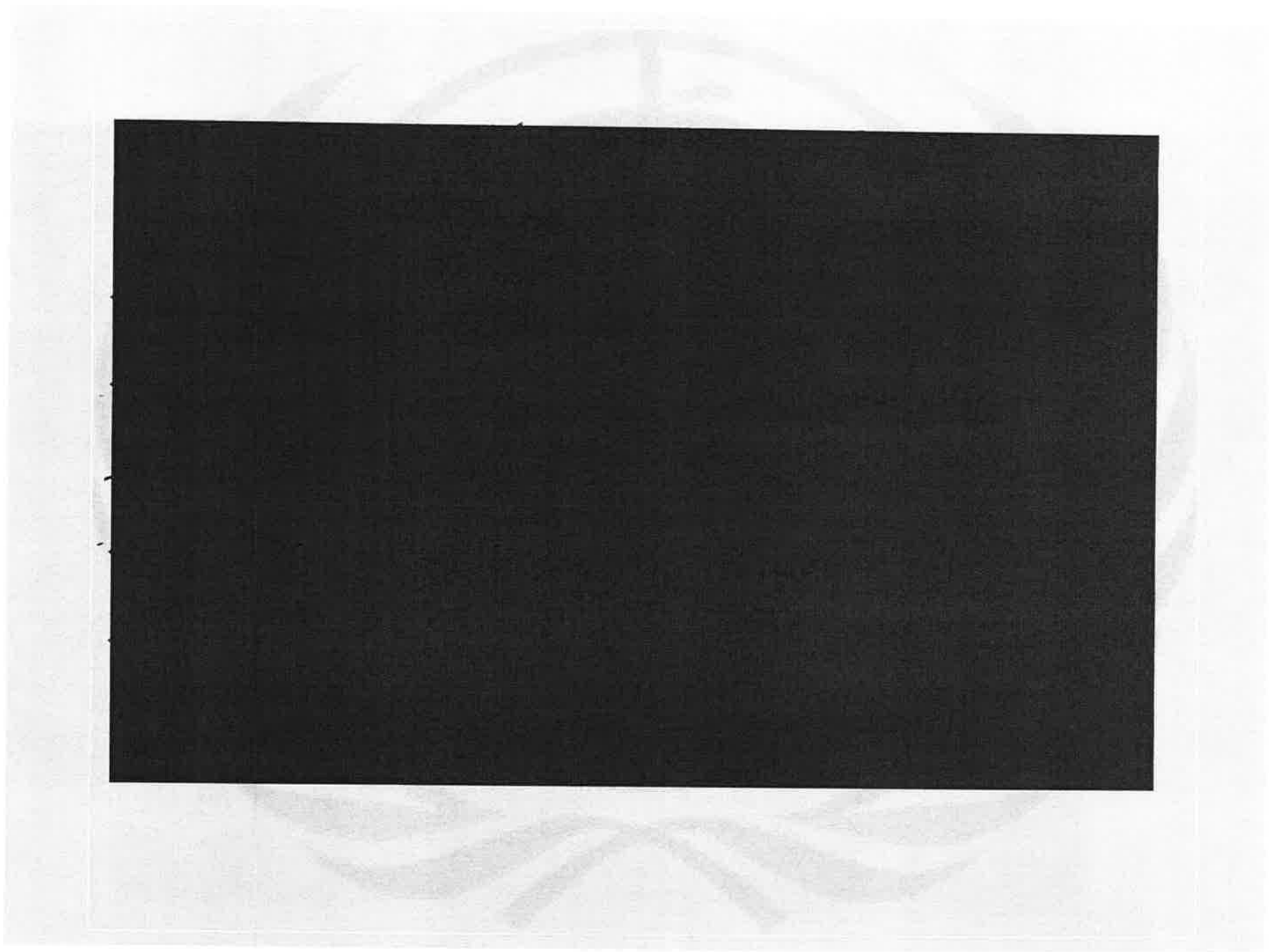
UNODC

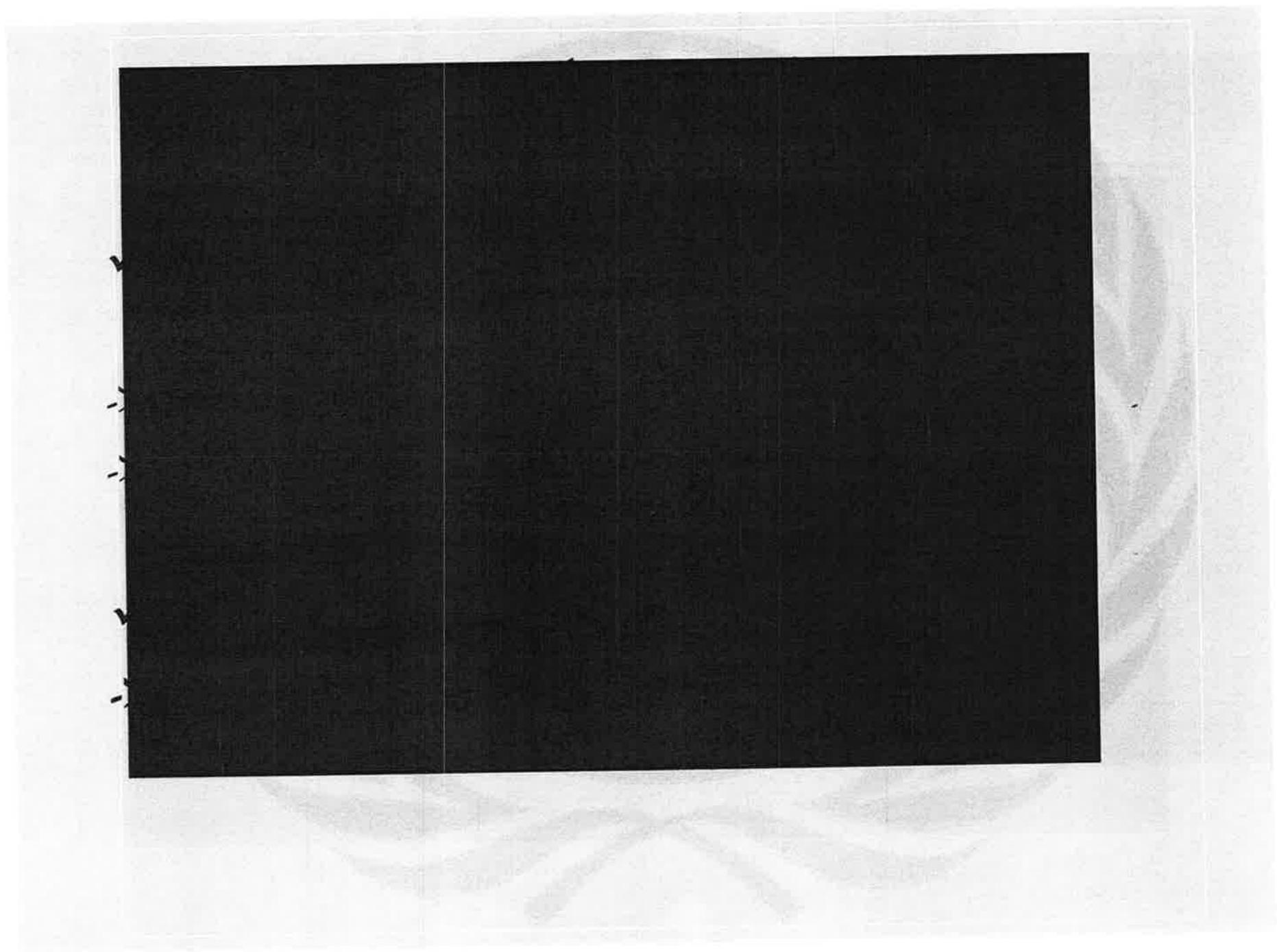
United Nations Office on Drugs and Crime

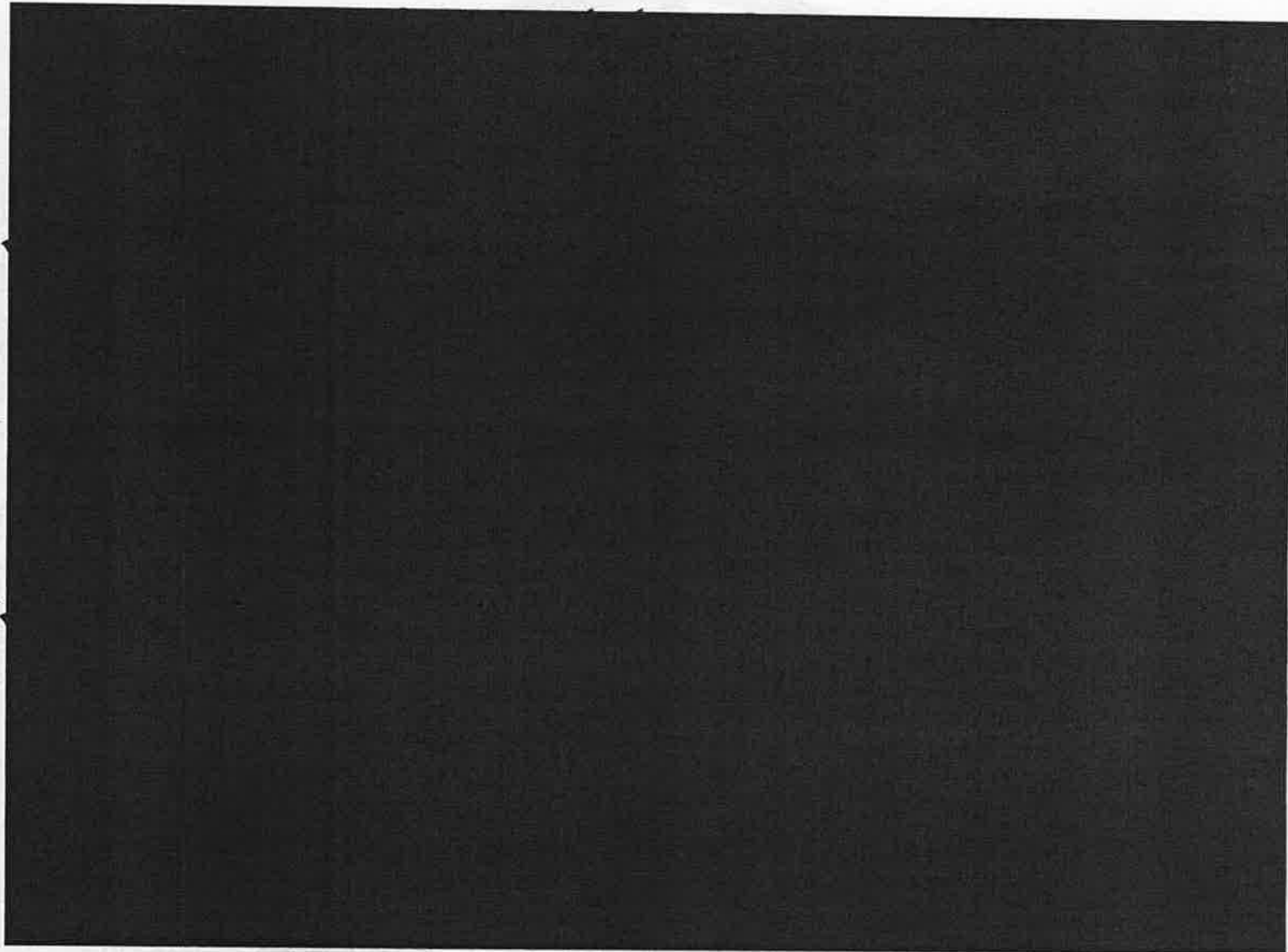
**JOINT INVESTIGATION
TEAMS**

Pristina, 9 October 2018







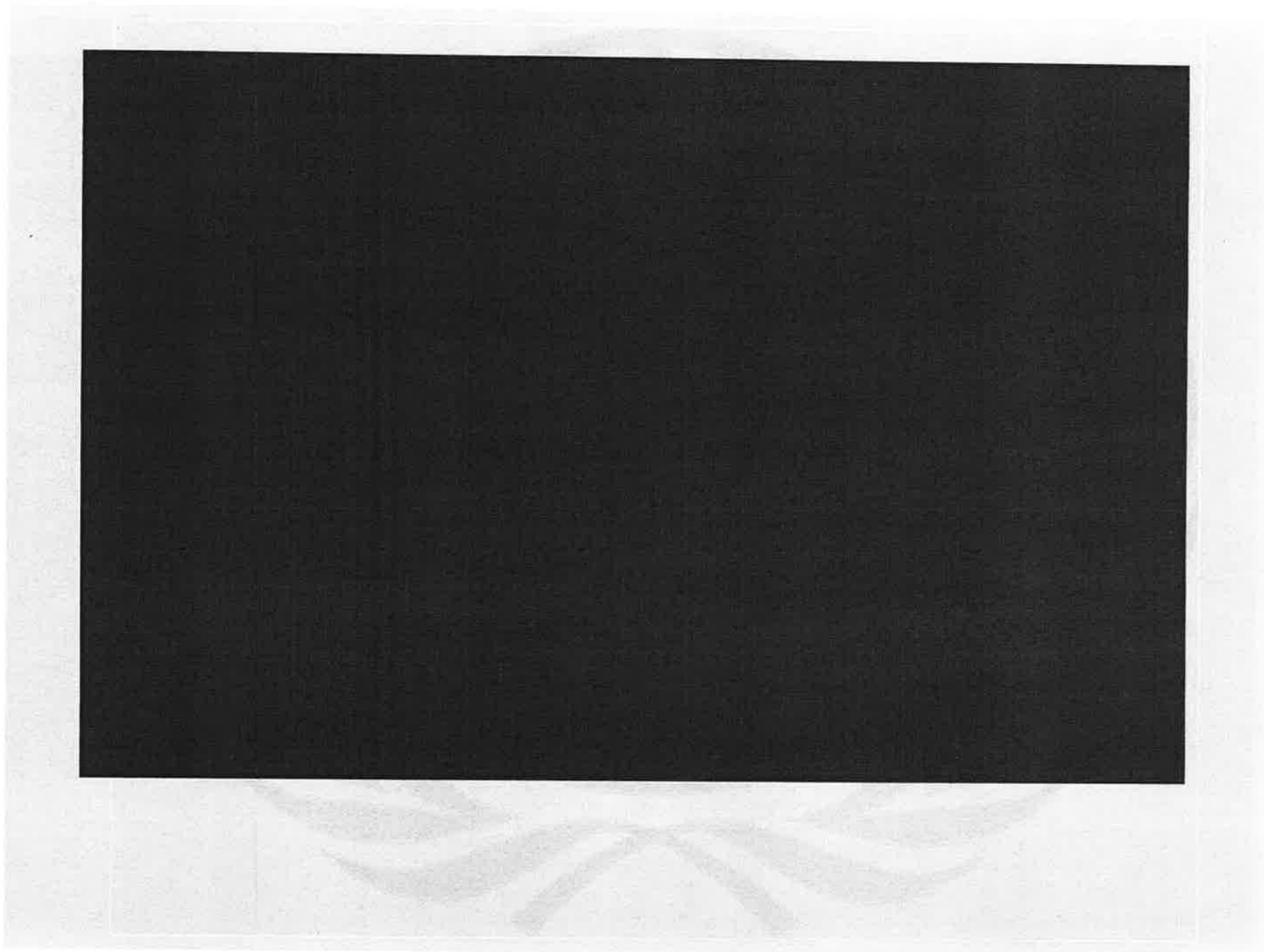


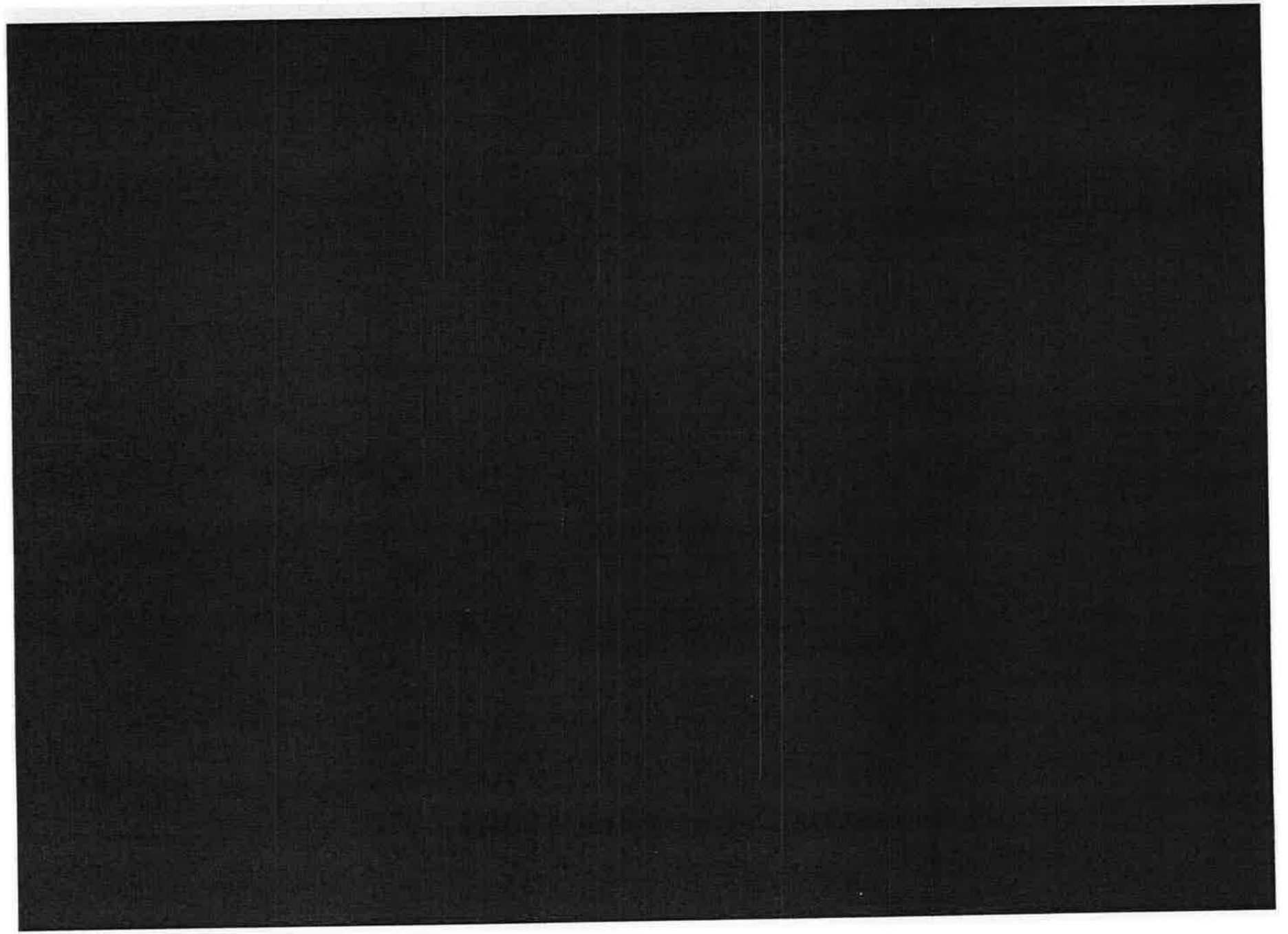
OR

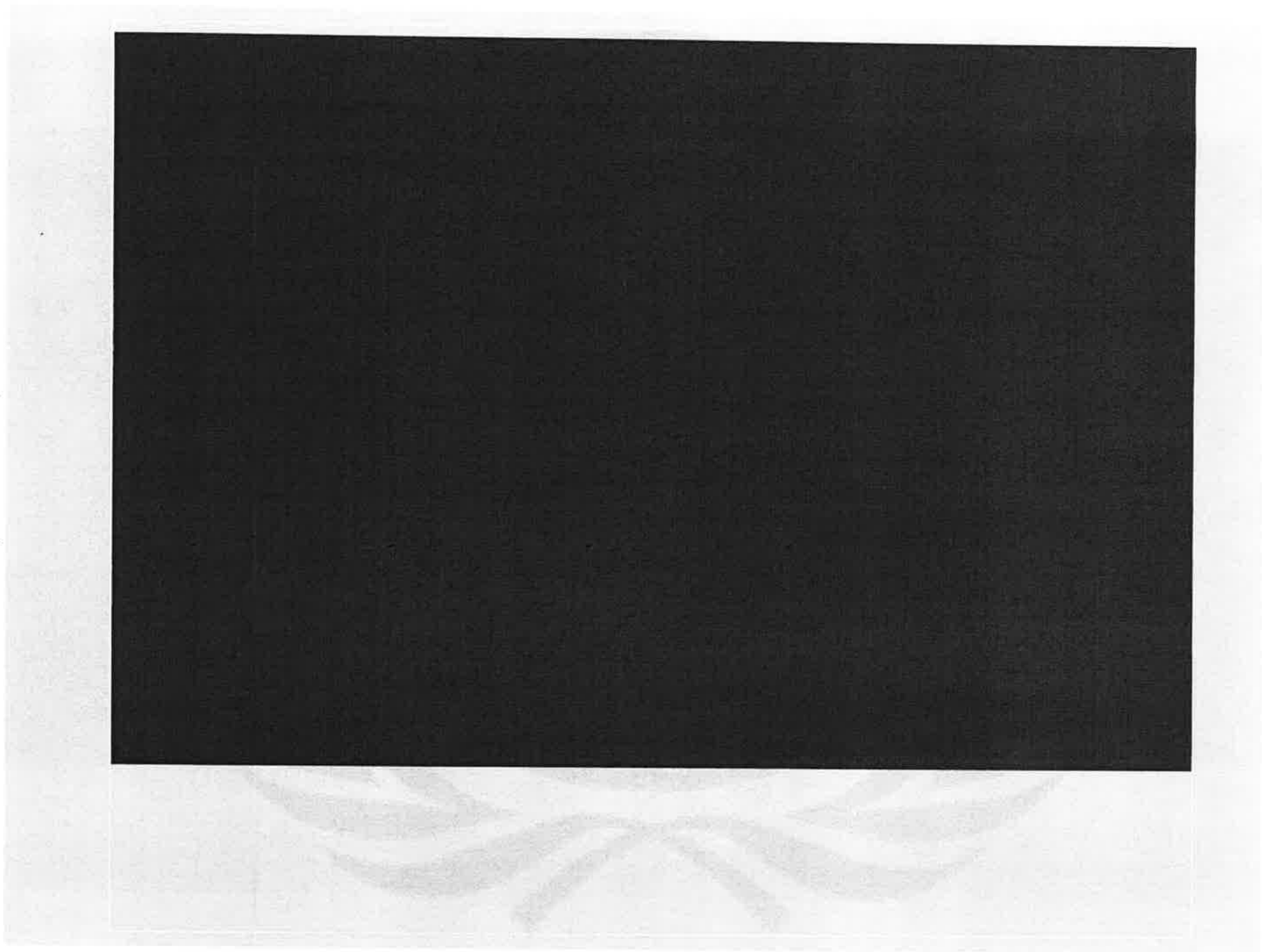
✓

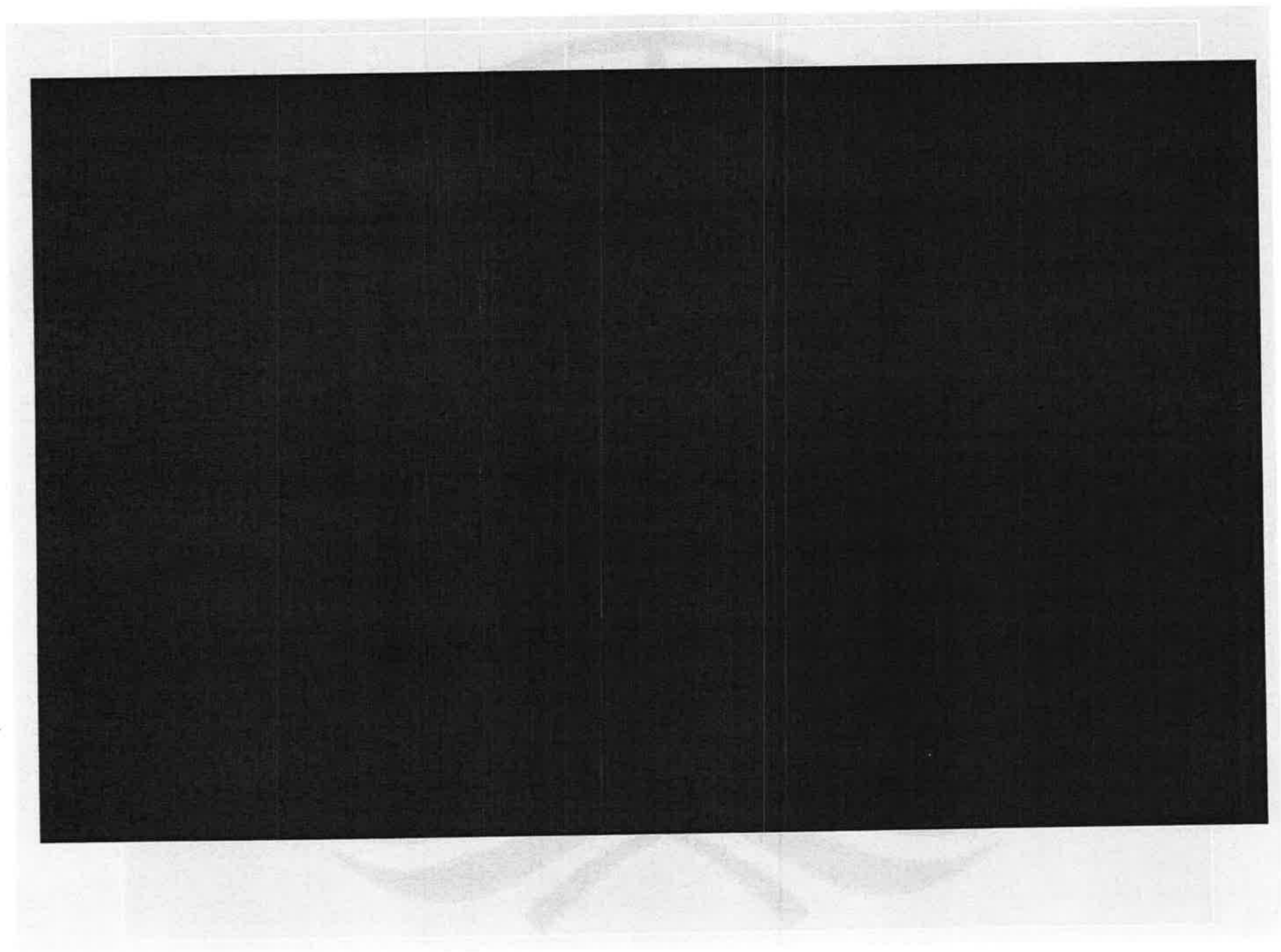
✓

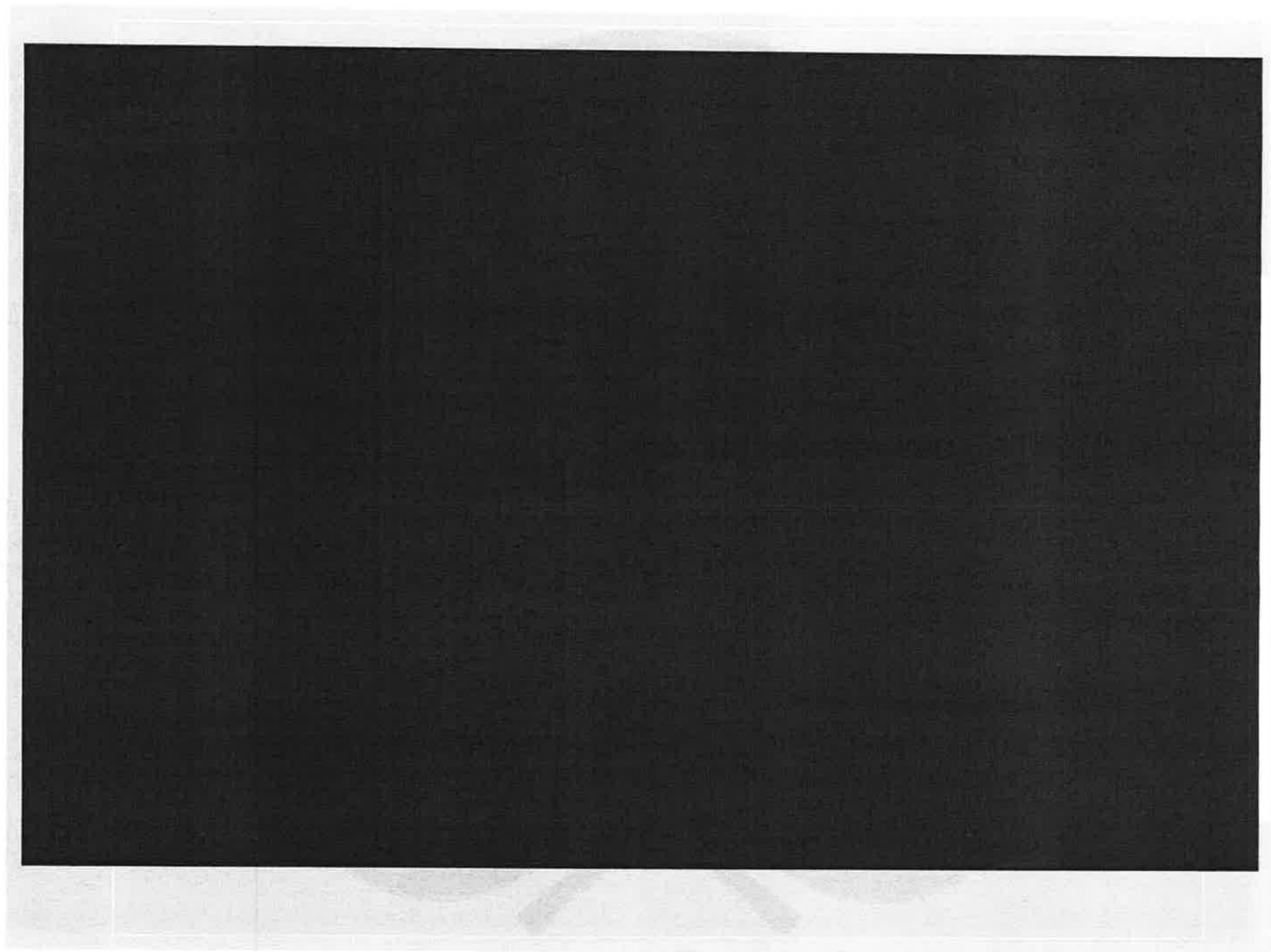
N

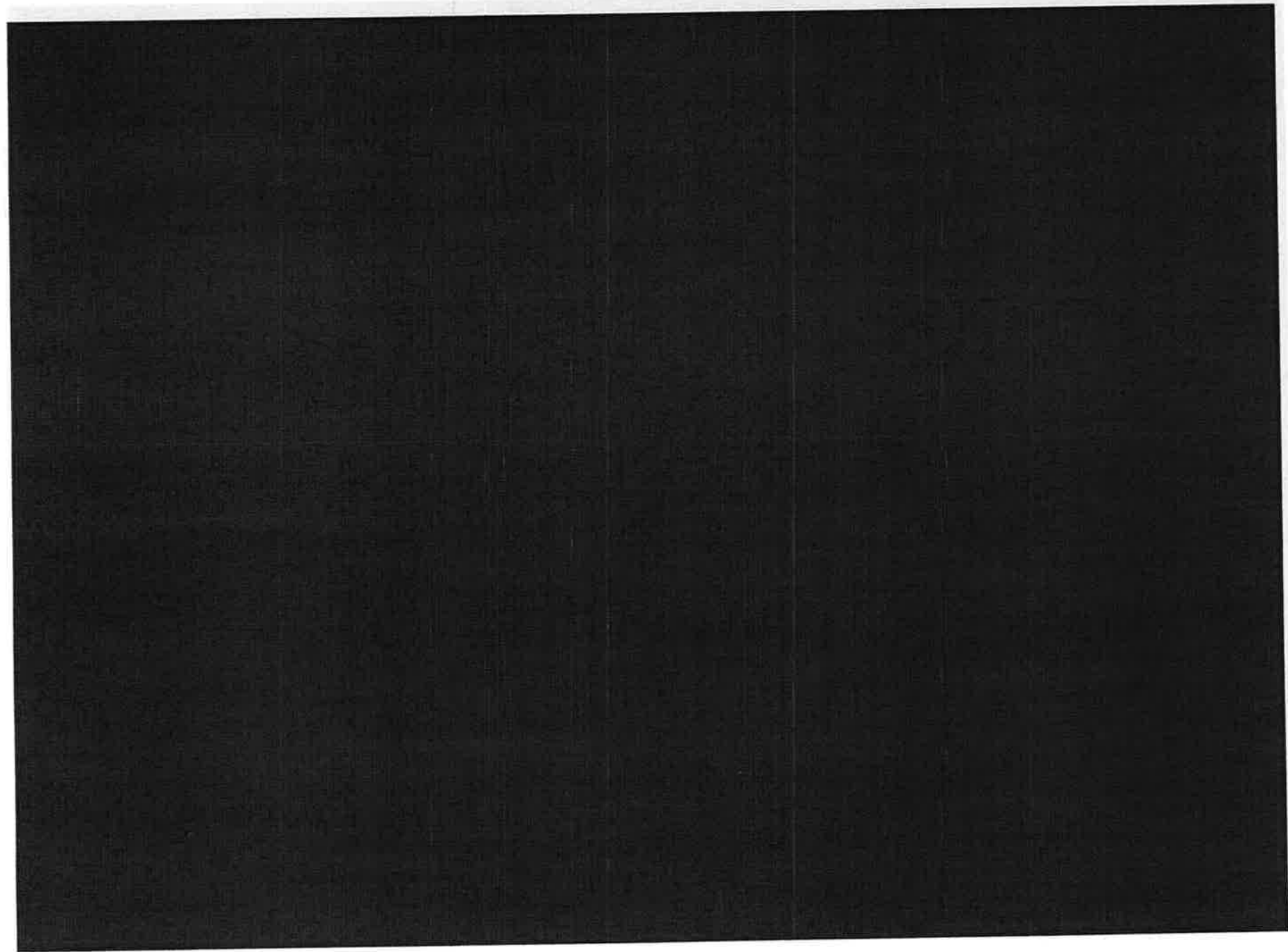


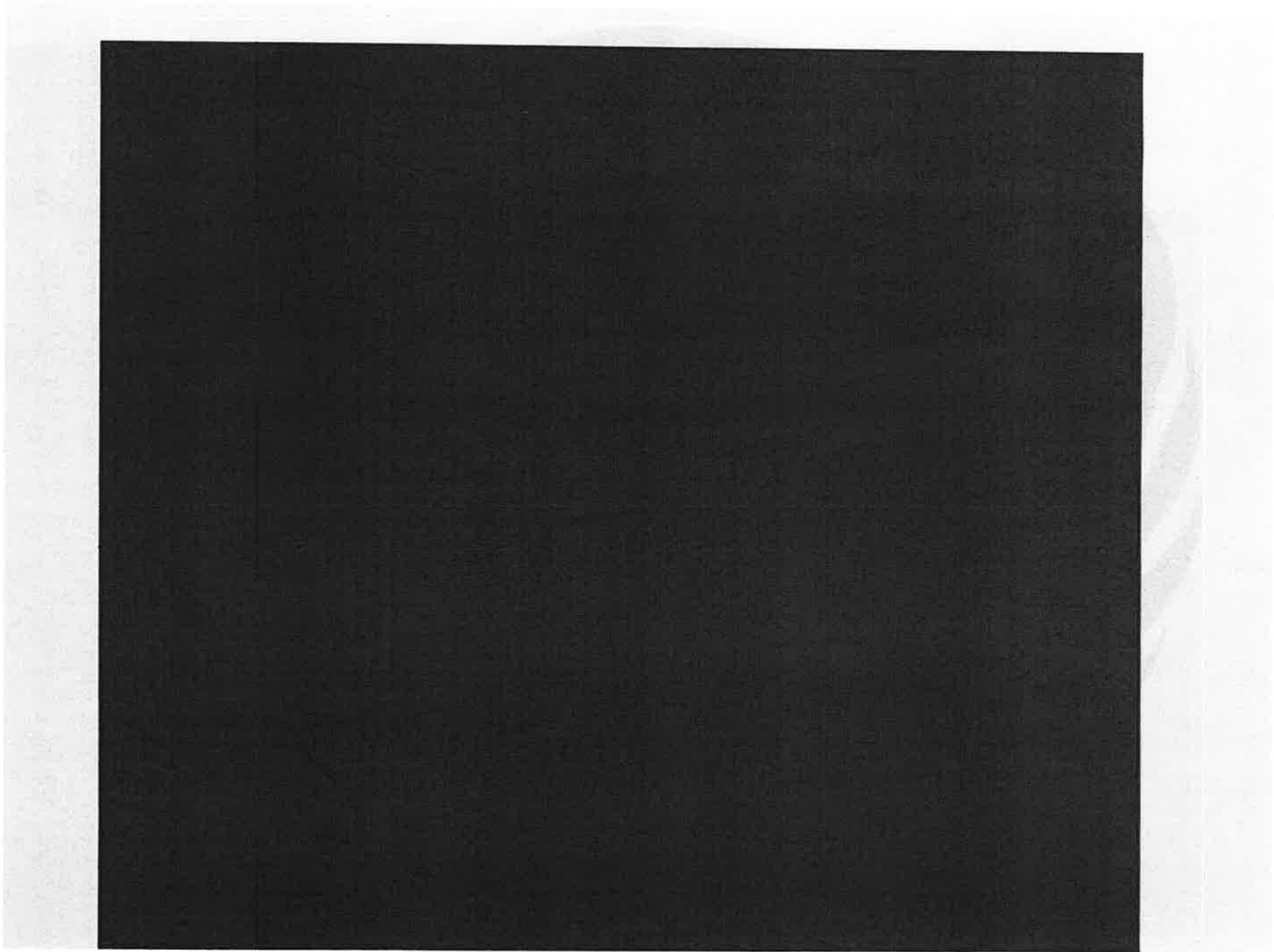


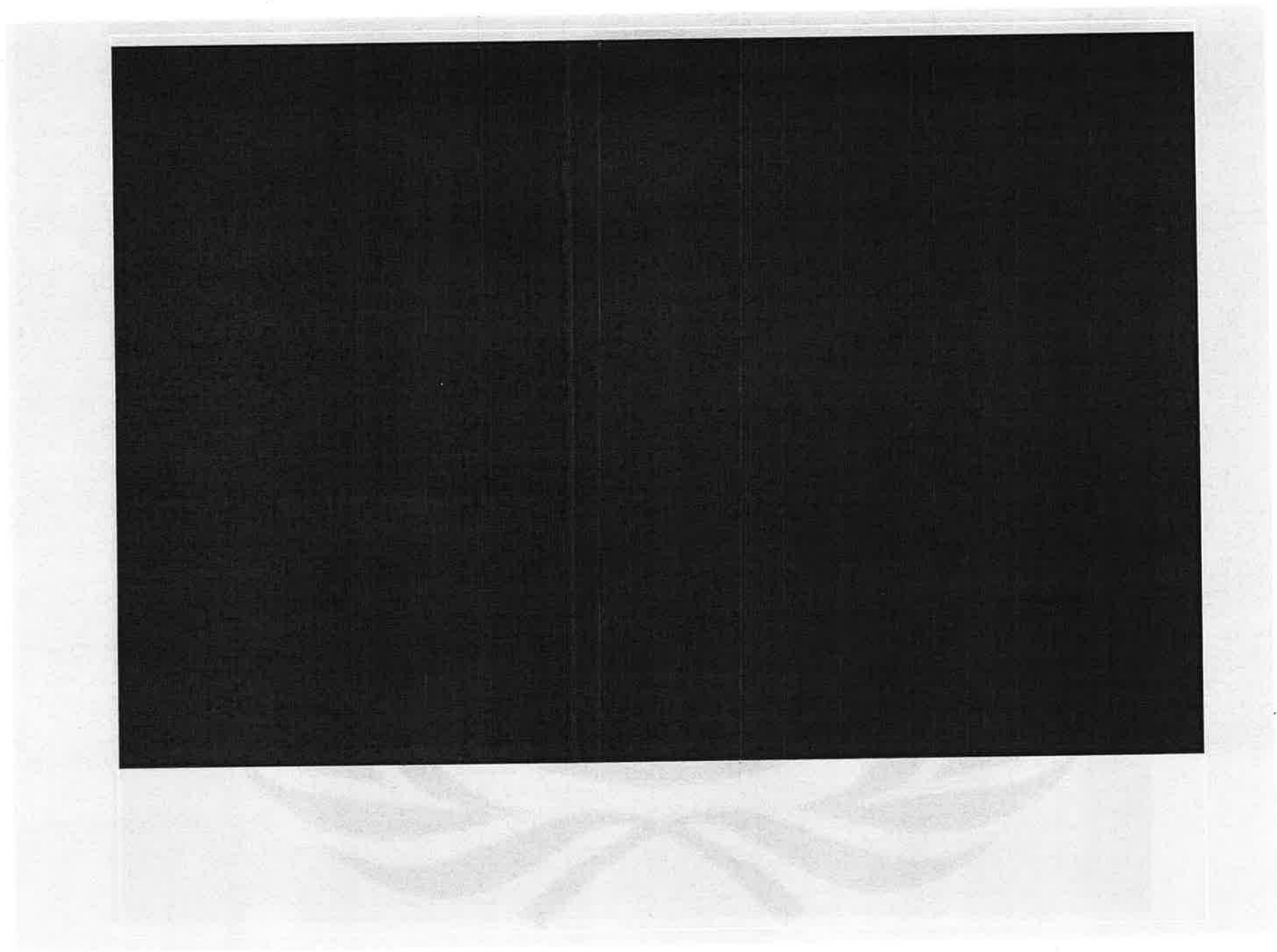


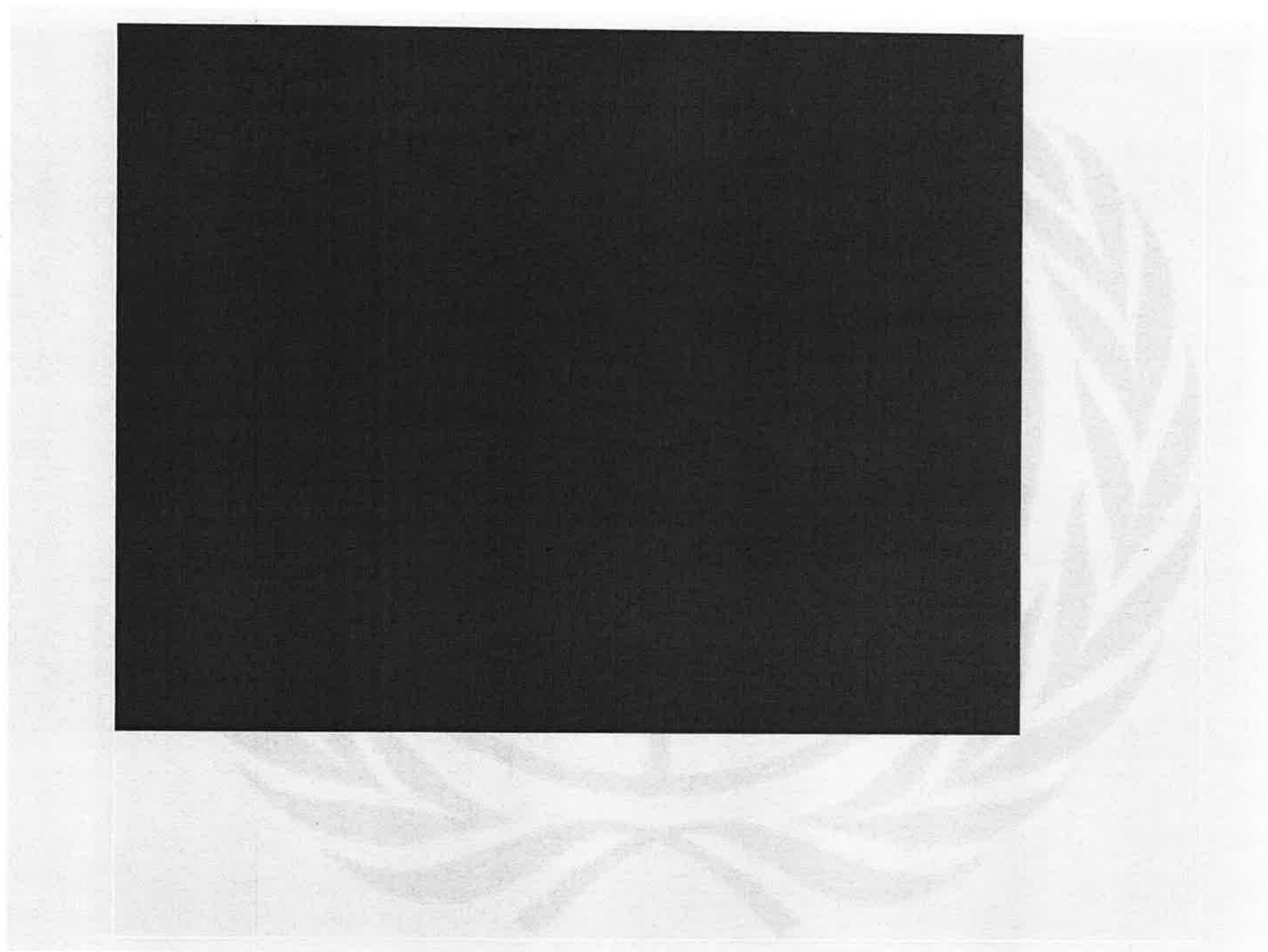


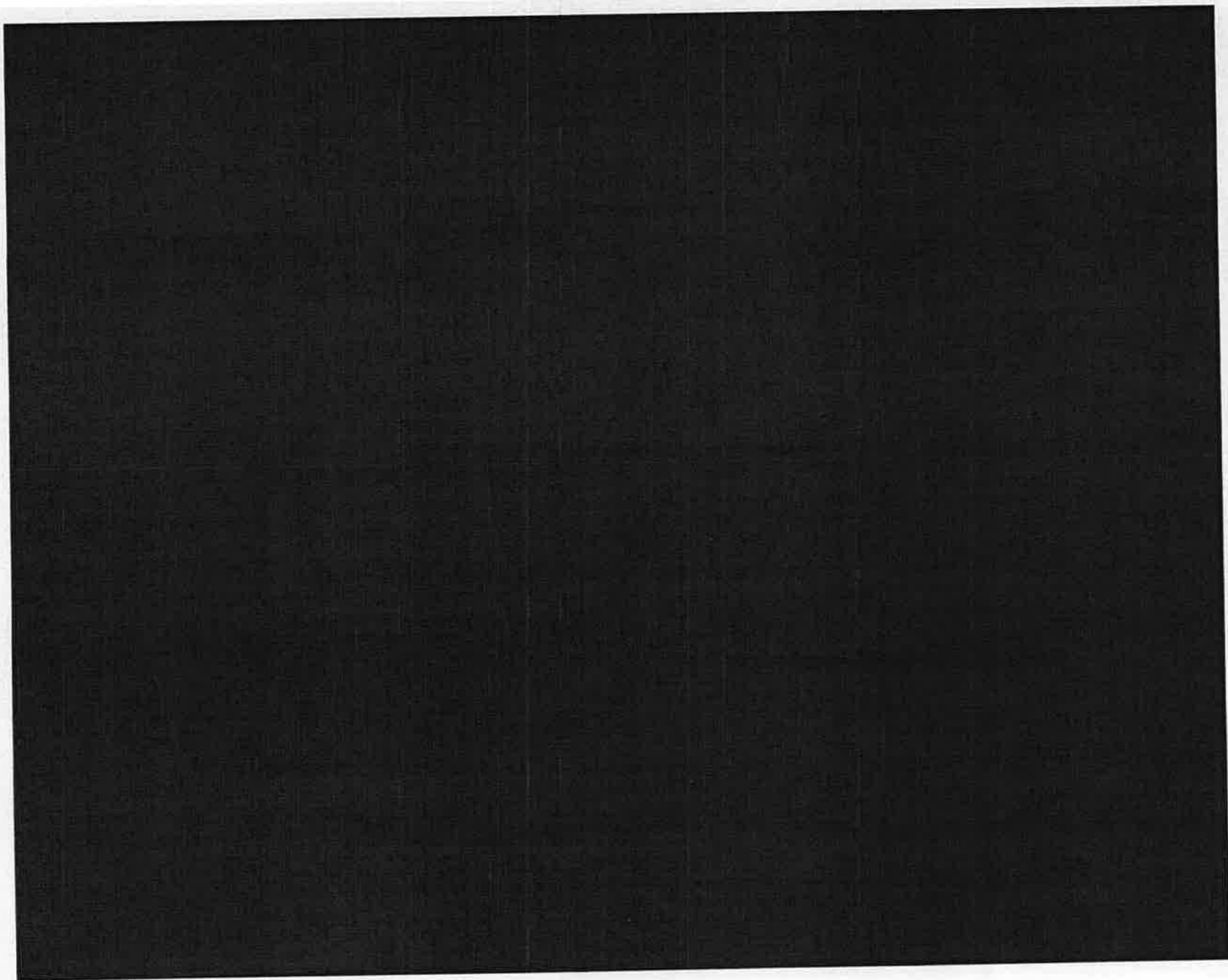


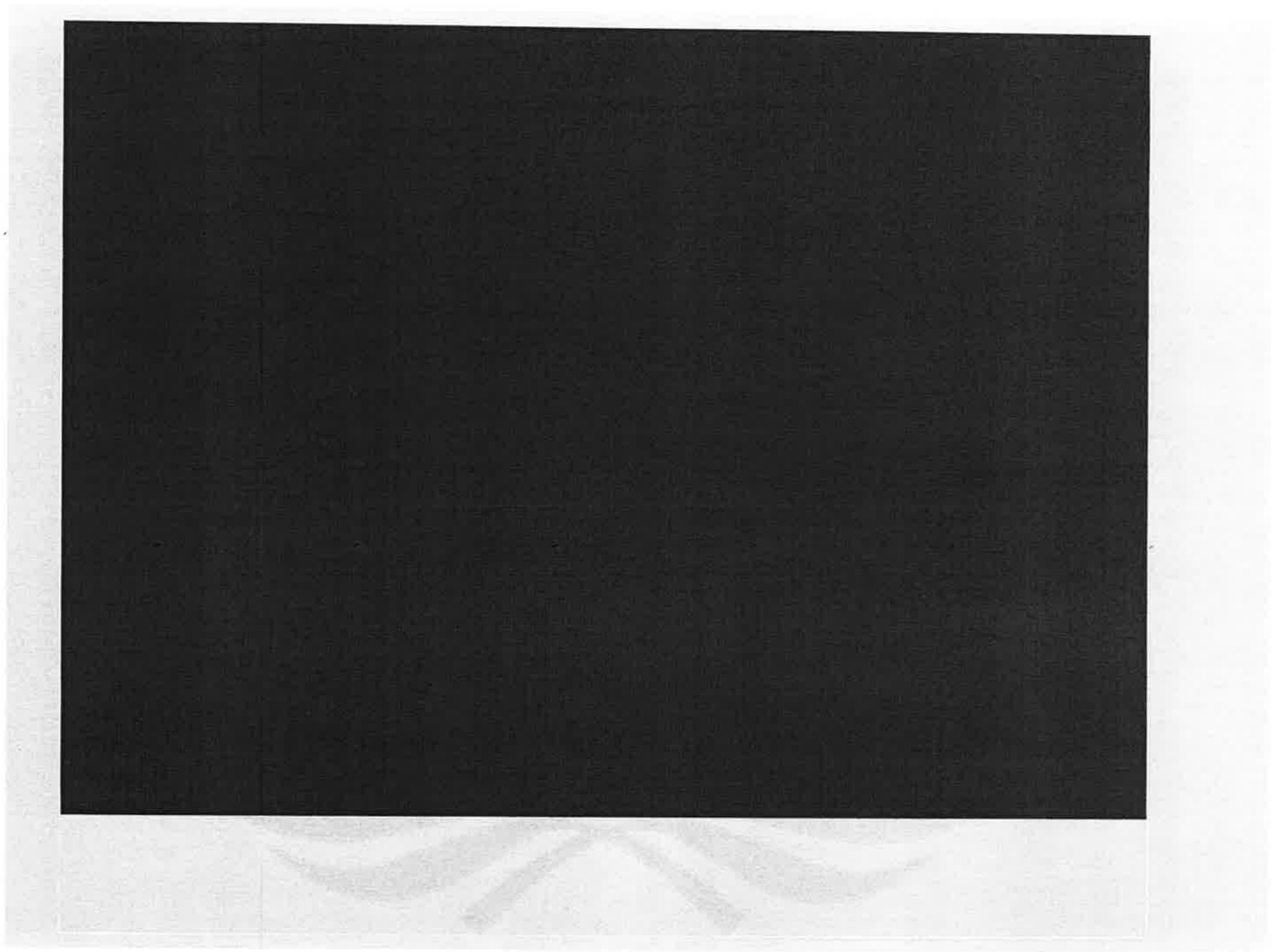


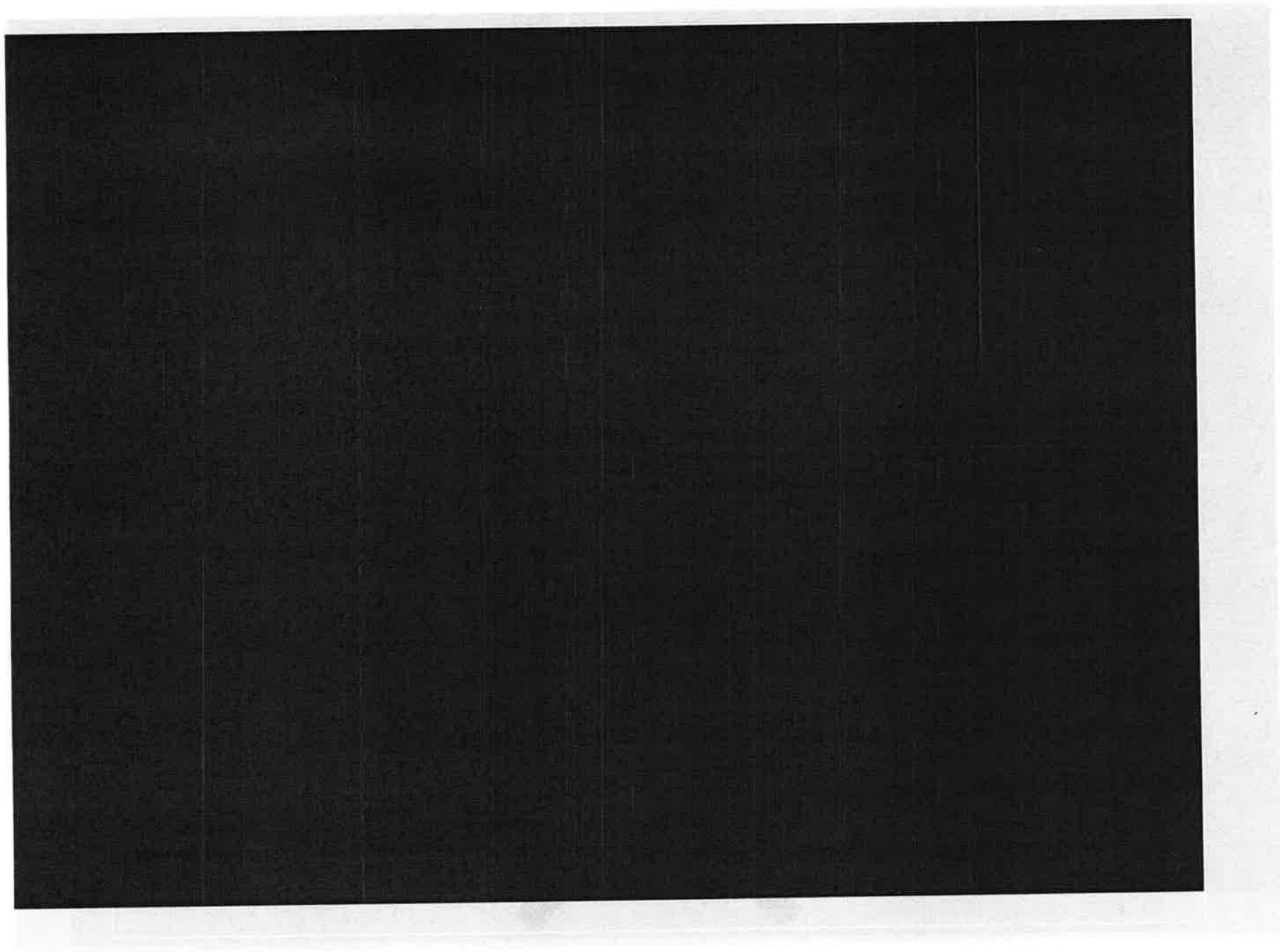


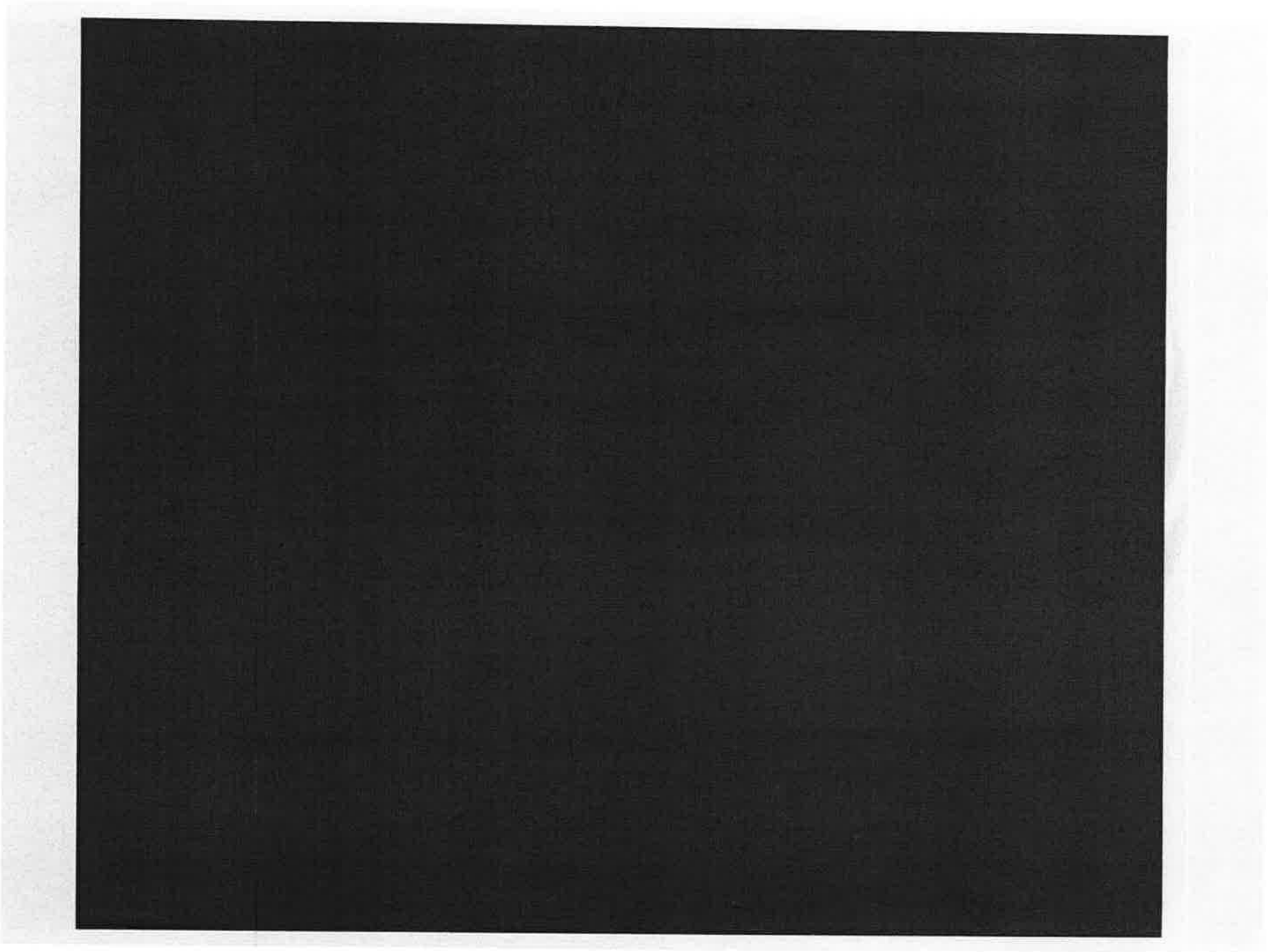


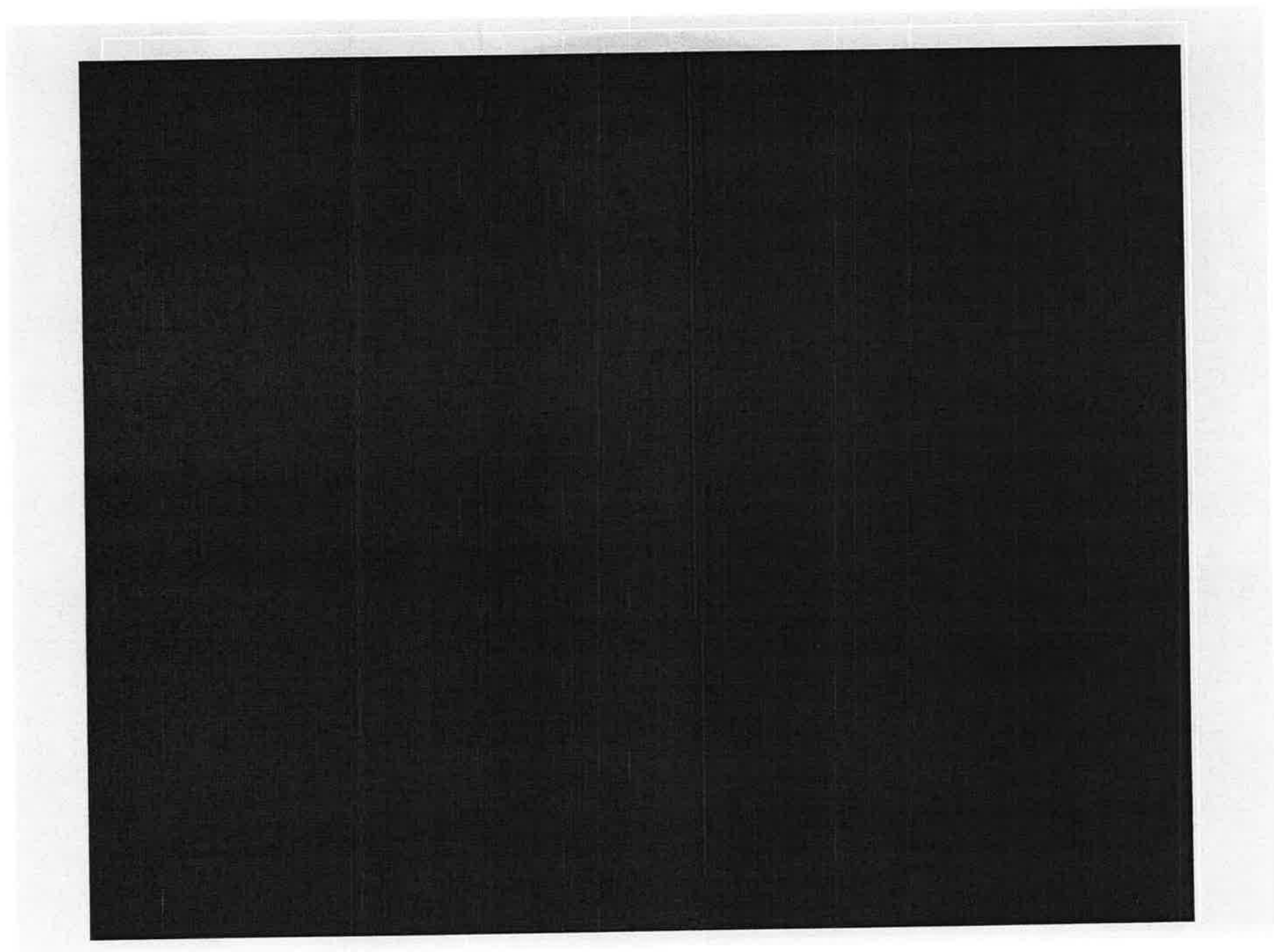


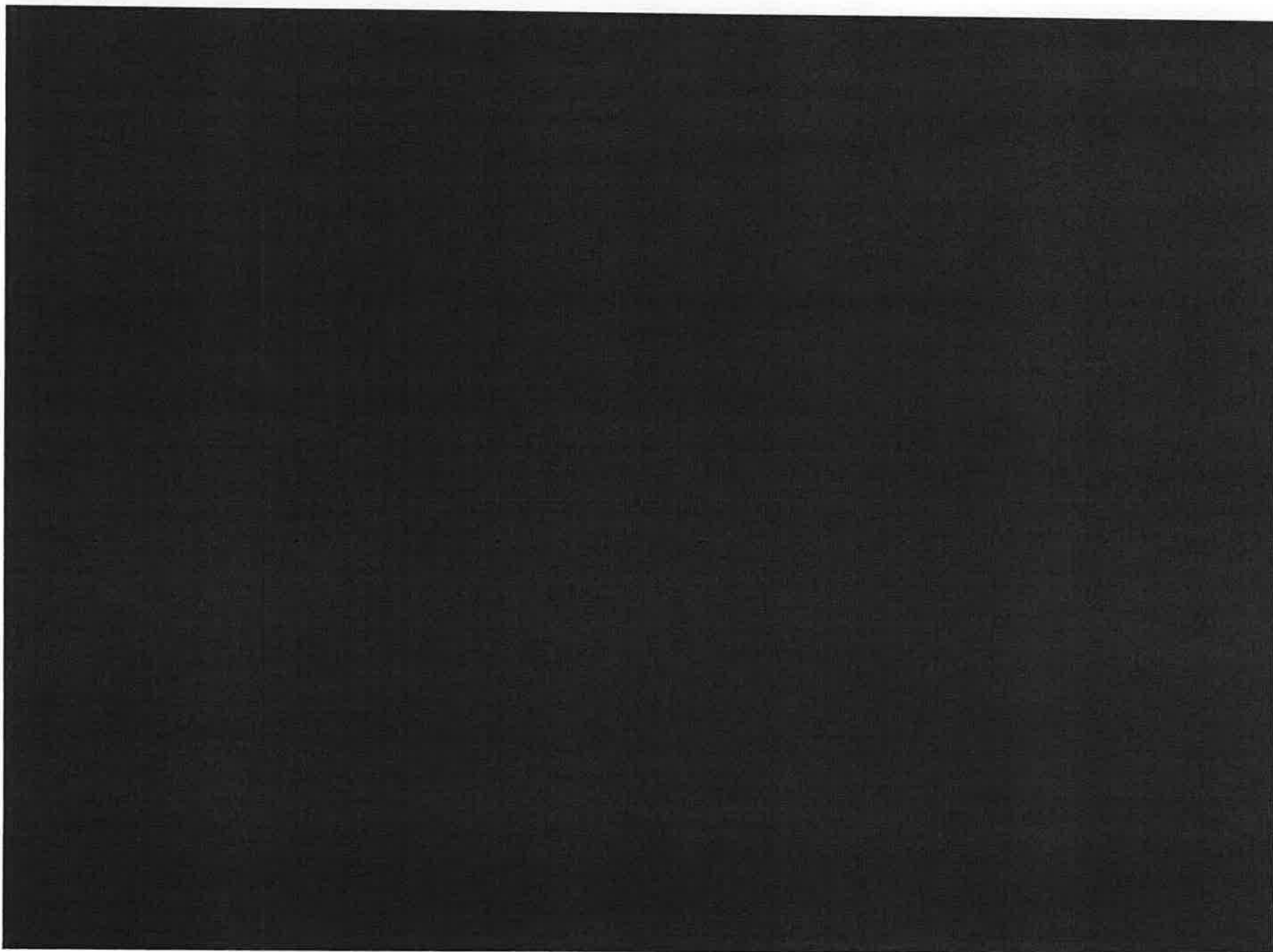


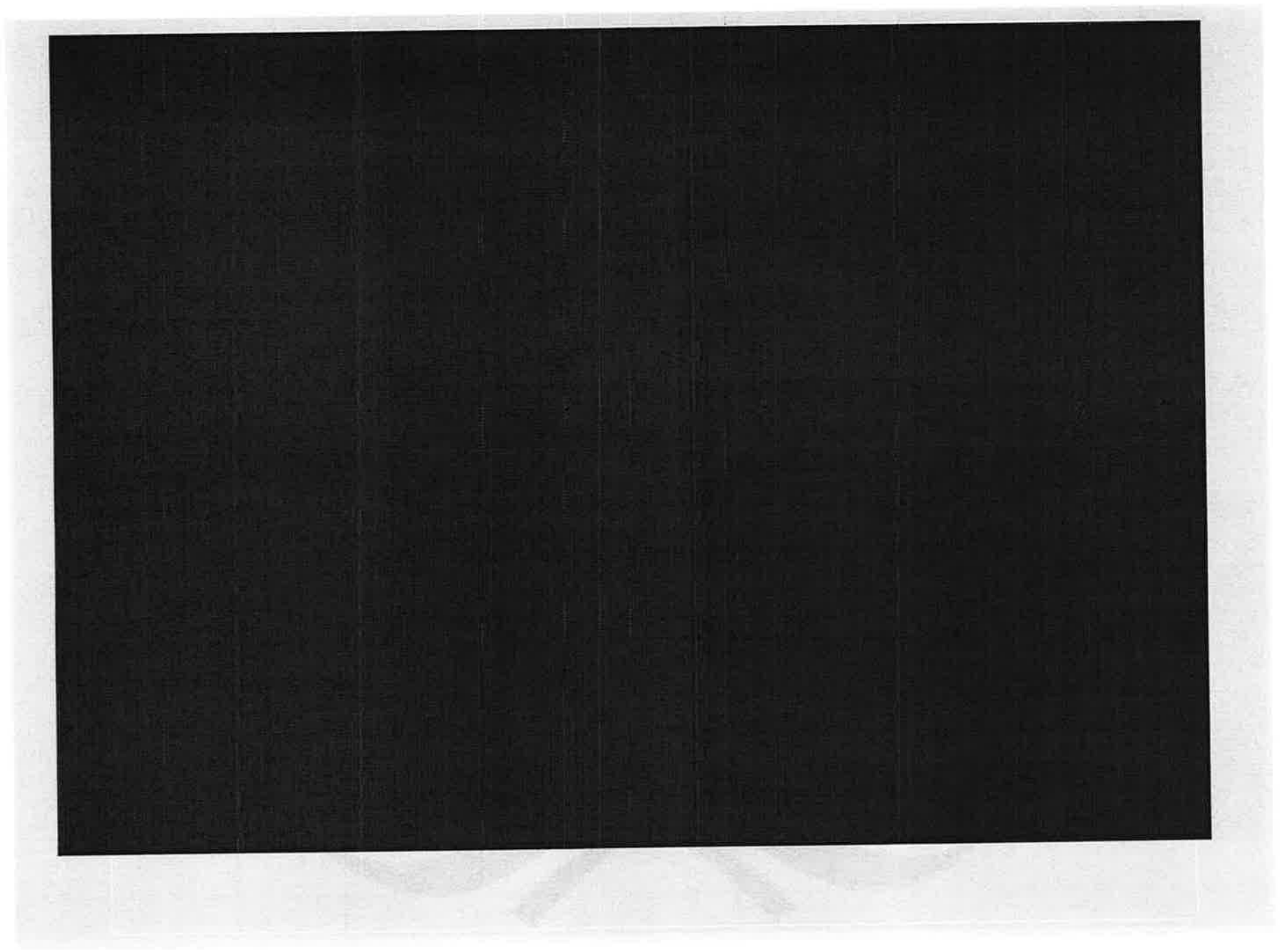


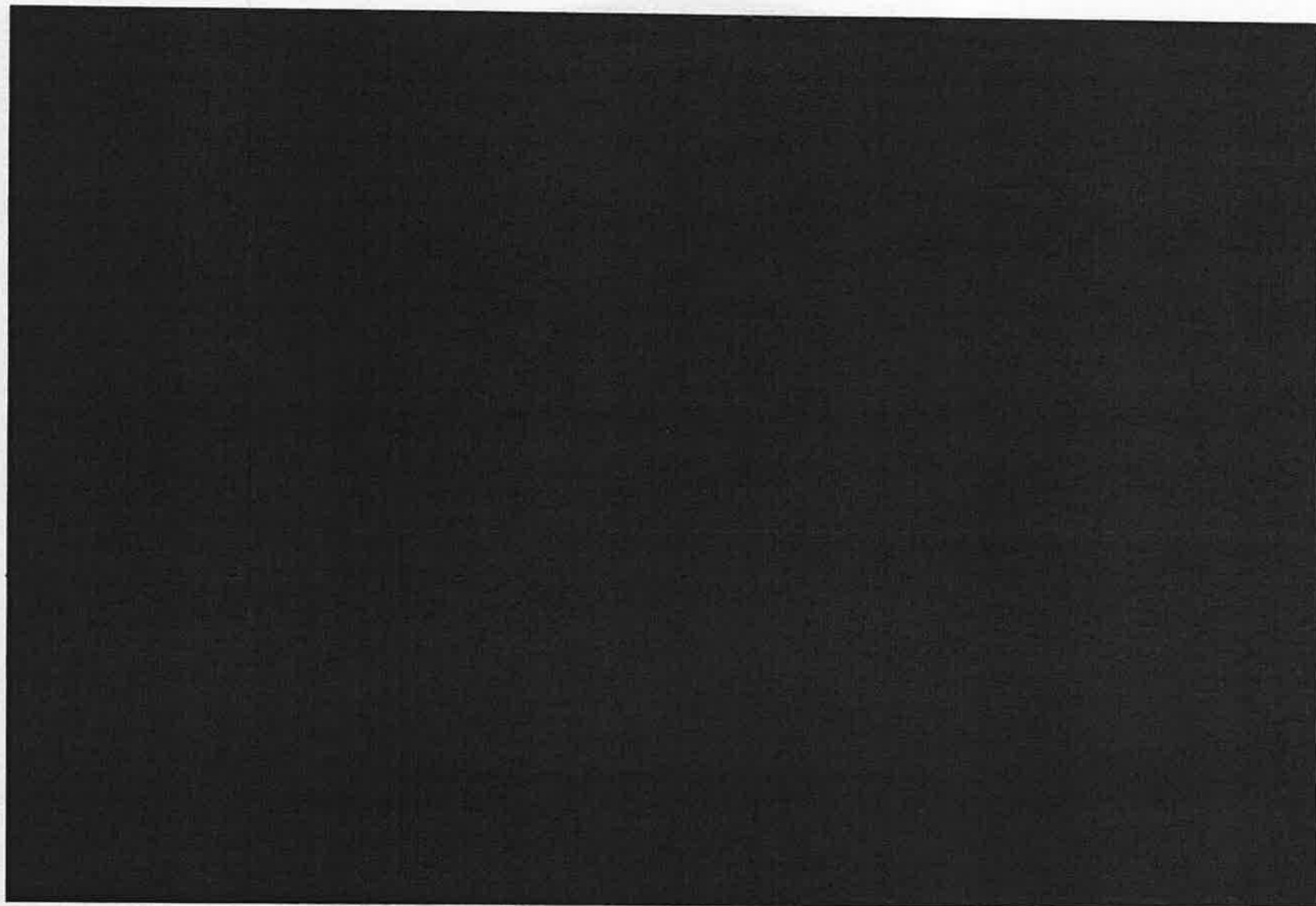


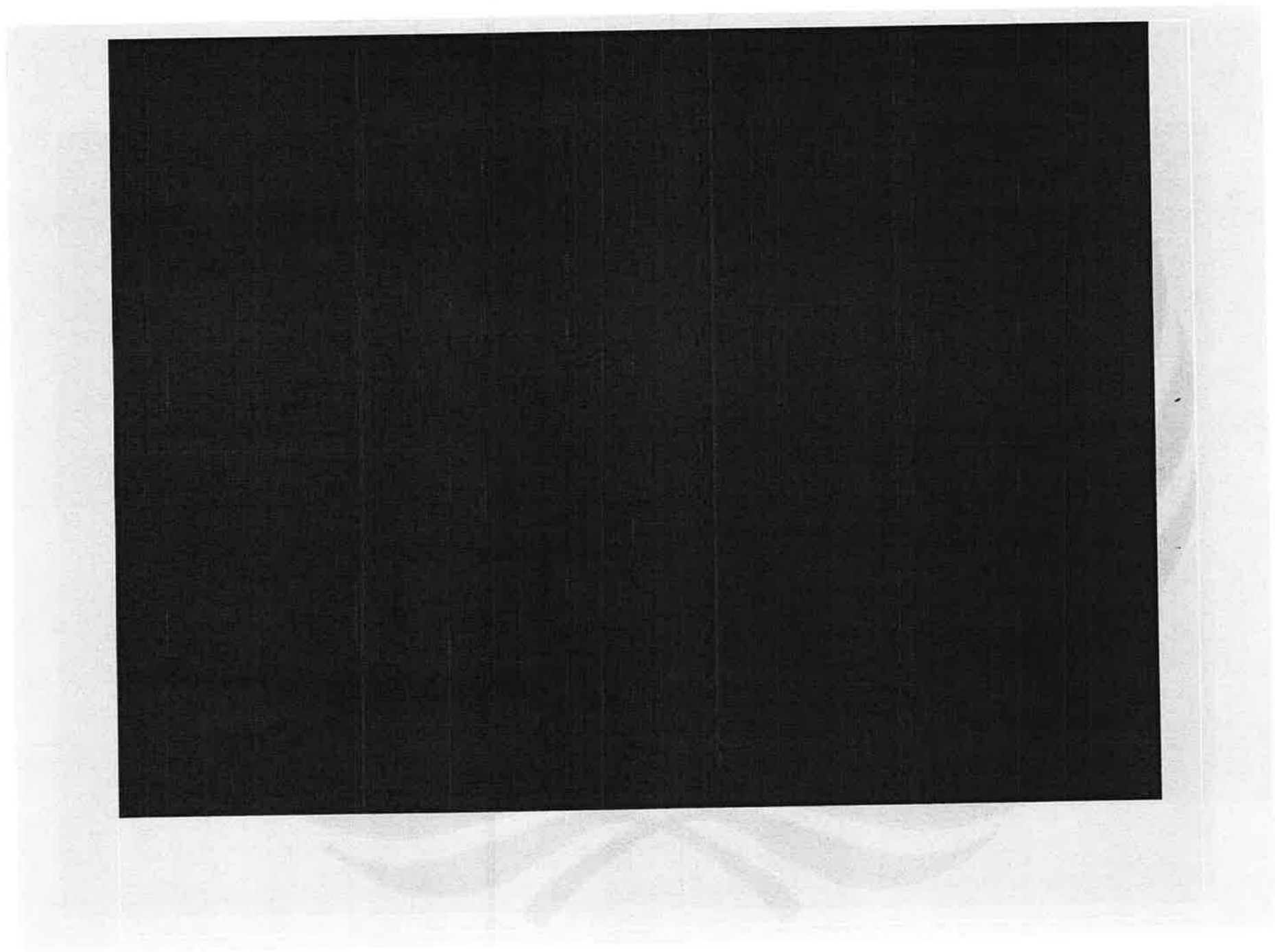


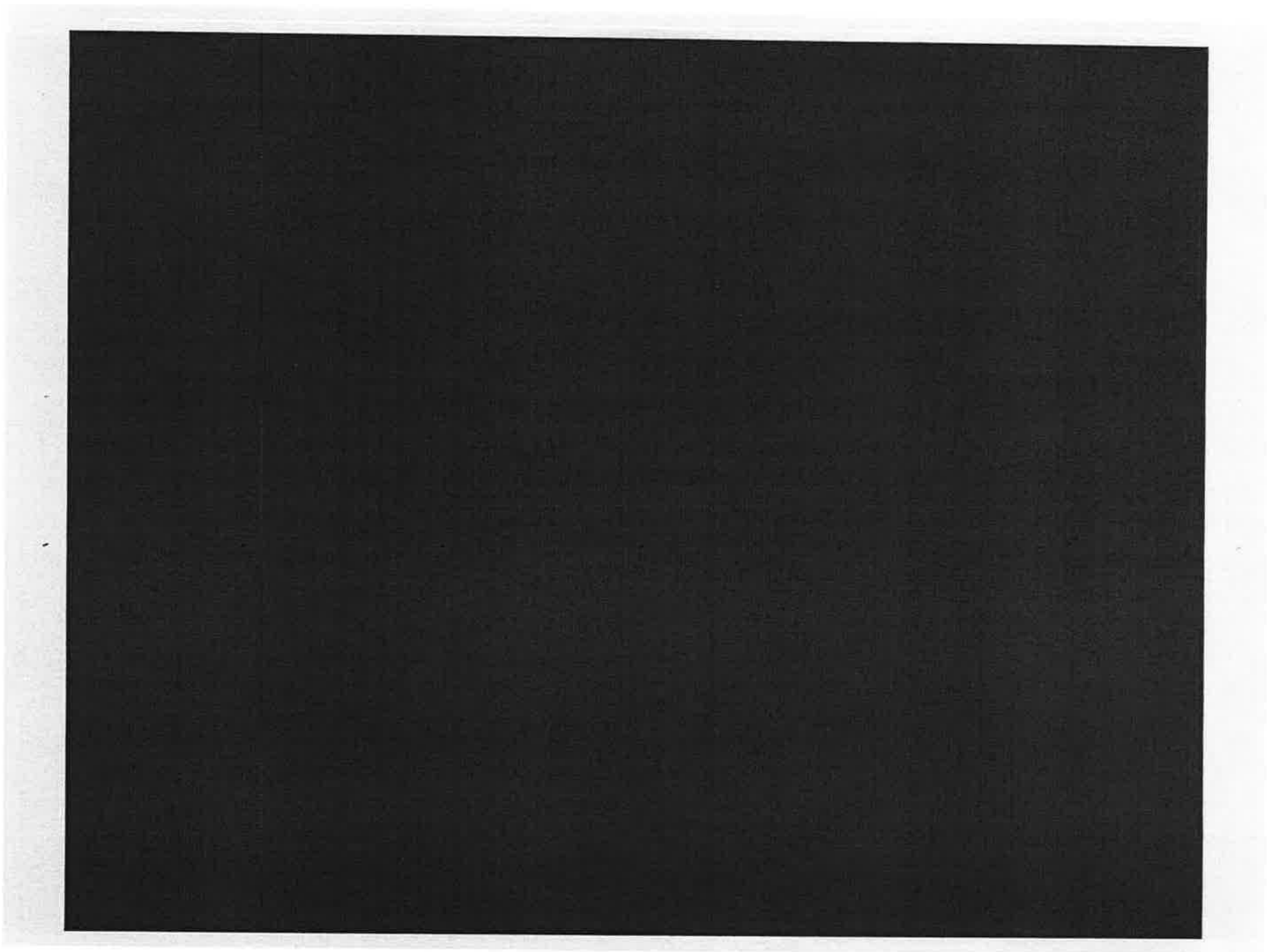




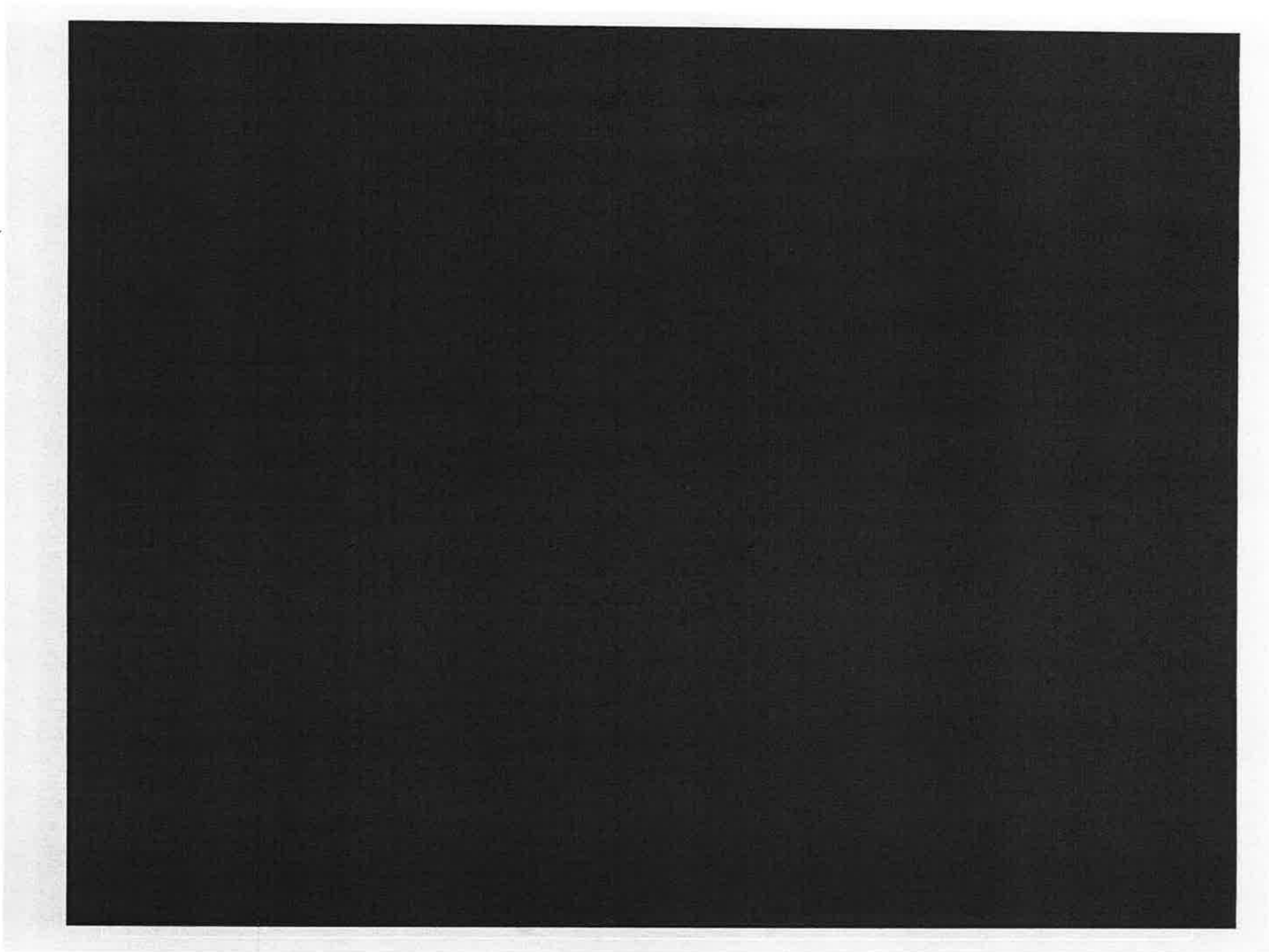


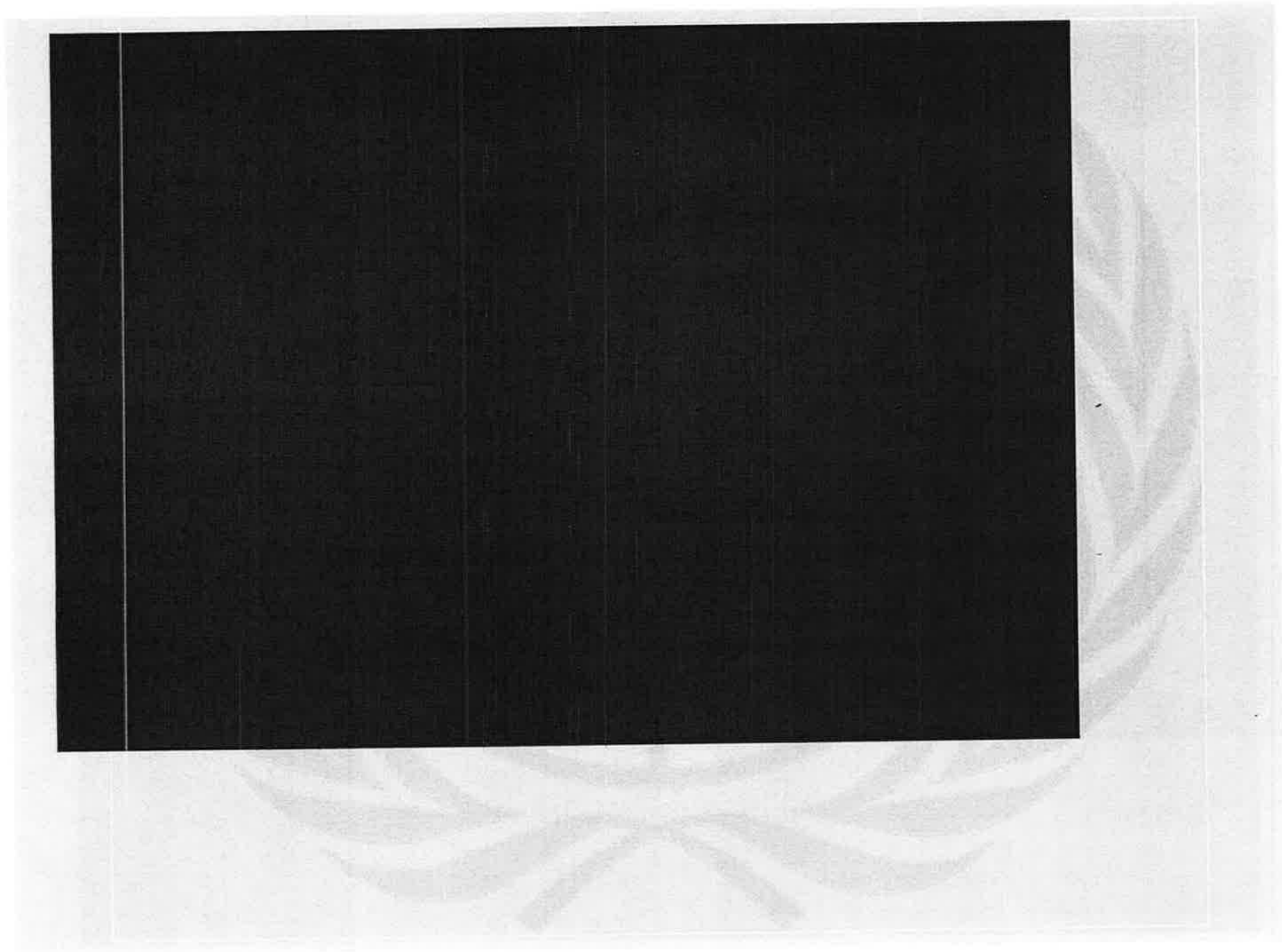








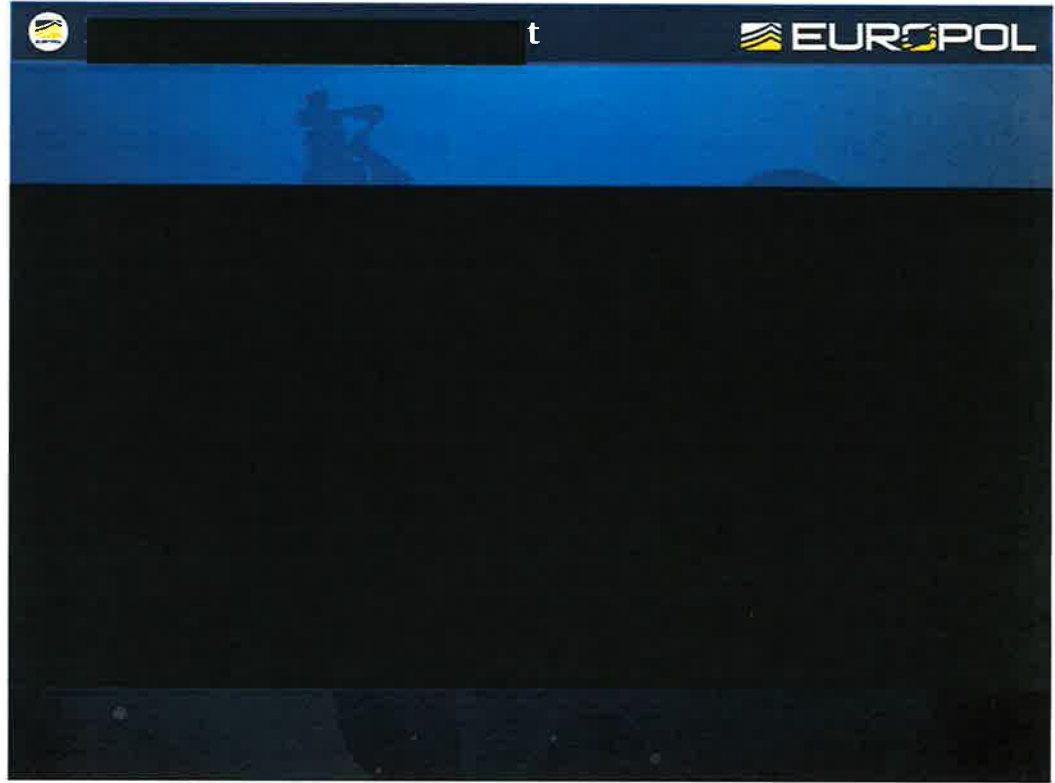
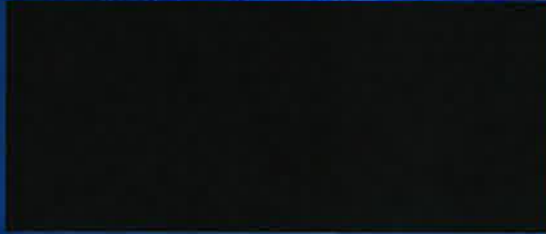


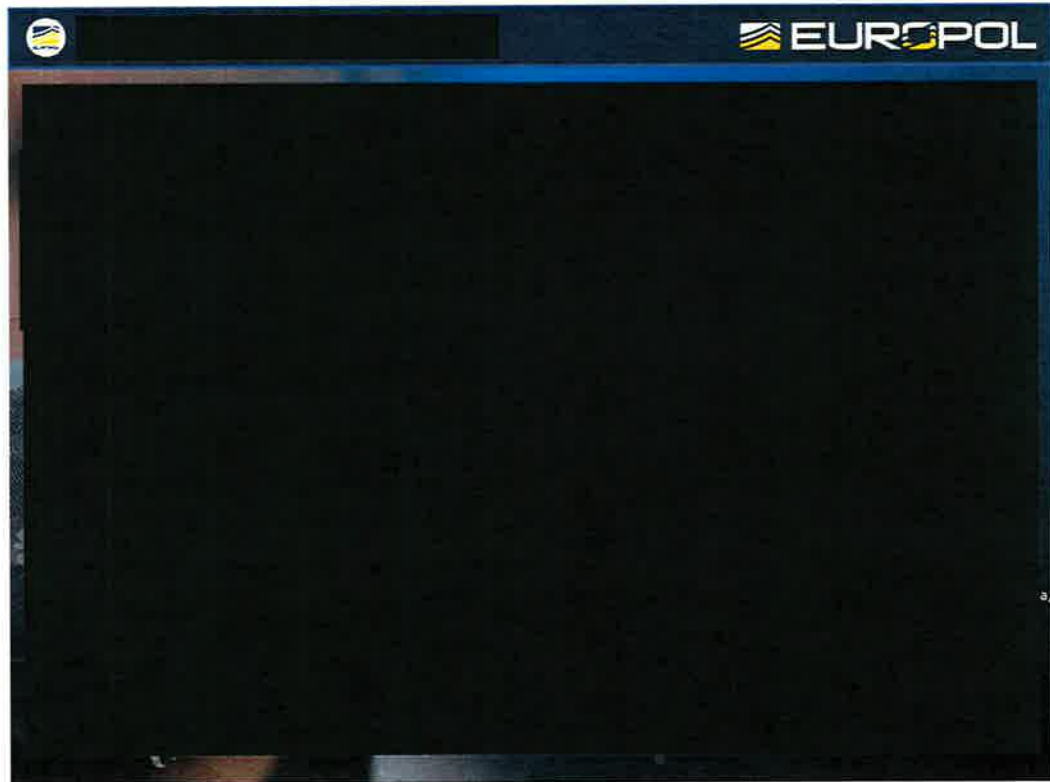


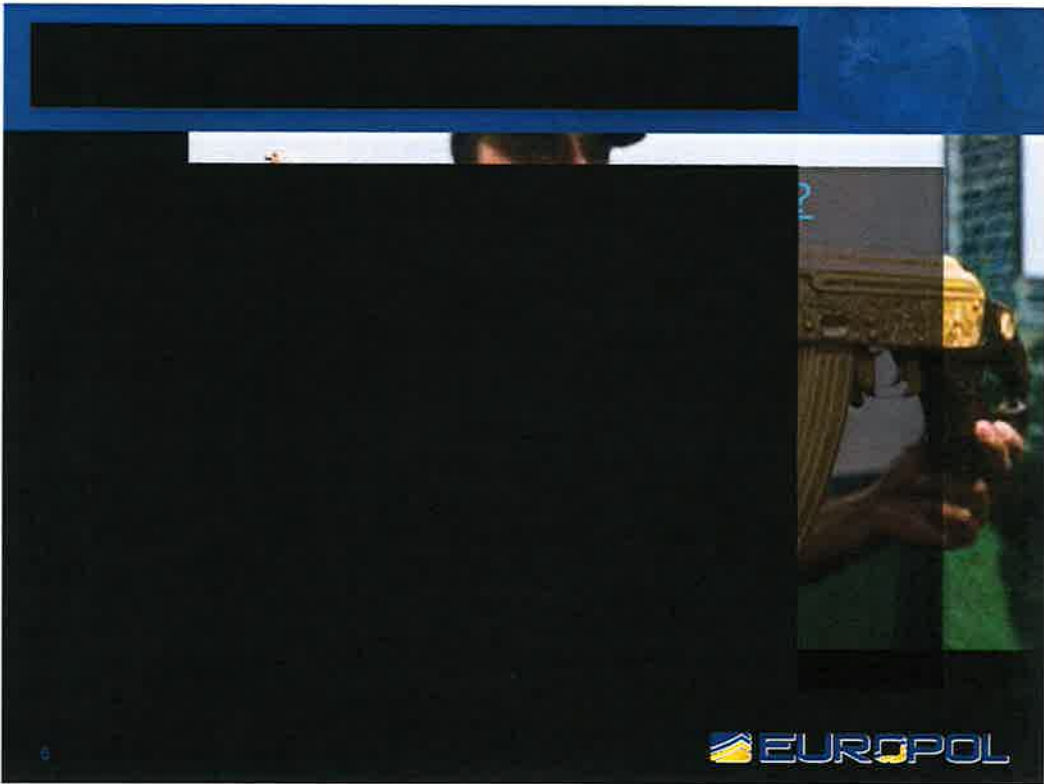
Thank you!

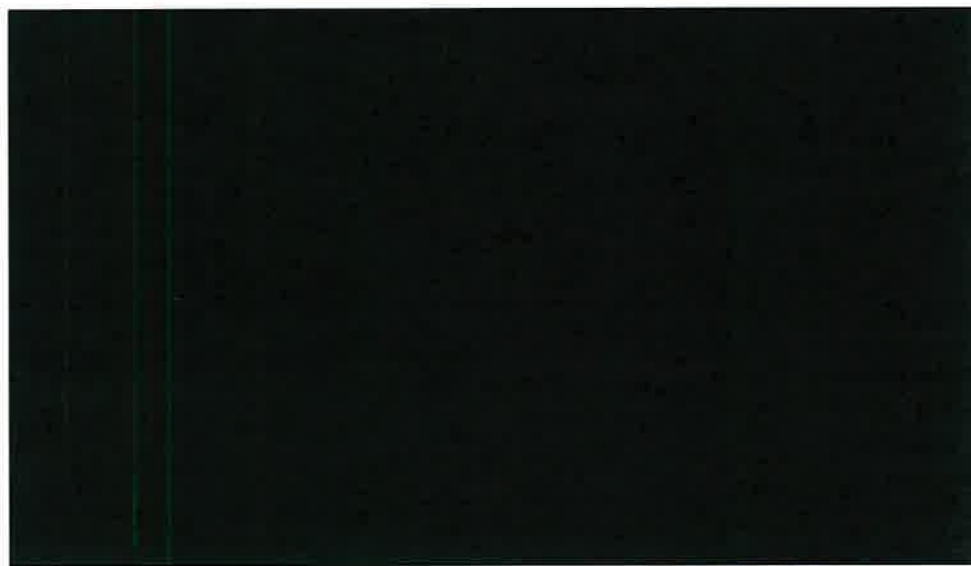
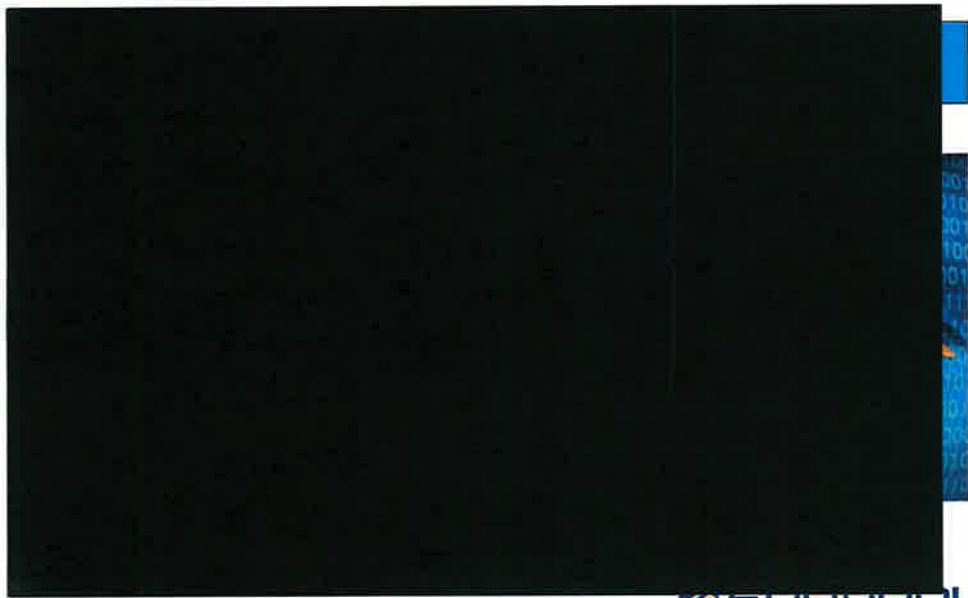


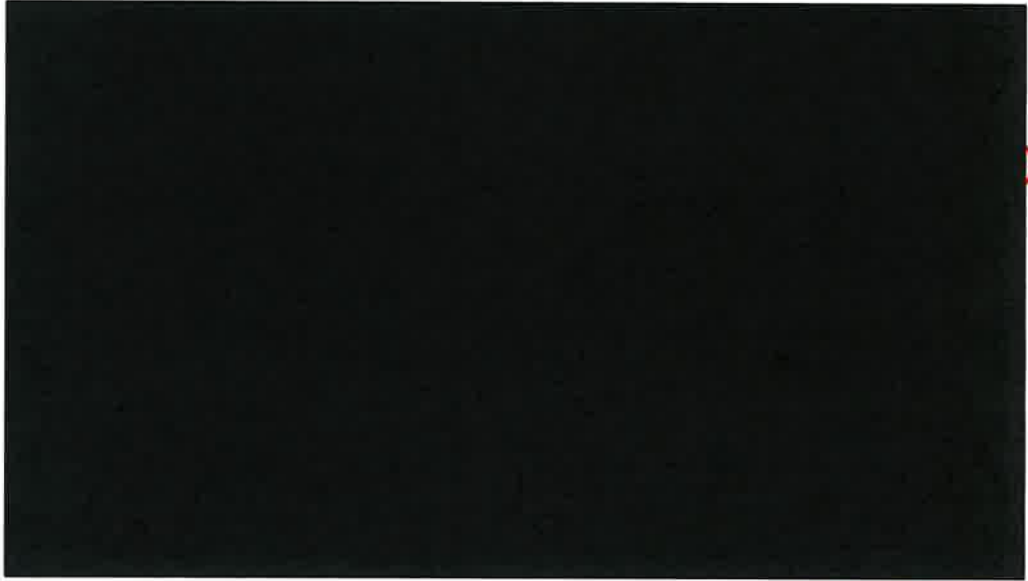
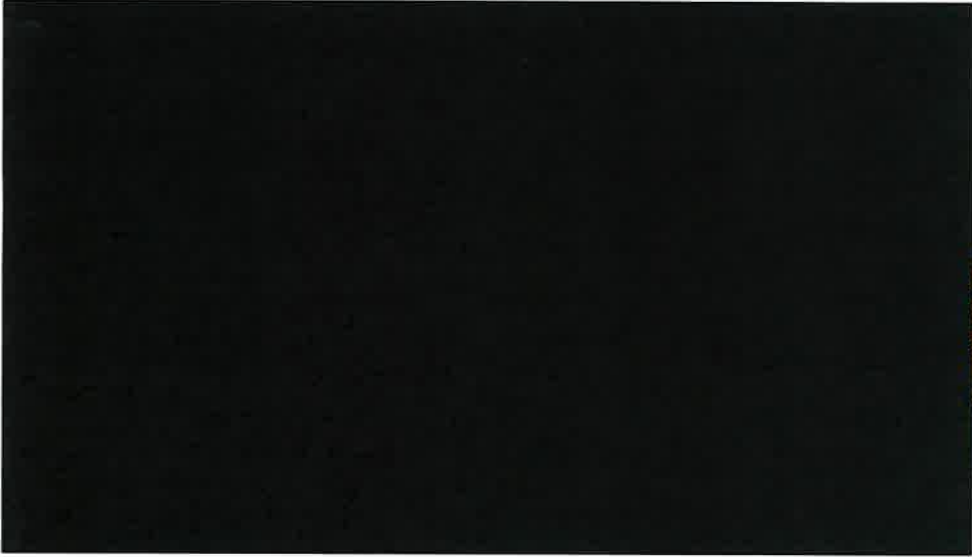
Support to international financial and money laundering investigations

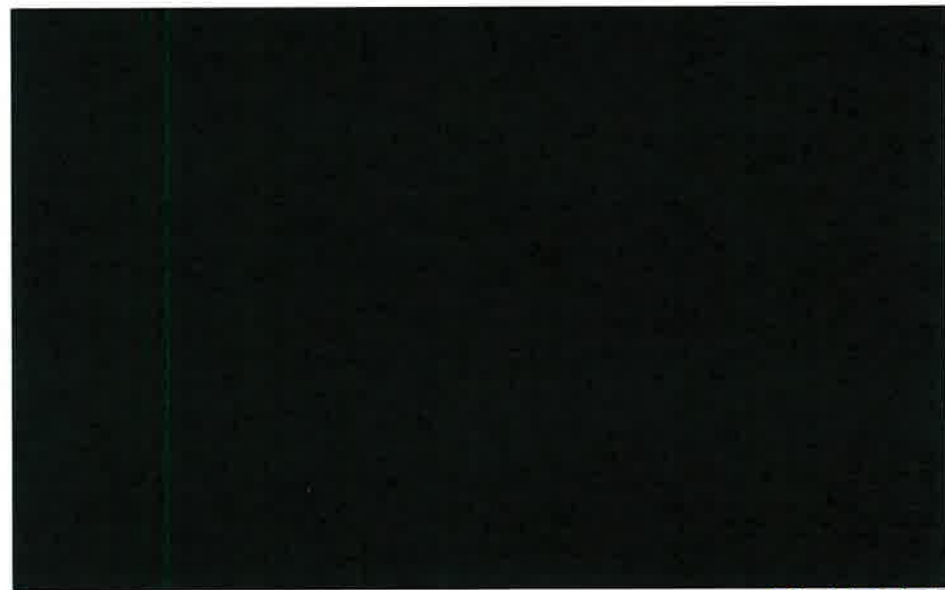
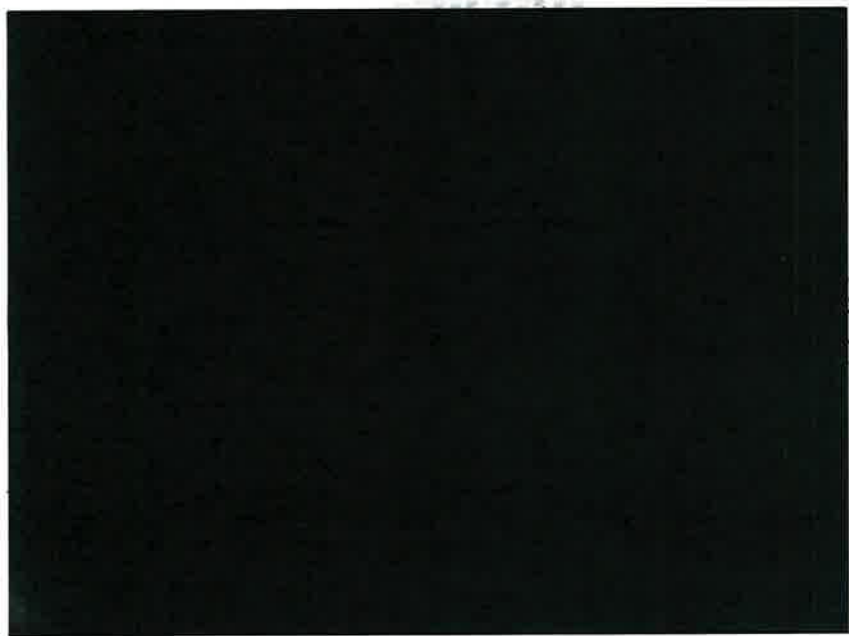


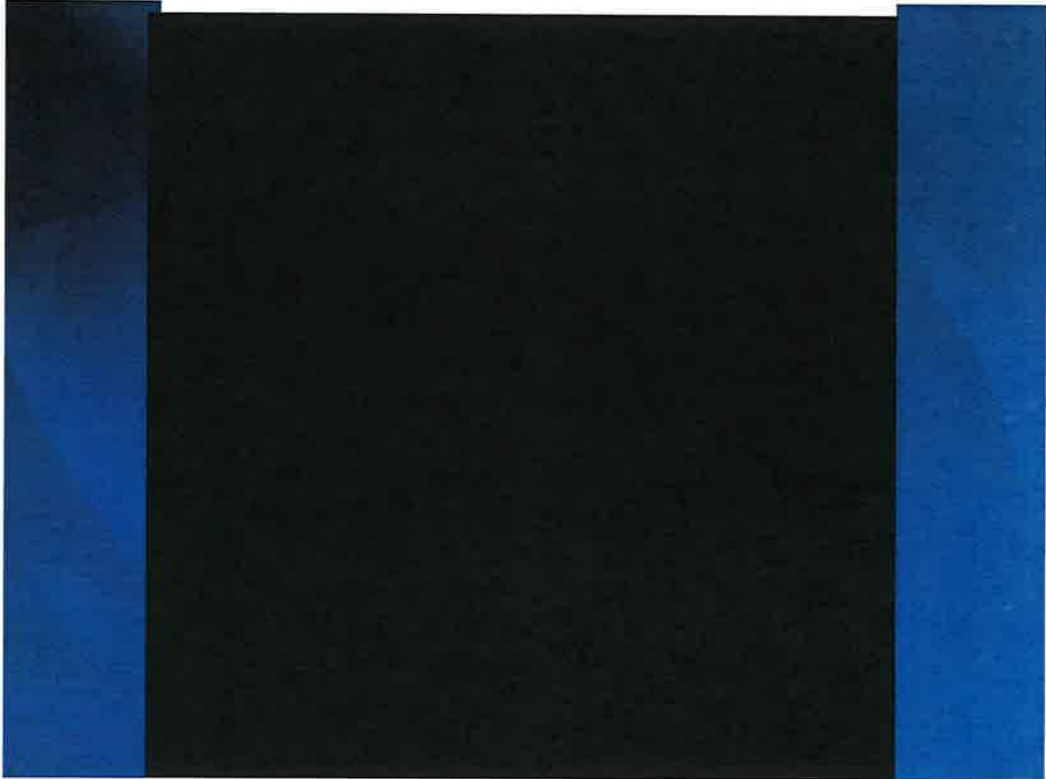


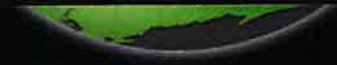
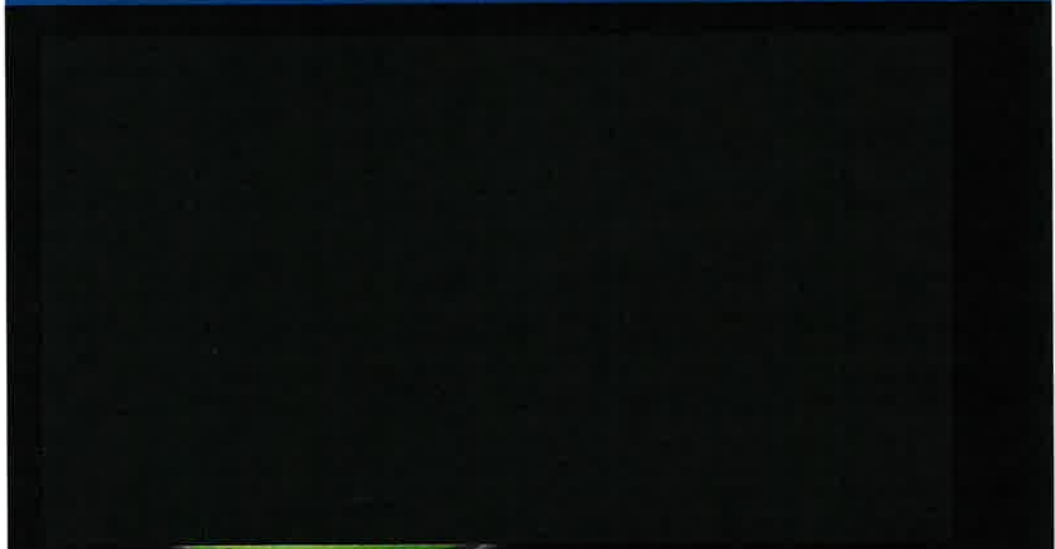


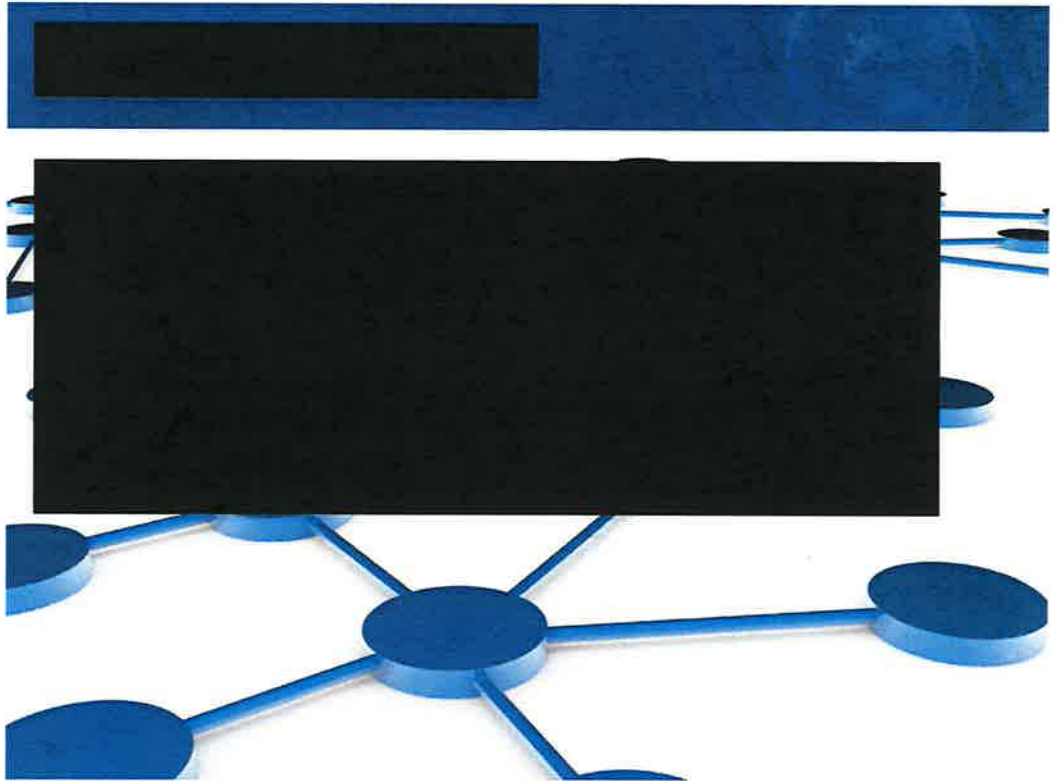
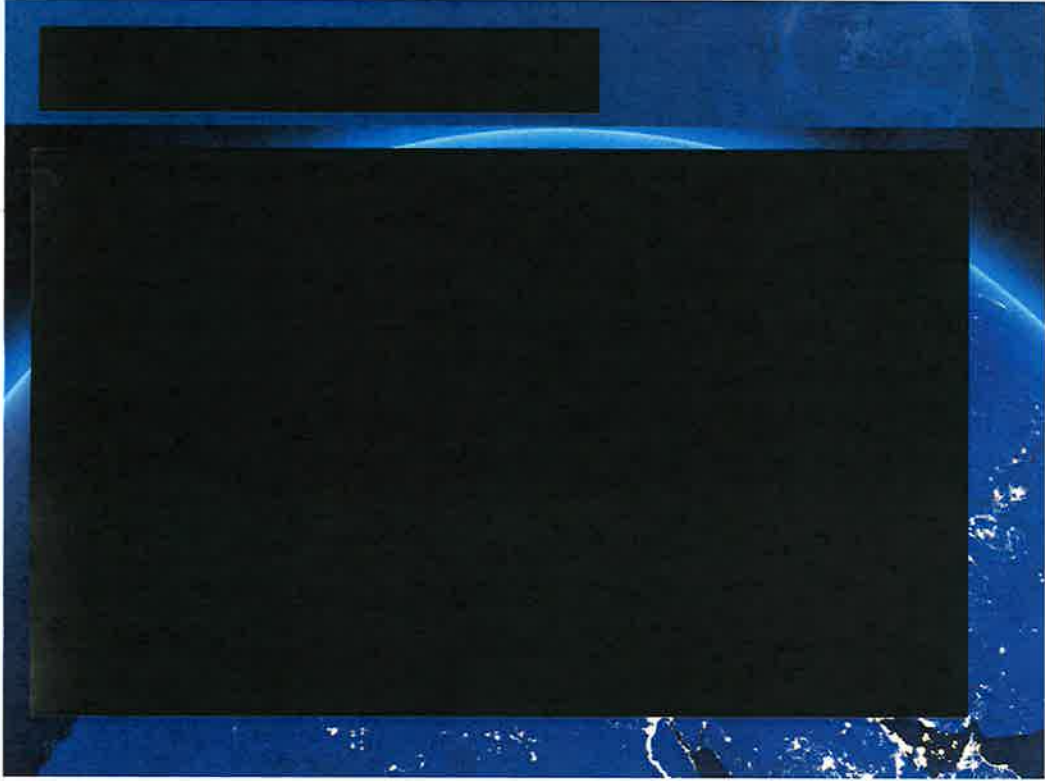


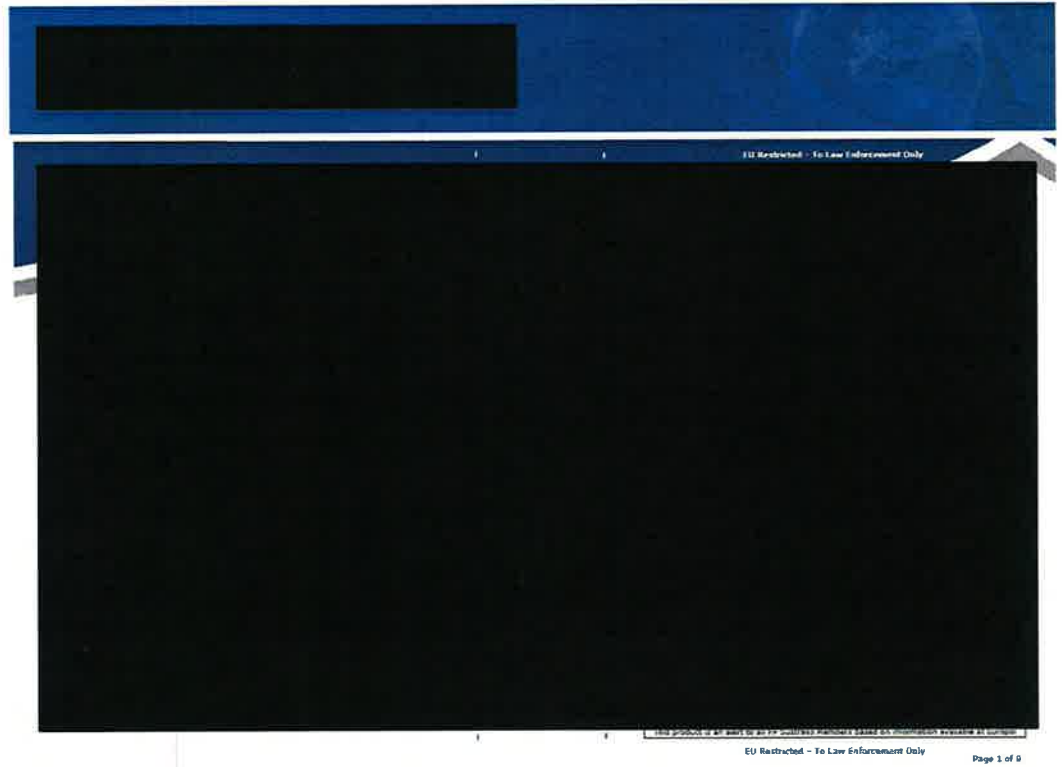
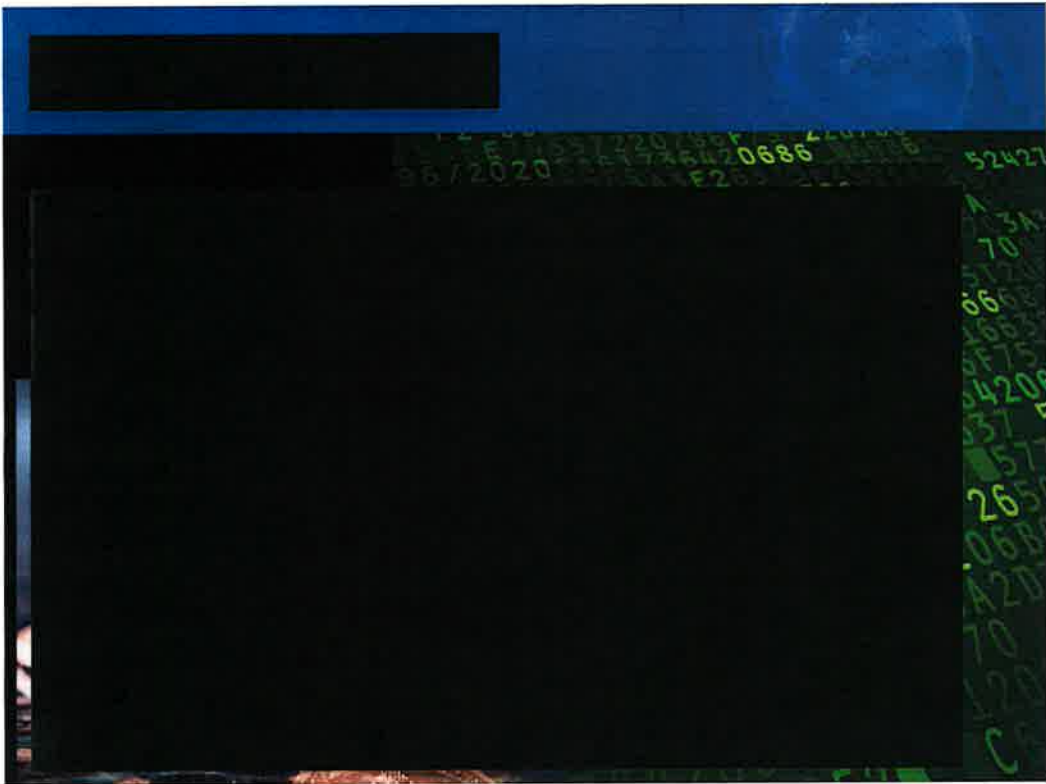


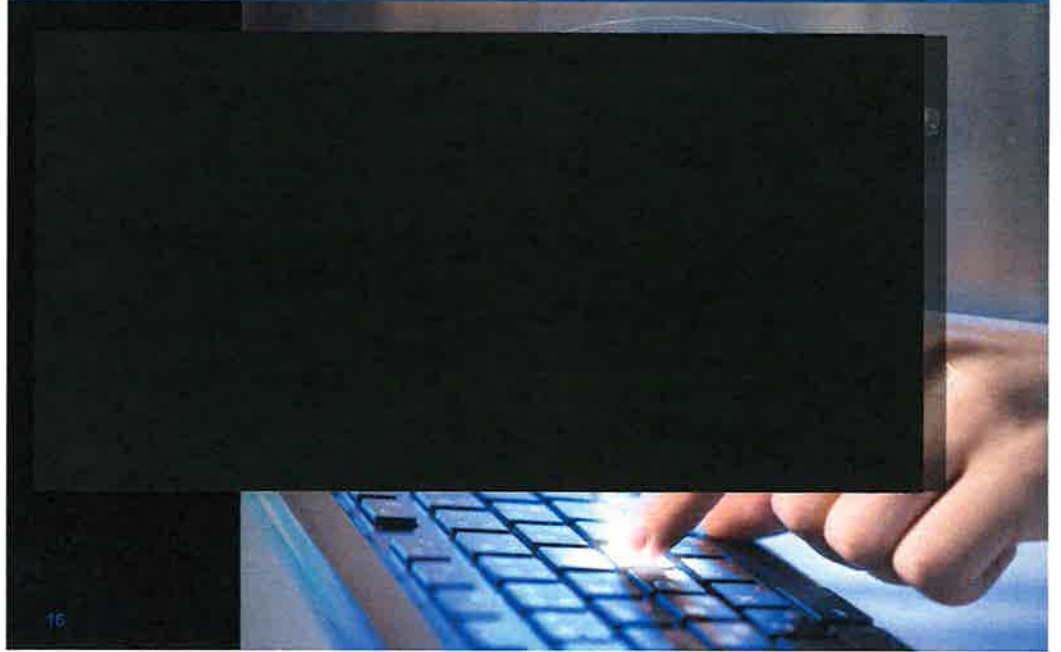
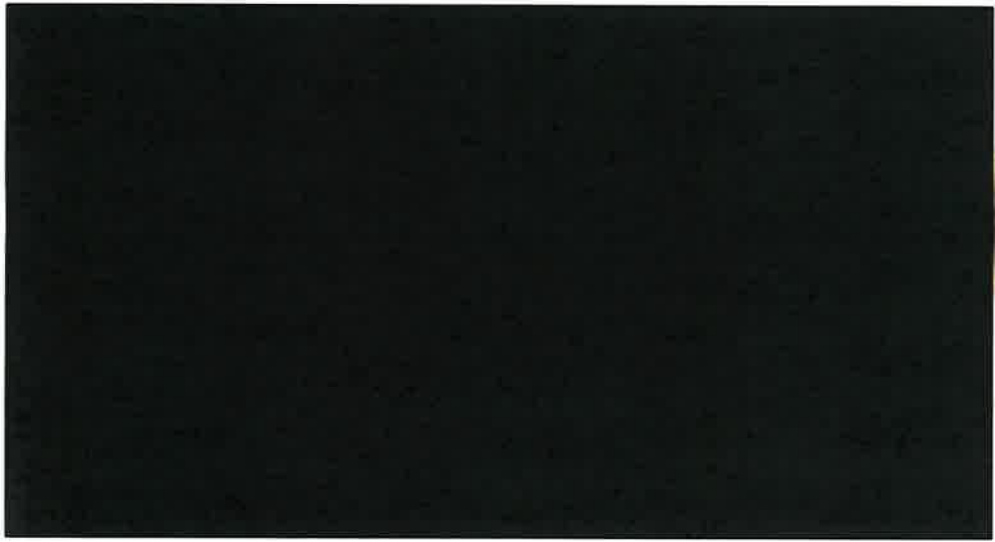


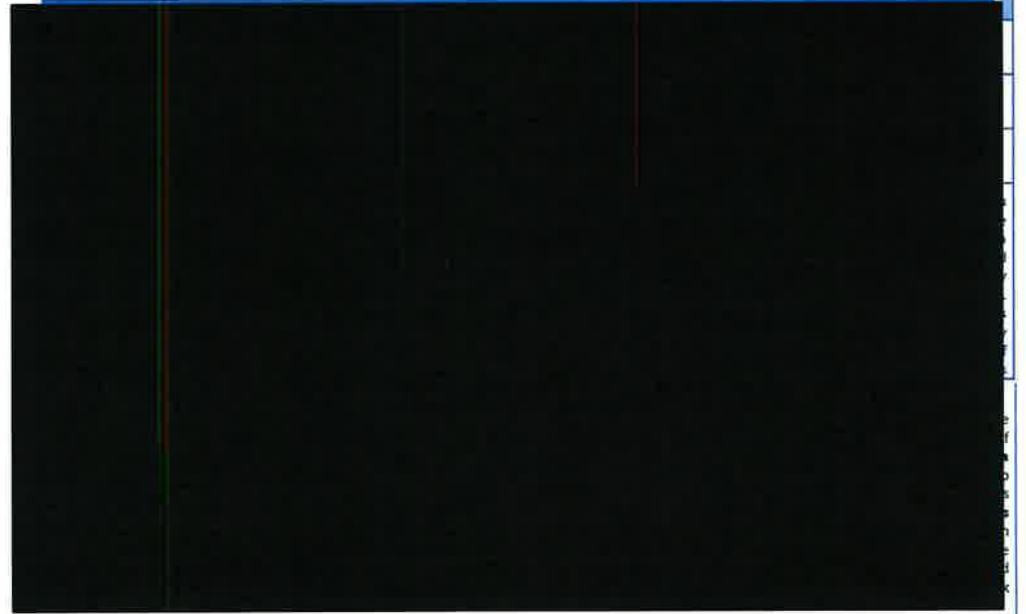
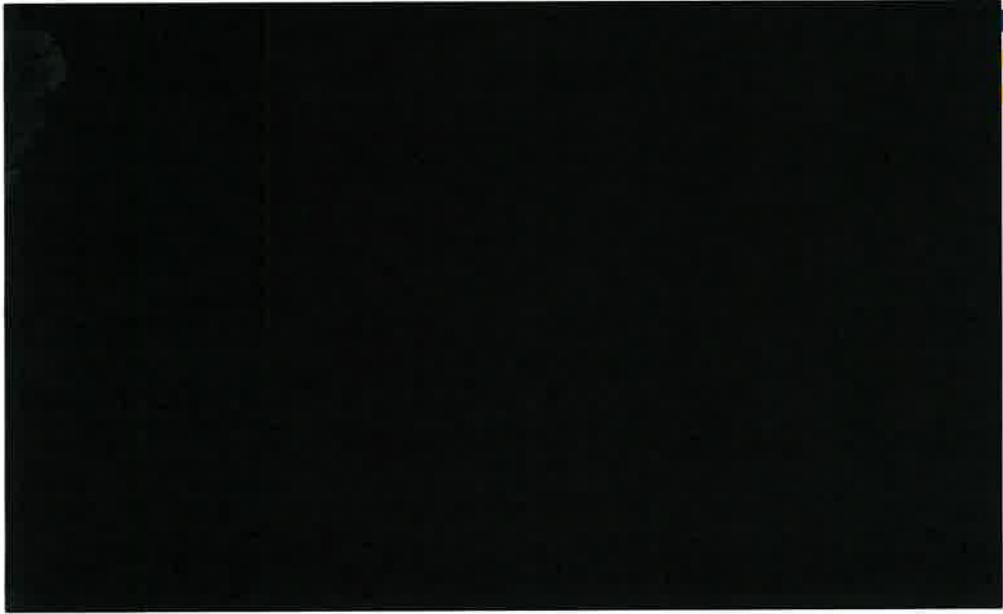










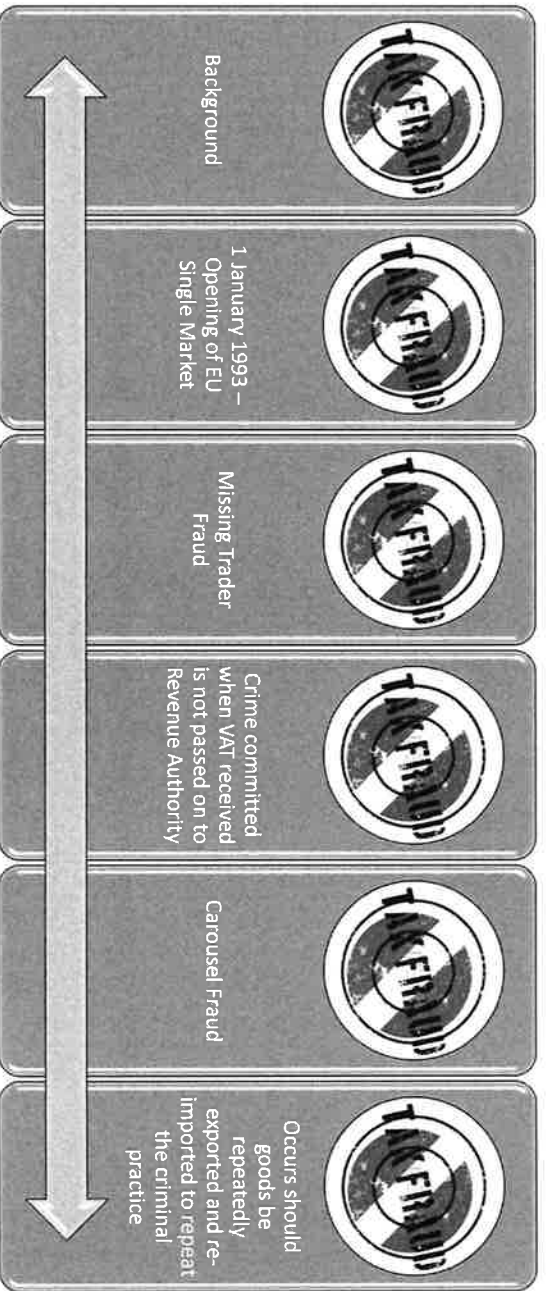


Economic Crimes

**CEPOL Western Balkan Financial Investigation In-Service
Training**

**'Financial Investigations in relation to Drug Trafficking'
08-12 October 2018 in Prishtina, KOSOVO**

Missing Trader Intra-Community Fraud

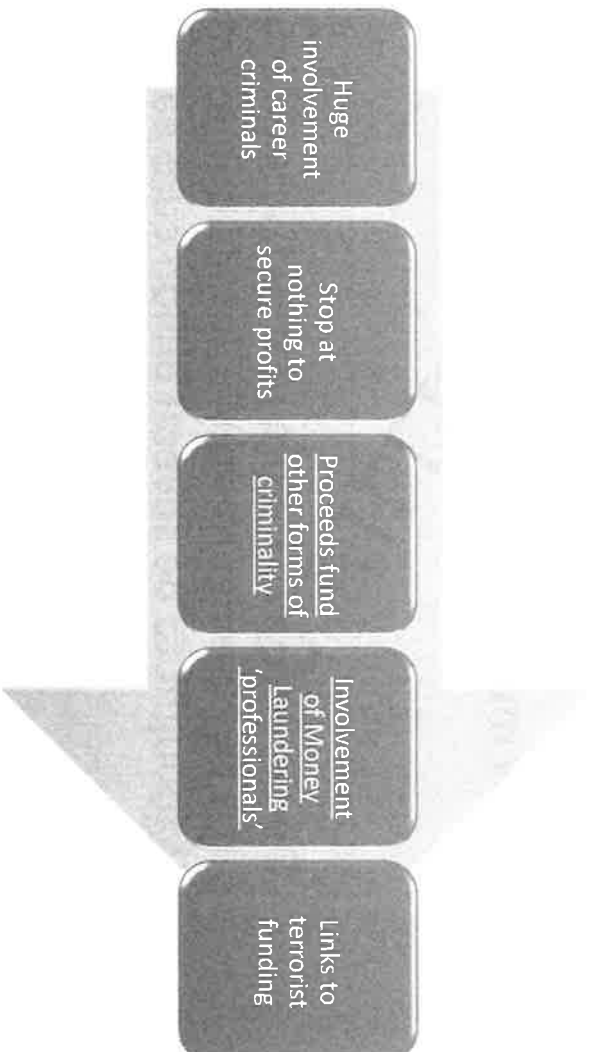


Scale of Problem

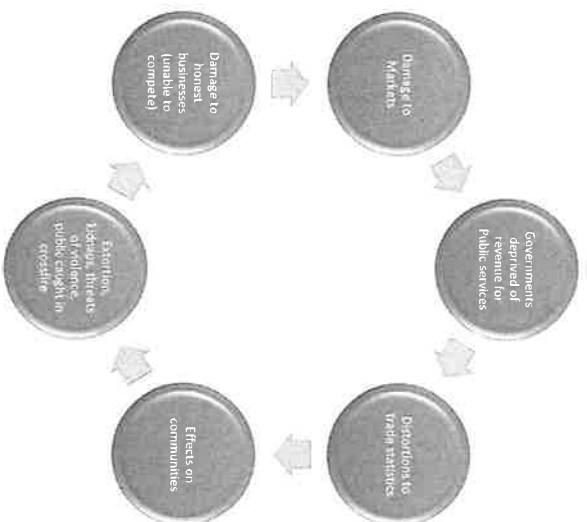
How much is lost every year because of VAT fraud?

Due to the very nature of fraud, it is difficult to put a precise figure on VAT losses due to fraud, it is thought to be **several billion** euro each year.

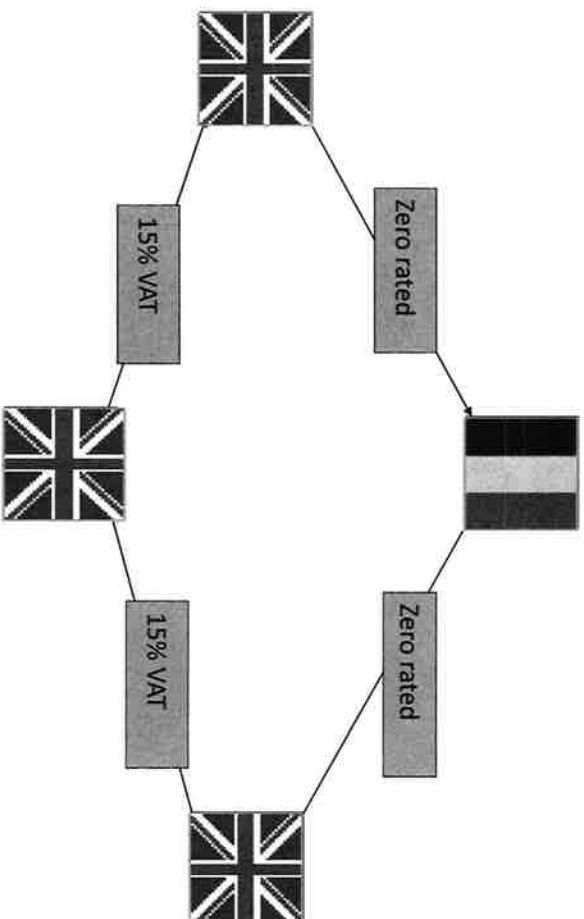
MTIC – “White collar” crime??



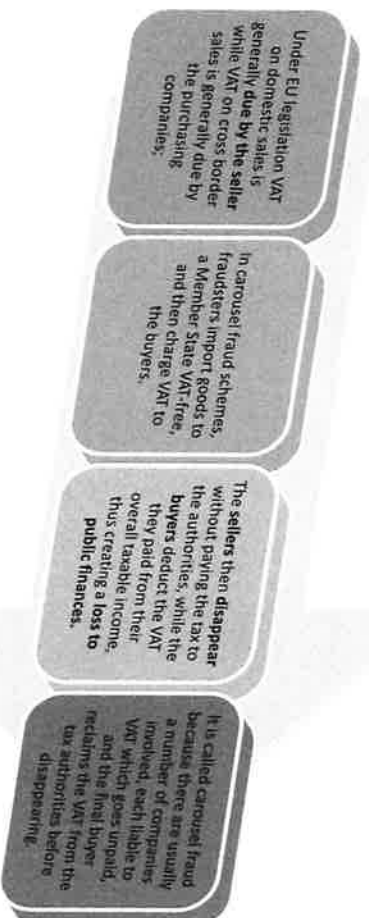
Victims



Basic MTIC Fraud

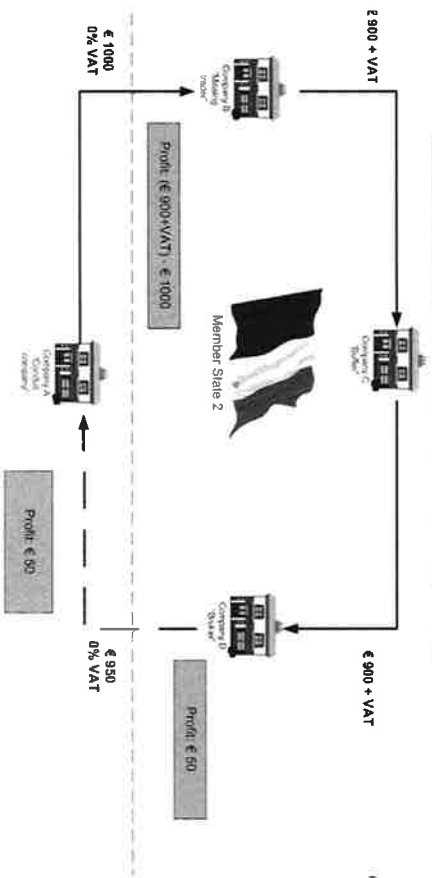


Basic MTTIC Fraud



Traditional fraud scheme

TRADITIONAL CAROUSEL FRAUD



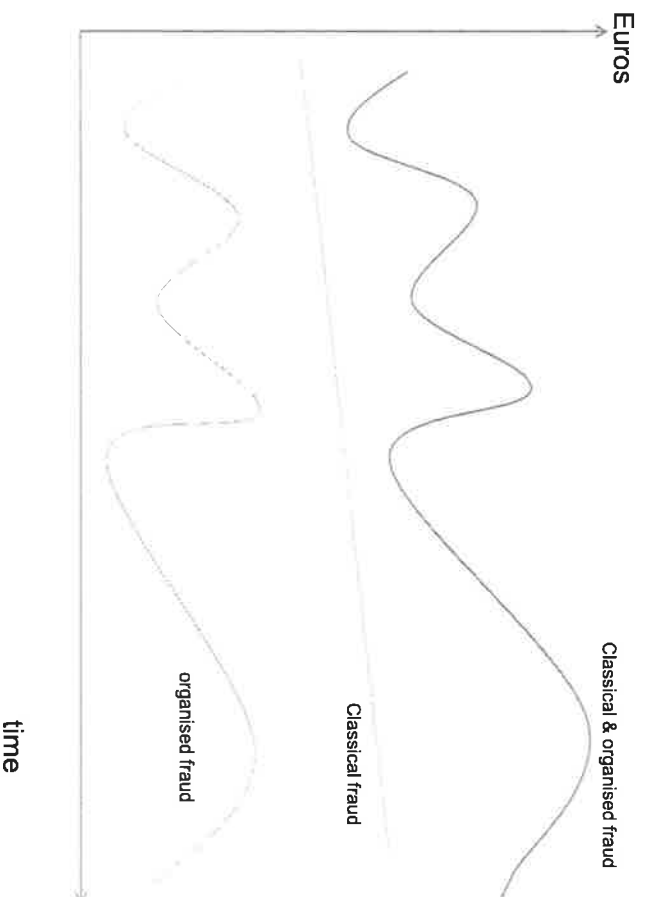
Disappearing into the ether?

Transformation VAT fraud:
from tangible to digital
commodities

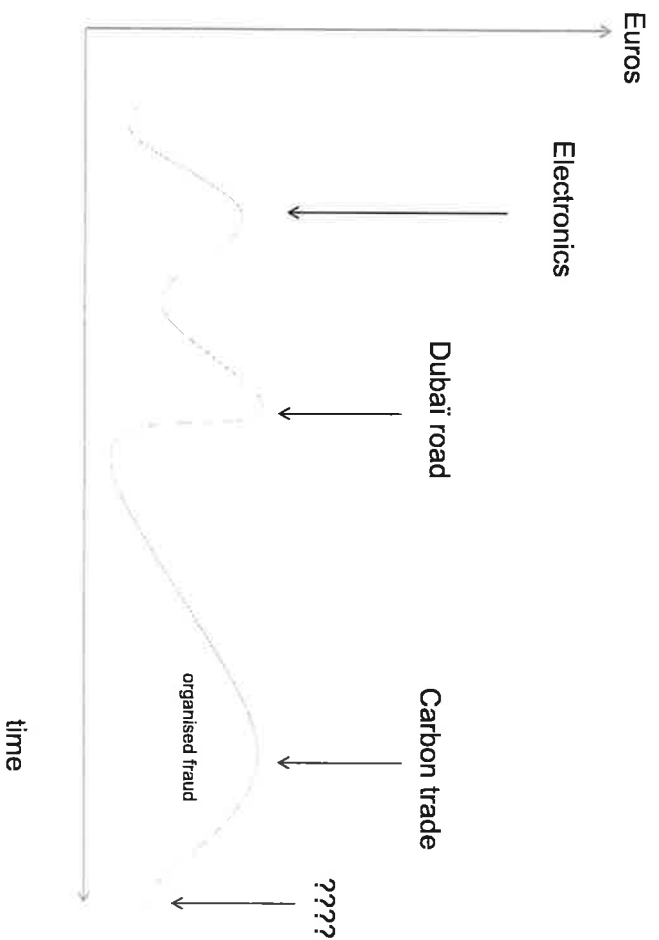
The involvement of virtual
financial institutions or
services in VAT-fraud
schemes



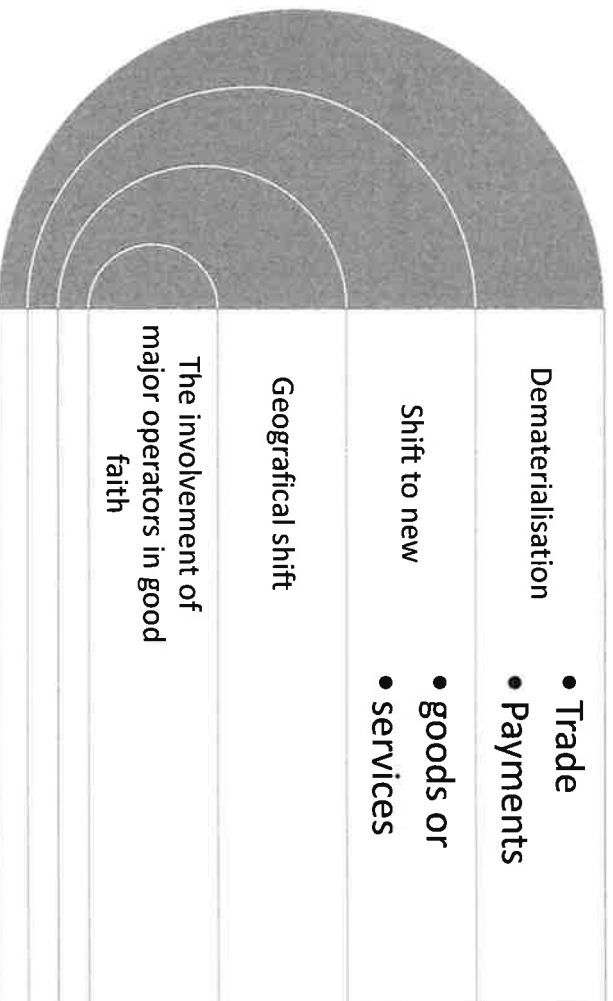
Volatility of organized fraud



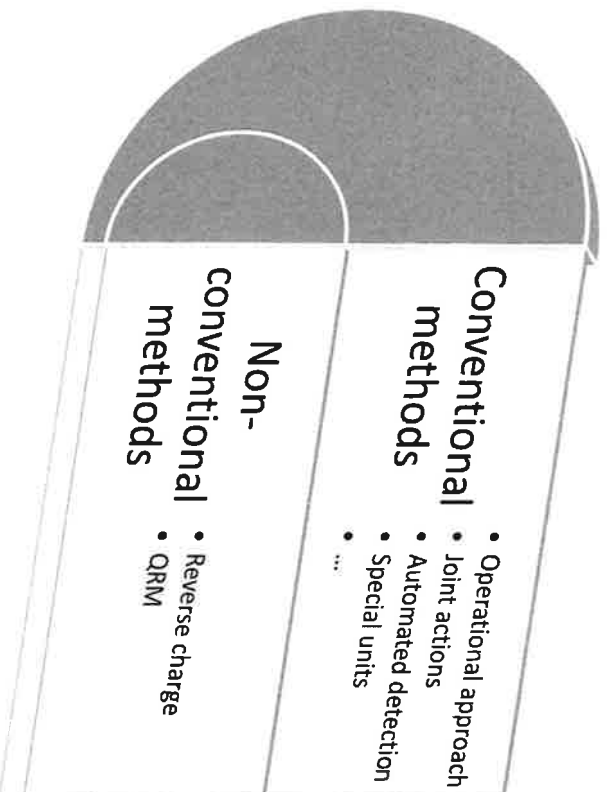
The causes of this volatility: violent attacks



New trends

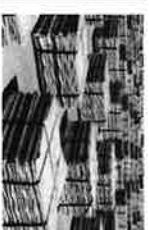
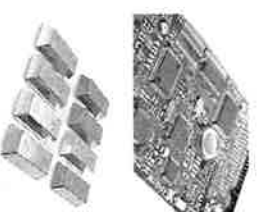


Reaction methods



MTIC VAT-fraud
Goods/services

- Gold/Silver/Platinum/Copper
- Mobile phones
- I phones
- I Pods'
- Computer components
- Computer games
- Game consoles
- Carbon credits
- Electricity
- Green certificates/EECS
- **What's next ?**



Background – VAT fraud energy market

In 2009 the tax authorities in the EU countries became aware that VAT fraud was being committed in relation to CO2 emission allowances.

The VAT fraudsters created chains with fraudulent companies from various countries registered with an account in different CO2 emission registries.

Rapid increase of the size of the emission market - Exchanges

Europol warned about an estimated 5 billion EUR in losses for European taxpayers, caused by VAT-fraud within the EU Emission Trading System (ETS)

EU Directive 2010/23/EU, introducing a domestic reverse charge mechanism on the trading of emissions, for a minimum of two years.

When the risk for VAT fraud in one market is eliminated, the fraudsters usually move on to other markets.

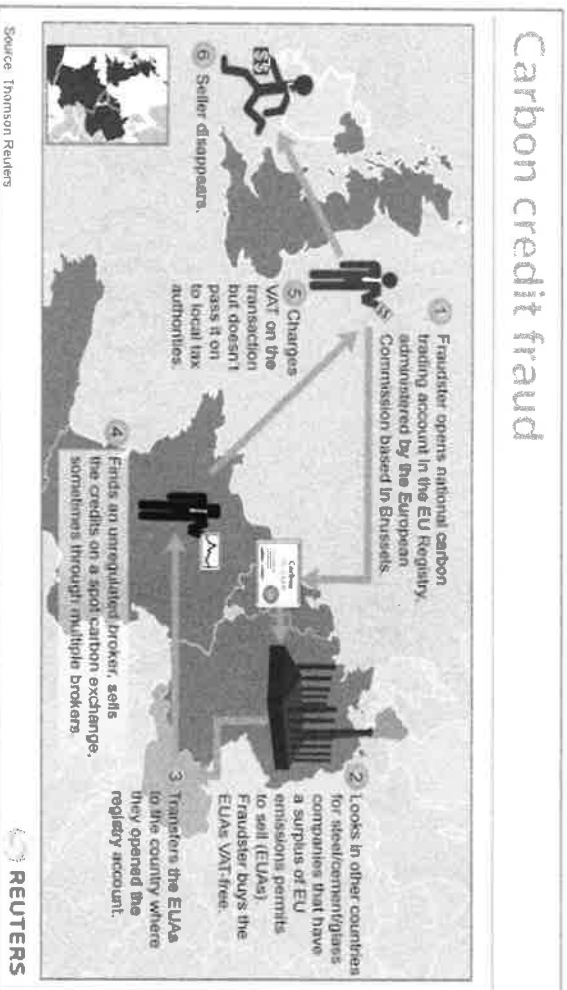
Carbon Credit Fraud

- Carbon credit fraud or VAT fraud in emission allowances trading



Recent development

Carbon credit fraud



Damage for European Taxpayer

Estimation by Europol:

€ 5.000.000.000

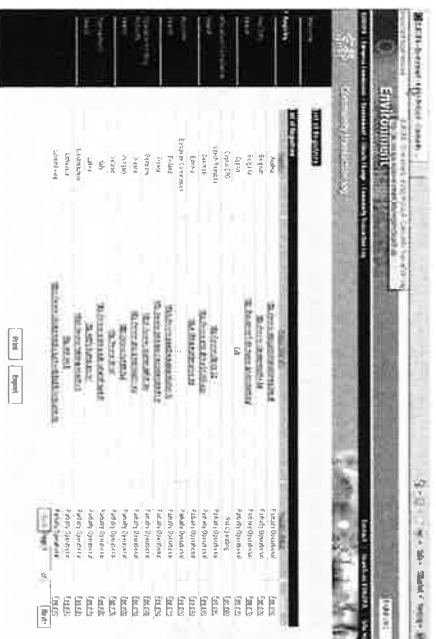
Hacked Registry Accounts

- **The case of the missing carbon credits**
- By Chris Lang, 25th January 2011
- The European Trading System suspended spot trading in carbon credits on 19 January 2011, after 475,000 EU carbon dioxide emissions allowances (EUAs) were stolen from the Czech Republic's carbon registry. The theft was discovered at 8:00 a.m. on 19 January 2011, by which time the thieves had already [sold the credits](#).
- The theft provides a glimpse into the mess that is carbon trading in Europe. Each country in the EU ETS has its own registry. The registries give a serial number to the carbon credits, allowing the buyer to know where the carbon credits come from and to make sure that that carbon credits have not already been sold to someone else (called double-counting). In Europe, there are [27 different registries](#), set up by 27 different development teams.
- The carbon credits were probably stolen on 18 January 2011, around 11:00 a.m., when a bomb scare was phoned in to the Czech Republic's carbon credit registry, OTE, and everyone left the building. By 12:00 am, the stolen carbon credits had been sold on to an account in the [Estonian registry](#).

Carbon credits - EU ETS scheme

- EU's Community Independent Transaction Log (CITL)

- Recapitulative statement
 - Emission registries
 - VIES
 - VAT declaration
 - Cross check
 - Information between MS
- Problem to access information from some national registries



DATE	ORIGINATOR	DESTINATION
2009-01-01
2009-01-02
2009-01-03
2009-01-04
2009-01-05
2009-01-06
2009-01-07
2009-01-08
2009-01-09
2009-01-10
2009-01-11
2009-01-12
2009-01-13
2009-01-14
2009-01-15
2009-01-16
2009-01-17
2009-01-18
2009-01-19
2009-01-20
2009-01-21
2009-01-22
2009-01-23
2009-01-24
2009-01-25
2009-01-26
2009-01-27
2009-01-28
2009-01-29
2009-01-30
2009-01-31

Electricity trading - VAT EU and none EU country

EU- Trade: The supply of electricity is subject to VAT where the customer is established, with a reverse charge, if the supplier is not established in the same country as the customer.

Import: Supply of electricity is subject to VAT where the customer is established. Electricity or gas can stay in the same hub/country and VAT fraud can be performed with a chain of companies of different fiscal residence in EU and third country.

Electricity can be traded cross-border within EU without being listed in an EU sales listing. (VIES)

Optimal for fraudsters – MTIC
VAT fraud

Developments in the use of
MTIC fraud-facilitating vehicles

**First Curacao International
Bank (FCIB)**

**UK HMRC Operation
Tangelo**

- STR 14 Feb 2007 re transfer from Banco Portuguese de Negocias to Laiki Bank in London via money service bureau;
- Production order to Laiki Bank – 40 account holders MTIC suspects, 100+ further STRs, 400 ex-FCIB account holders

UMBS

- Universal Mercantile Building Society EF (created 24/2/2006)
- Membership limited to 1,000 members
- Maximum deposit 50,000 krona (c 5,000€)

Misuse of SCU

- **UMBS EF** Internal transfers exceed £2 billion
- External payments amount to £42 million.
- Director linked to suspect MTIC companies in Portugal.
- Skatterverket audit identified Regulatory breaches
- UMBS EF blacklisted on Swedish FSA website
- Ceased trading 26 November 2006.

- **UMBS Online** inc 27 November 2006 under New Zealand law.
- Opened account with Technocash pty, NZ
- 846 of 848 'EF' members transferred to 'Online'
- 1570 members by 14 February 2007 (date of STR to HMRC)

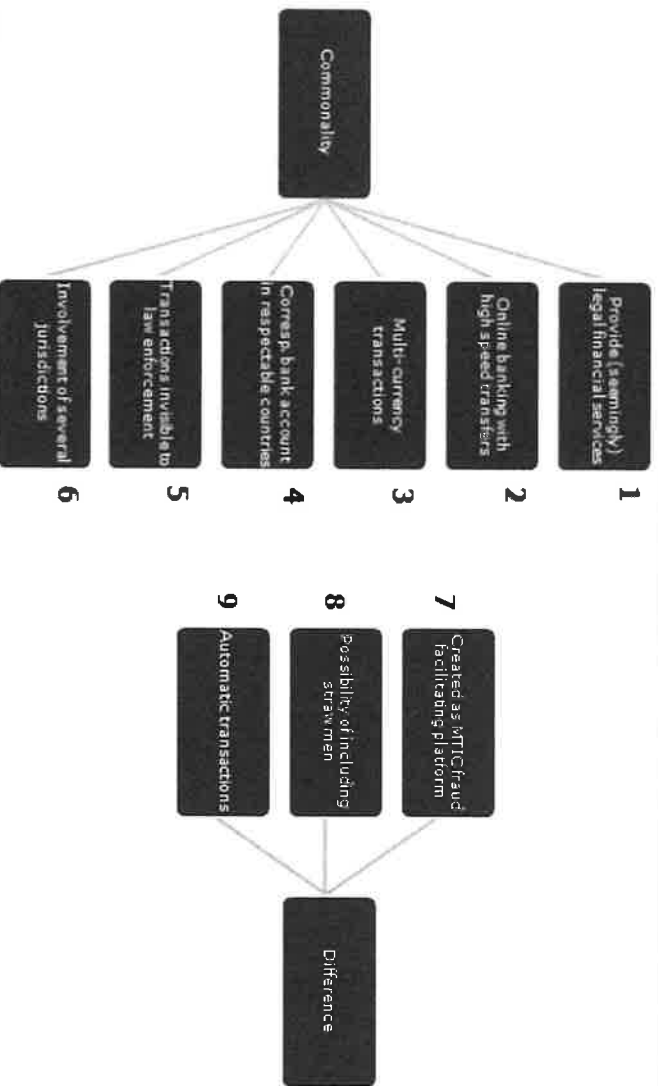
- Both UMBS EF and Online had their base of operations in Wembley, London
- Holding company based in Panama.

Why SCUS?

As SCU, UMBS had several features making it attractive to MTIC fraudsters

- Concept was Legal
- Exemption from license requirements and supervision by the Swedish Financial Supervisory Authority
- Offer services normally limited to fully licensed banks
- High-quality online banking software; high speed international transactions
- Obscuring transaction details
- Involvement of several jurisdictions

Other virtual financial institutions at risk I



Current developments

The cloud, its capacities, and potential consequences for stopping MITIC fraud

- Connected, information sharing servers worldwide
- Private, community, public, or hybrid forms of cloud
- Data scattering

Fraud facilitating platforms and services for sale

Difficulties faced in tracing and prosecution

- Involvement of multiple jurisdictions
- Restricted cooperation between competent authorities

Excise Oil Frauds

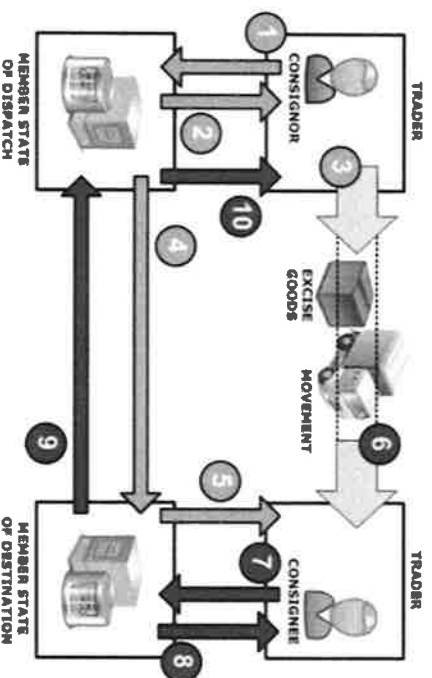
FRAUDS TYPOLOGIES

Oil products from Est Europe – VAT fraud

Fake declaration for zero-rated VAT

**Excise frauds – use of different products
(on paper lubricant oil used as gasoline)**

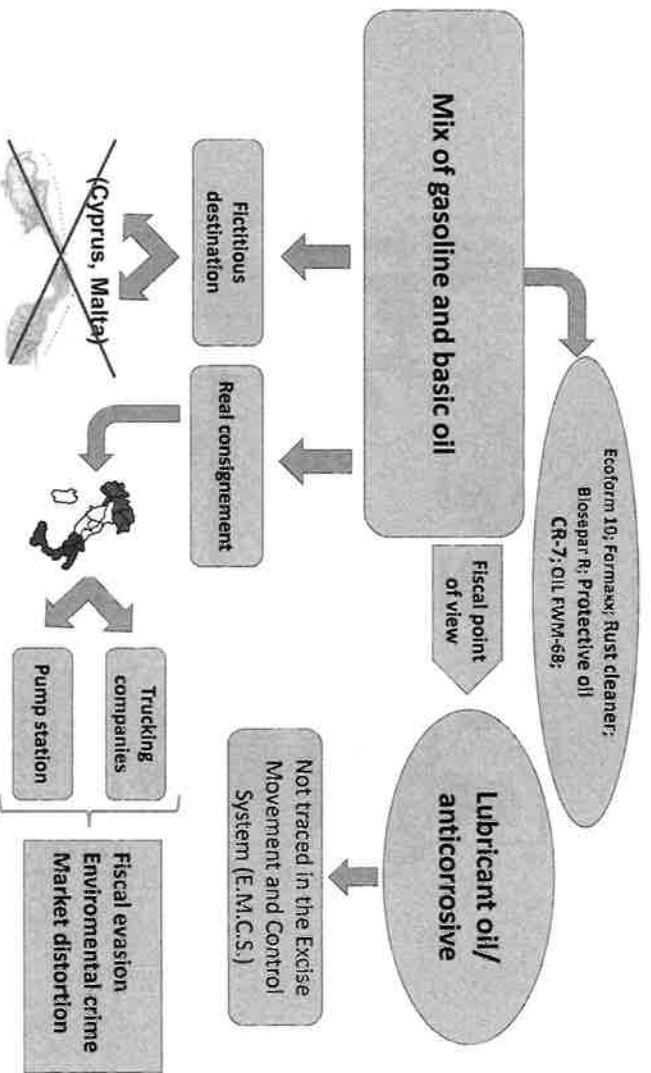
E.M.C.S.



1. The consignor submits the e-ADD
2. The Member State of dispatch validates the e-ADD and sends it back to the consignor (including the e-ADD Registration Code - ANCI)
3. The consignor dispatches the excise goods
4. The Member State of dispatch transmits the e-ADD to the Member State of destination
5. The Member State of destination forwards the e-ADD to the consignee

6. The excise goods arrive at destination
7. The consignee submits a report of receipt
8. The Member State of destination validates the report of receipt and sends it back to the consignee
9. The Member State of destination transmits the report of receipt to the Member State of dispatch
10. The Member State of dispatch forwards the report of receipt to the consignor

Eastern Europe incoming products



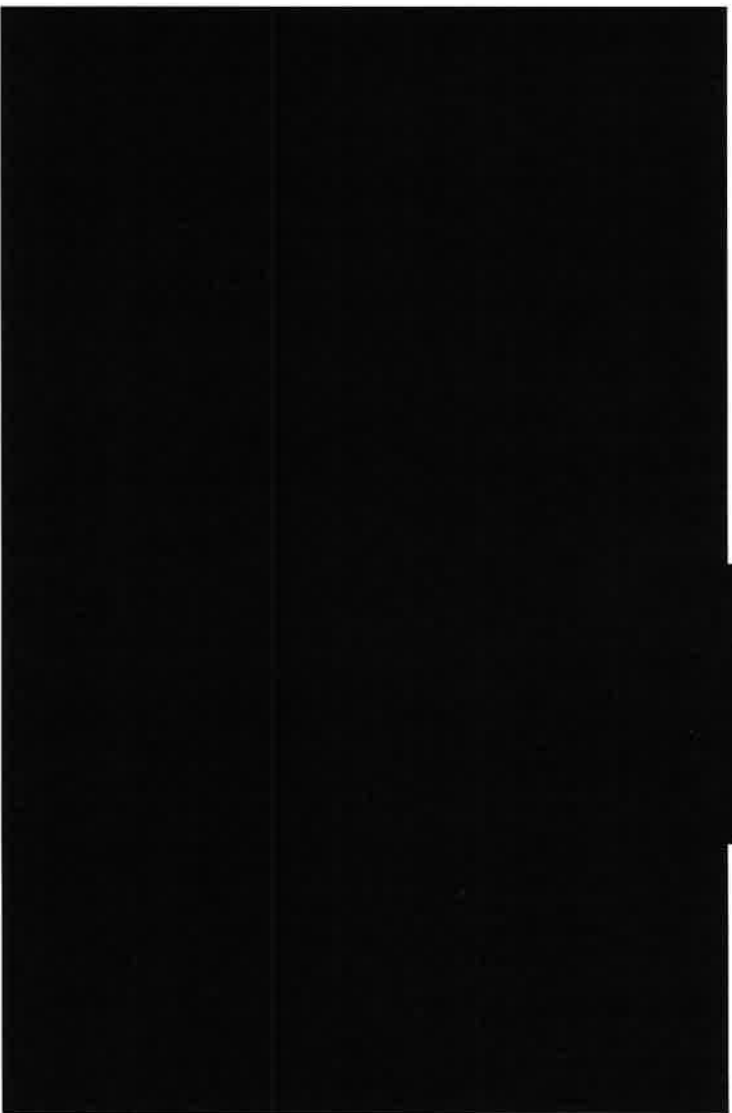
National consumption tax on lubricants

- In Italy, lubricating oils are subject to national consumption tax: 787,81 Euro/1.000 kg;
- Infringements in movements of lubricating oils are punished as well as those of excisable products.



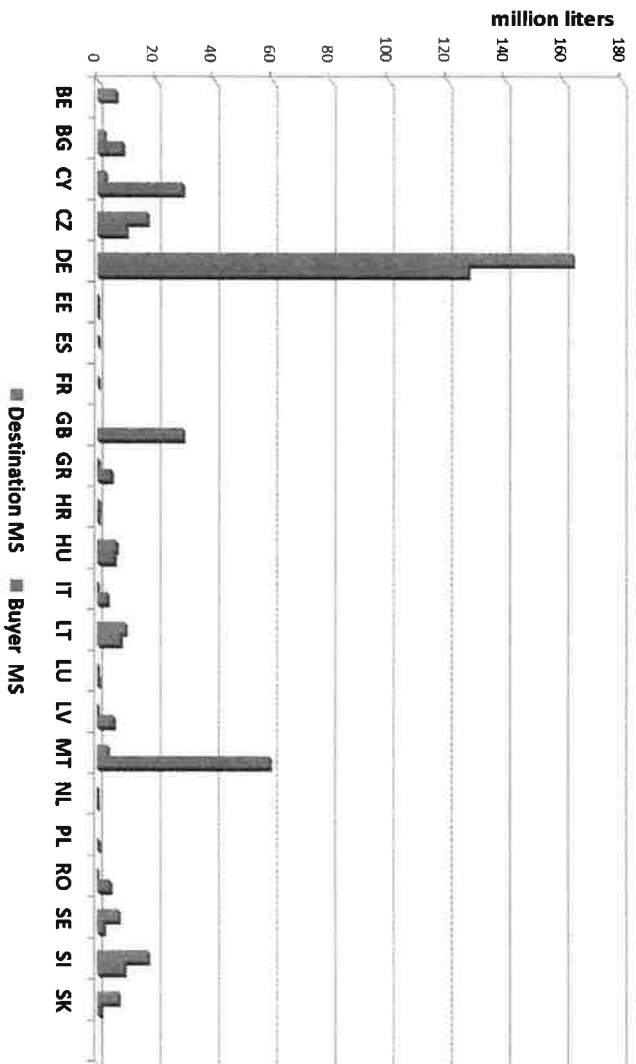
If the place of delivery is fictitious or the consignee is not authorized to receive this kind of products, goods are considered as illegally released for consumption and consequently seized.

Oil market Fraud: use of fictitious documents



Lubricant oil expeditions from Poland

Dispatch from PL
(Jan-Nov 2015)



Value of the illicit trade

«Black market»

The Hungarian National Tax and Customs Administration – NTCA, had estimated:

“According to data from Polish tax warehouses 503 million liters of base oil entered into free circulation between June 2011 and July 2013 in the EU Member States without the payment of taxes, the excise tax content of which is almost 270 million EUR, the VAT content of which is almost 122 million EUR which amounts to a damage of almost 400 million EUR in Member State budgets. In 2014, 216.5 million liters were exited from warehouses.”

Evolution of the fraud market: new products

The different OCG's had started to produce and sell **new typologies of products**.

They use **solvent** or **diluent** (combined nomenclature code 38140090) in a mix with gasoline. During an inspection the **new product** is chemically solvent or diluent thus is not monitored in the EMCS and is not excise duty as well.

EXAMPLE

Commercial name: **ENOL 103, THINNER S**

Invented: in Hungary, actually produced in UA, Serbia, ecc.

Composition: gasoline 92 %-biodiesel 6%-dichloromethane 2%

The dichloromethane is highly volatile.



over the last 5 months...

- **SEIZED PRODUCTS:**
Energy products (kg.) 1.818.000
- **SEIZED VEHICLES:** 146
- **INDIVIDUALS REPORTED TO THE
JUDICIAL AUTHORITY:** 751
- **ARRESTED INDIVIDUALS:** 34



