

Expose & Enrich Intelligence Related to
Front Companies and their Influence
Operators



FALKOR

&

DARKYOWL

Introduction

Front companies are often used to disguise illicit activities, making them a critical focus for investigative analysts. By leveraging OSINT (Open-Source Intelligence) and dark web data, investigators can uncover hidden networks, track suspicious activities, and identify key players involved in illicit operations. This guide provides a step-by-step approach to investigating front companies using advanced intelligence tools like Falkor and DarkOwl.

Understanding Front Companies

A front company appears to be a legitimate business but operates with the intent of hiding illicit activities.

These entities are commonly used for:

- Sanctions evasion
- Money laundering
- Cybercrime and fraud
- Geopolitical influence operations

Identifying these organizations requires access to advanced investigative tools and methodologies.

OSINT & Dark Web Intelligence: The Power of Falkor & DarkOwl

Falkor provides an analyst-driven platform for data fusion, case management, and AI-assisted intelligence gathering. It integrates OSINT sources, including deep and dark web data, to enhance digital investigations.

DarkOwl specializes in collecting and structuring data from the dark web, uncovering illicit communications, leaked credentials, and compromised assets.

Combined, these platforms offer investigators a full-spectrum approach to analyzing front companies.



Case Study: Exposing a Russian Front Company

A recent investigation using Falkor and DarkOwl focused on the Center for Geopolitical Expertise (CGE), a Moscow-based entity linked to influence operations.

- Sanctioned by the US Treasury, CGE was found to have ties to Russian intelligence.
- Investigators traced leaked credentials and emails to employees linked to multiple front companies.
- Telegram and deep web analysis uncovered connections to global influence operations, targeting elections in Germany and the US.

This investigation demonstrated the importance of integrating dark web data with OSINT for high-confidence attribution.

GRU-AFFILIATED ENTITY USES ARTIFICIAL INTELLIGENCE TOOLS TO INTERFERE IN THE U.S. 2024 ELECTION

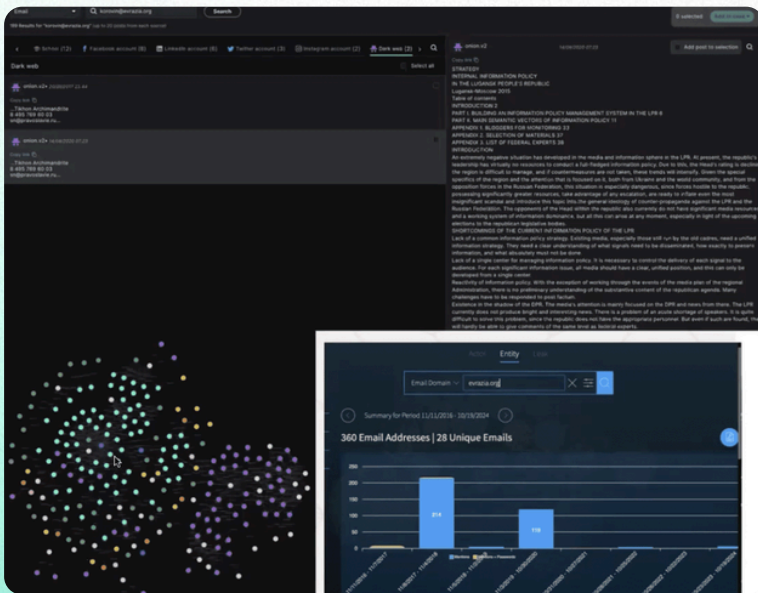
The Moscow-based **Center for Geopolitical Expertise** (CGE), founded by OFAC-designated Aleksandr Dugin, directs and subsidizes the creation and publication of deepfakes and circulated disinformation about candidates in the U.S. 2024 general election. CGE personnel work directly with a GRU unit that oversees sabotage, political interference operations, and cyberwarfare targeting the West. Since at least 2024, a GRU officer and CGE affiliate directed CGE Director **Valery Mikhaylovich Korovin** (Korovin) and other CGE personnel to carry out various influence operations targeting the U.S. 2024 presidential election.



Key Investigative Techniques

1. Mapping Digital Infrastructure

- Utilize DarkOwl to uncover dark web references, including email leaks and domain mentions.
- Use Falkor's link analysis to visualize connections between front companies and associated individuals.



2. Leveraging Sanctions Data

- Identify sanctioned entities using public sanctions lists and enrich findings with dark web data.
- Trace transactions linked to these entities through leaked data sets.

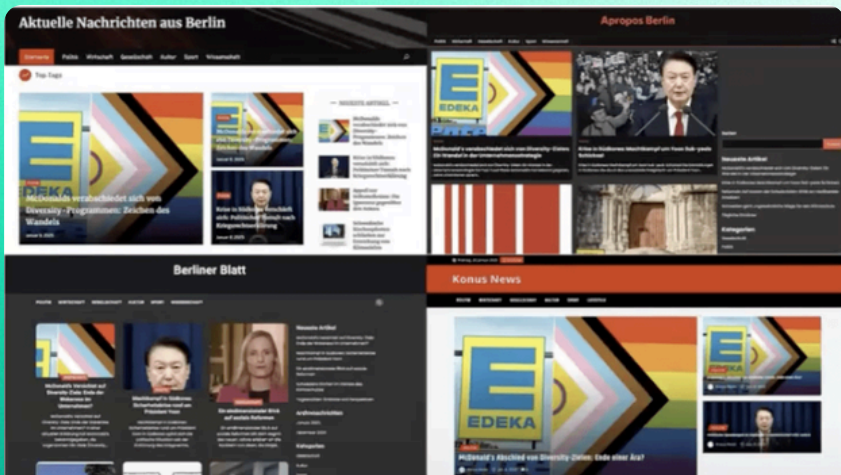


The following individuals have been added to OFAC's SDN List:

KOROVIN, Valery Mikhaylovich (Cyrillic: КОРОВИН, Валерий Михайлович) (a.k.a. KOROVIN, Valerii Mikhailovich), Moscow, Russia; DOB 31 May 1977; POB Vladivostok, Russia; nationality Russia; citizen Russia; Gender Male; Secondary sanctions risk: See Section 11 of Executive Order 14024.; Tax ID No. 504700223250 (Russia); Russian State Individual Business Registration Number Pattern (OGRNIP) 305504719503200 (Russia) (individual) [ELECTION-EO13848] [RUSSIA-EO14024] (Linked To: INTERNATIONAL NON-PROFIT FOUNDATION CENTER FOR GEOPOLITICAL EXPERTISE).

3. Tracking Personnel & Influence Networks

- Identify personnel affiliations by analyzing leaked email accounts, Telegram chats, and social media profiles.
- Cross-reference individuals with known geopolitical influence operators.



Fake local and national news sites An-berlin.de (top left), Apropos-berlin.de (top right), B-blatt.de (bottom left), and Konusnews.de (bottom right) are nearly identical in layout and content. (Screenshots via NewsGuard)

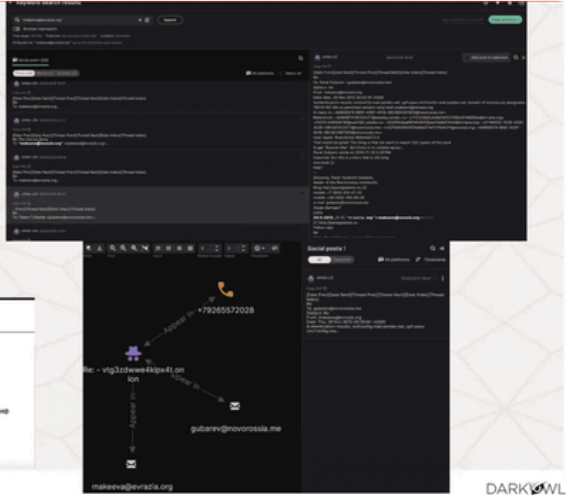
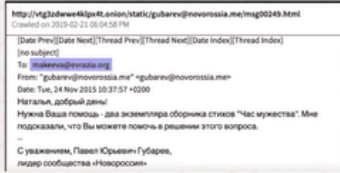


Natalia DarkOwl Email Results

Leaked Emails from conversations with pro-Russia Novorossiya movement in Donbass

Providing material, guidance and other contacts

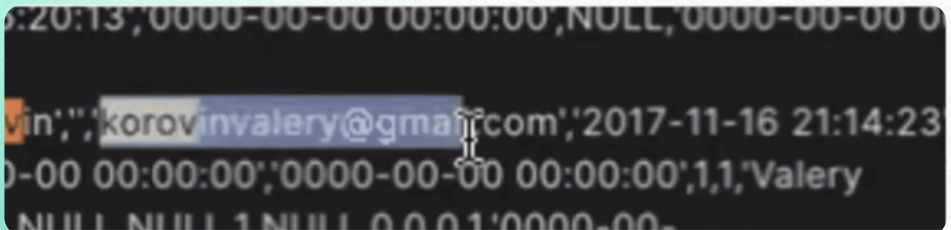
Falkor Extraction of DarkOwl Tokenized Entities



DARKOWL

4. Uncovering Digital Footprints

- Investigate domain registrations and IP allocations to find common addresses among multiple front companies.
- Search for reused infrastructure, a common tactic used by illicit organizations to set up multiple entities

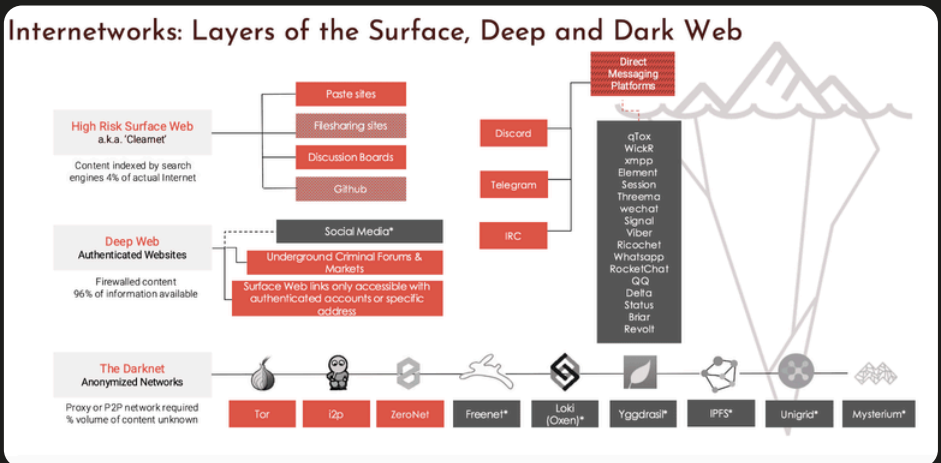


The Role of the Dark Web in Front Company Investigations

Threat actors use the dark web to:

- Discuss operational security techniques
- Trade illicit financial services and stolen credentials
- Obscure corporate ownership through underground markets

By monitoring dark web activity, investigators gain early insights into emerging threats and identify new front company networks.



https://t.me/1001526461340/from/1717918051000/to/1717918197000
Crawled on 2024-06-09 03:29:57 AM

2024-06-09T07:27:31 PPBoysOct2020 wrote: https://t.me/edicionesfides/974
WEBPAGE: https://t.me/edicionesfides/974

Title: Amigos de Ediciones Fides

Description:   PROXIMAMENTE 

El final de Europa. Juntos con Rusia en el camino hacia la multipolaridad


  Valery Karavayev


 EDICIONES FIDES

 https://edicionesfides.es/

 https://www.facebook.com/ediciones.fides

 https://twitter.com/EdicionesFides

 https://t.me/edicionesfides

 fidesediciones@yahoo.com

TODA LA INFORMACIÓN

EN NUESTRA PÁGINA WEB

<https://edicionesfides.es/producto/el-final-de-europa-juntos-con-rusia-en-el-camino-hacia-la-multipolaridad/>

Deep Web (Telegram, Discord) data on entities promoting Korovin

Example – Ediciones Fides – Platform amplifying Duginism in Spanish to global audiences

Other examples abound – other deep web platforms are critical

Post details

https://t.me/MELANDRINAZA

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

7/10/2024 11:42

Ethical Considerations & Compliance

Investigating front companies requires strict adherence to:

- Legal frameworks (GDPR, DOJ guidelines, etc.)
- Ethical intelligence gathering practices
- Responsible use of sensitive information

Falkor and DarkOwl implement compliance controls, ensuring lawful and transparent investigations.



Conclusion: Strengthening Investigative Capabilities

- Dark web data can be useful for investigations of all kinds, such as profiling, finding leaked data, and more.
- Leaked data can expose ties to additional organizations, i.e., CGE to Evrazia, Evrazia to Novorossiya.
- Other data points such as shared physical addresses can link to other front organizations.
- Deep web data from Telegram, Discord, and other sources can be useful for international investigations and identifying other potentially affiliated organizations.

Combining OSINT with dark web intelligence significantly enhances an analyst's ability to track illicit networks. By leveraging Falkor and DarkOwl, organizations can:

- Identify and expose front companies faster
- Enrich investigations with verified intelligence
- Maintain compliance while accessing sensitive data



Next Steps: Take Your Investigations Further

Want to see how Falkor and DarkOwl can strengthen your investigations?

- [Request a Demo](#) for a hands-on look at the tools in action.
- [Watch the full webinar](#) — Get full access now
- [Stay Ahead](#)— Subscribe for intelligence updates on emerging threats.

