Between a Rock and a Hard Target: Investigating Activity in Russia and China

4 methods used by modern analysts

FALKOR

Table of Contents

Introduction

Russia and China have always been challenging to investigate, even in the best of times. Their distinct ecosystems—complete with unique search engines, social media platforms, and language barriers—often leave non-native analysts unsure where to begin.

Today, a host of new factors complicates the picture. In Russia, the government is actively restricting foreign visibility to protect its interests, independent journalism is under attack, and many foreign organizations and professionals have left the country. Similarly, in China, corporate registries have been sealed off, key domains are geoblocked, and the government has cracked down on Western due diligence firms.

At the same time, understanding these countries has never been more crucial. Russia's invasion of Ukraine has increased the need to assess geopolitical risks, screen for connections to the Russian government, and mitigate cyber threats. Meanwhile, China's growing influence—through espionage, trade wars, and its geopolitical stance—presents its own complex challenges, such as the looming threat of a Taiwan invasion or potential disruptions in global trade.

This contradiction leaves analysts at a crossroads. If investigating Russia and China was already daunting due to cultural and linguistic differences, how can one find actionable insights in today's restricted landscape?

This white paper explores these challenges and equips analysts across sectors—financial intelligence, cyber threat intelligence, law enforcement, and government—with actionable tools, methods, and creative strategies to access the information they need.

Part 1: Building on Familiar Tools

While it's true that investigating Russia and China is harder than before, traditional tools still play an essential role.

Platforms like Google, Bing, and other Western search engines remain valuable resources, especially for historical context and information related to expatriates or activities outside of Russia and China.

In Russia, Western platforms such as YouTube, Facebook, and Instagram are still widely used by a significant segment of the population, despite government bans.

For mainland China, this is less the case, but Hong Kong and Chinese communities abroad still engage with these platforms.

These tools provide a strong foundation—don't overlook them. Starting with what you already know and trust can help build confidence before branching into more specialized sources.

Oftentimes, you'll find what you need, at least at first, in the tools that you already use.

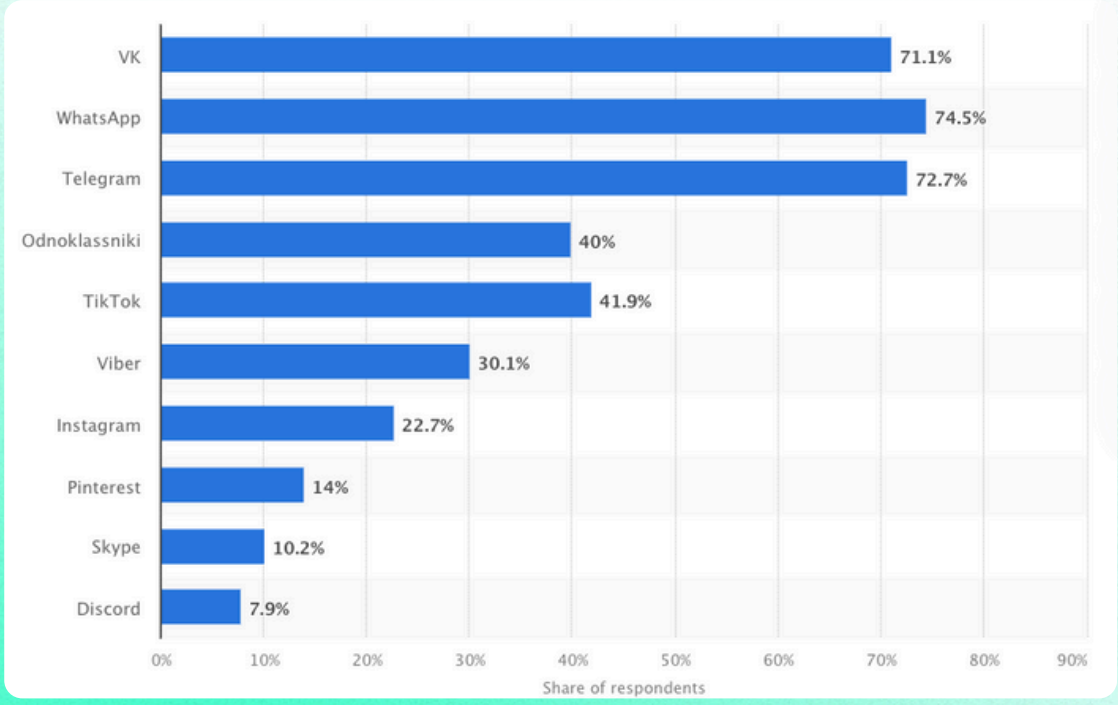
Part 2: Chinese and Russian Platforms and Search Engines

Russia and China have created unique and largely self-contained digital ecosystems that demand specialized approaches for investigations.

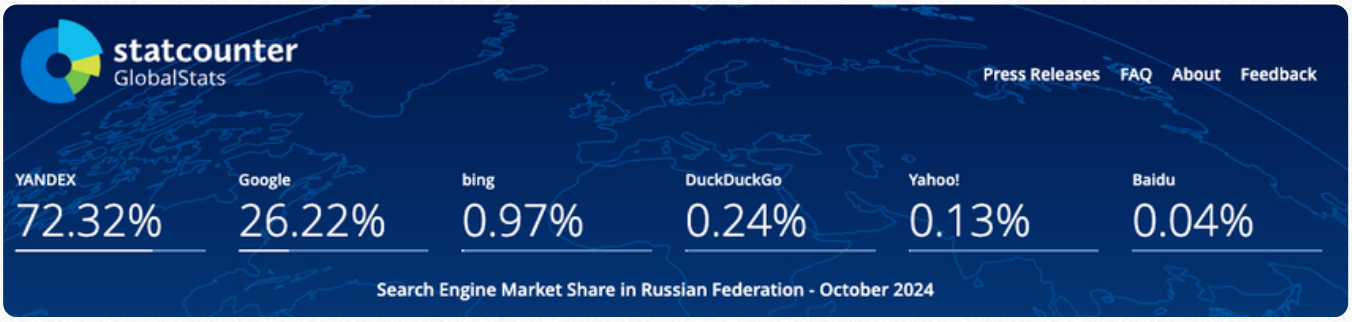
The Russian internet, commonly referred to as “RuNet”, offers a surprisingly rich landscape for its comparatively small audience. Take social media, for instance—platforms like Vkontakte (VK), akin to Facebook, dominate. Whatsapp leads as a messaging service, closely followed by Telegram, originally developed in Russia. Other platforms, such as Odnoklassniki, surpass their Western counterparts in popularity. Falkor supports searches for Telegram data via Telemetry, a Telegram data platform.

For search engines, Yandex reigns supreme in Russia, holding the lion's share of the market over Google. Email providers like Yandex Mail and Mail[.]ru are integral parts of RuNet, offering associated services like cloud storage (Yandex Disk) and chat platforms. LiveJournal, a classic blogging platform, remains popular and is a valuable resource for investigations.

Top active social media platforms in Russia
source:https://www.statista.com/statistics/867549/top-active-social-media-platforms-in-russia/



Search engine market share in Russia, source:
Source: https://gs.statcounter.com/search-engine-market-share/all/russian-federation



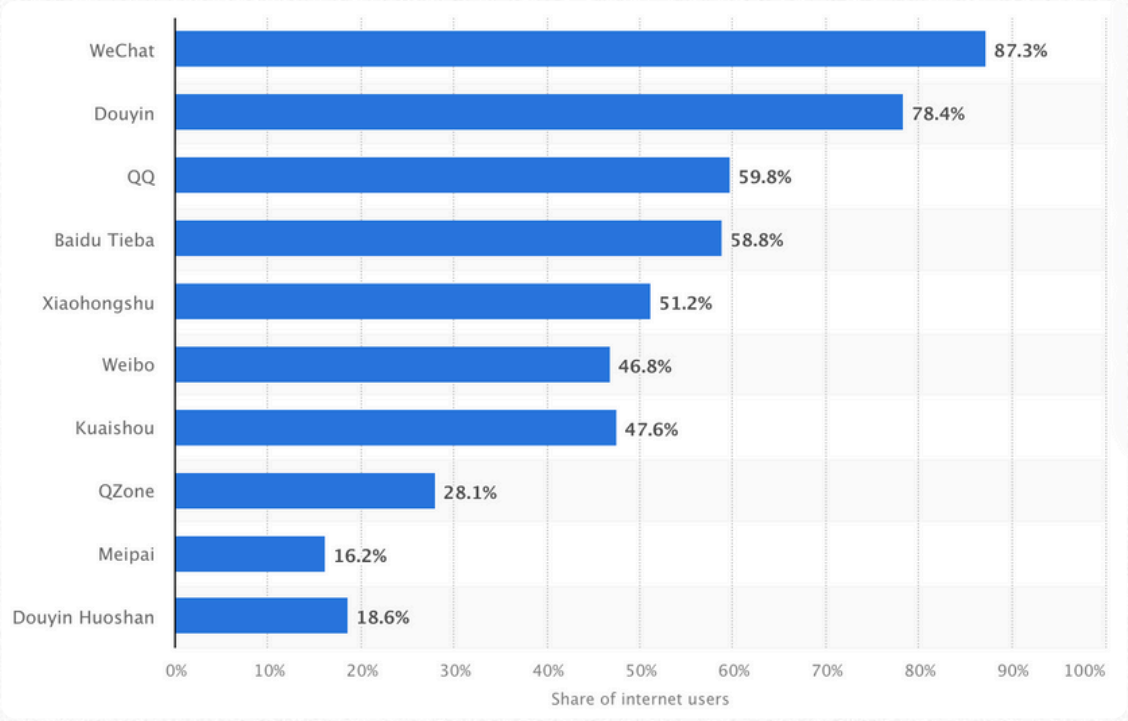
China presents an entirely different challenge. Its internet operates behind the "**Great Firewall**", heavily restricting access to external platforms while maintaining tight control over its domestic digital sphere.

The segmented internet environment has led to the creation of an ecosystem entirely its own, with platforms like **WeChat** (a multi-purpose app), **Weibo** (a microblogging platform akin to Twitter), and video-sharing platforms such as **Douyin** (Chinese TikTok) and **Kuaishou**. Many other Chinese platforms exist as well, such as iXigua, Xiaohongshu and more.

However, accessing Chinese platforms isn't always straightforward. For example, creating a WeChat account now requires both a valid phone number and approval from a verified user. Alternatives like Weibo and Douyin are less restrictive but may still require a workaround, such as using a Chinese, Hong Kong, or Taiwanese SIM.

For search engines, **Baidu** dominates in China, with others like **Sogou** playing a smaller role. While Google and Bing remain less utilized, they often provide surprisingly comprehensive results for Chinese searches, making them valuable additions to your investigative toolkit. Be sure to utilize their map tooling as well, as these often have street view or other geographic data that Google doesn't.

Top active social media platforms in China
Source:https://www.statista.com/statistics/250546/leading-social-network-sites-in-china/



Search engine market share in China
Source:https://www.peripherydigital.com/blog/baidu-chinas-largest-search-engine

Part 3: Corporate Data

Social media insights are just one piece of the puzzle. Investigating corporate and company data is equally critical for understanding Russia and China.

Historically, data from sources like **Hong Kong's corporate registry** was easily accessible and instrumental for financial investigations. However, access to the Hong Kong corporate registry, as well as mainland registries, has since been restricted by government measures to shield corporate data.

In Russia, corporate data can sometimes be accessed at the **oblast** (regional) level, while in China, the provincial-level registries may hold critical insights.

Both countries have introduced significant hurdles, including **geoblocking** and other restrictions. Tools like **VPNs** or **TOR** can sometimes bypass these barriers, but access is not guaranteed. Russian corporate registries are on the whole more accessible directly compared to their Chinese counterparts.

T**hird-party providers** like **AsiaVerify** offer a workaround, allowing investigators to access company data without direct access to local registries.

Additionally, government tender databases and job platforms, such as LinkedIn, provide alternative ways to gauge corporate activity, including hiring patterns and operational scale.

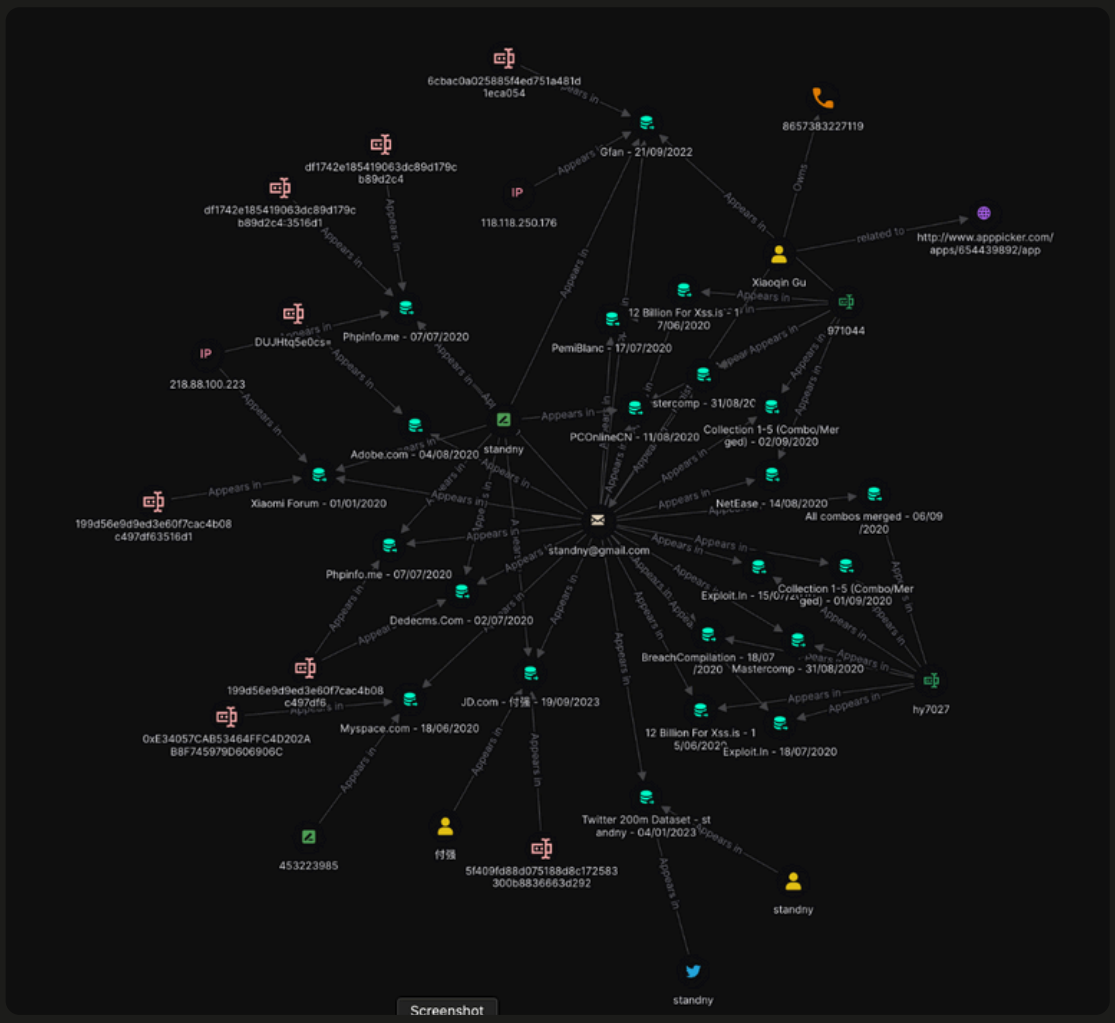
Import data is another underutilized resource. Platforms such as **ImportGenius** and **ImportYeti** can shed light on companies' trading partners, export volumes, and operational addresses, offering invaluable insights.

Part 4: Into the Breach

While formal data sources may be restricted, both Russia and China have active underground cybercrime communities, offering troves of leaked data on clearweb forums, Telegram, and darkweb sources.

Breached data can include everything from government documents to corporate records. This is especially critical when investigating Russia and China, as the highly developed cybercrime underground of data breaches means that almost any person, company or organization has at least one, if not multiple, data leaks available.

Tools like District 4 and Dehashed consolidate these leaks, providing searchable databases for investigators. Breached data can uncover usernames, passwords, IP addresses, and even linked social media accounts, offering a powerful lens into otherwise opaque entities.



Take, for example, the domain **mil[.]ru**, the Russian Ministry of Defense. Breached data associated with this domain can reveal significant insights, from email addresses to operational details, amplifying investigative efforts.

There are many, many more elements to investigating foreign activity, let alone Russia and China. Working multilingually with various file types and datapoints, diving into the history and culture to better understand references and linguistic cues, developing human sources online and beyond are all their own worlds in of themselves, and are critically important to investigating these effectively. If you'd like to learn more about these and other investigative topics, follow our publications HERE.

While there's always much to learn, Russia and China are more accessible than one may have otherwise thought. Using the above tips, sources, and techniques, we hope that your investigations and research are fruitful.

Discover the future with Falkor

Visit falkor.ai or contact us at hello@falkor.ai

More resources:

OSINT Evolution: How Collaboration Drives Innovation

Staying Secure Online: Essential Tips for Investigators

Decoding Digital Evidence: Overcoming Challenges in Cyber Investigations