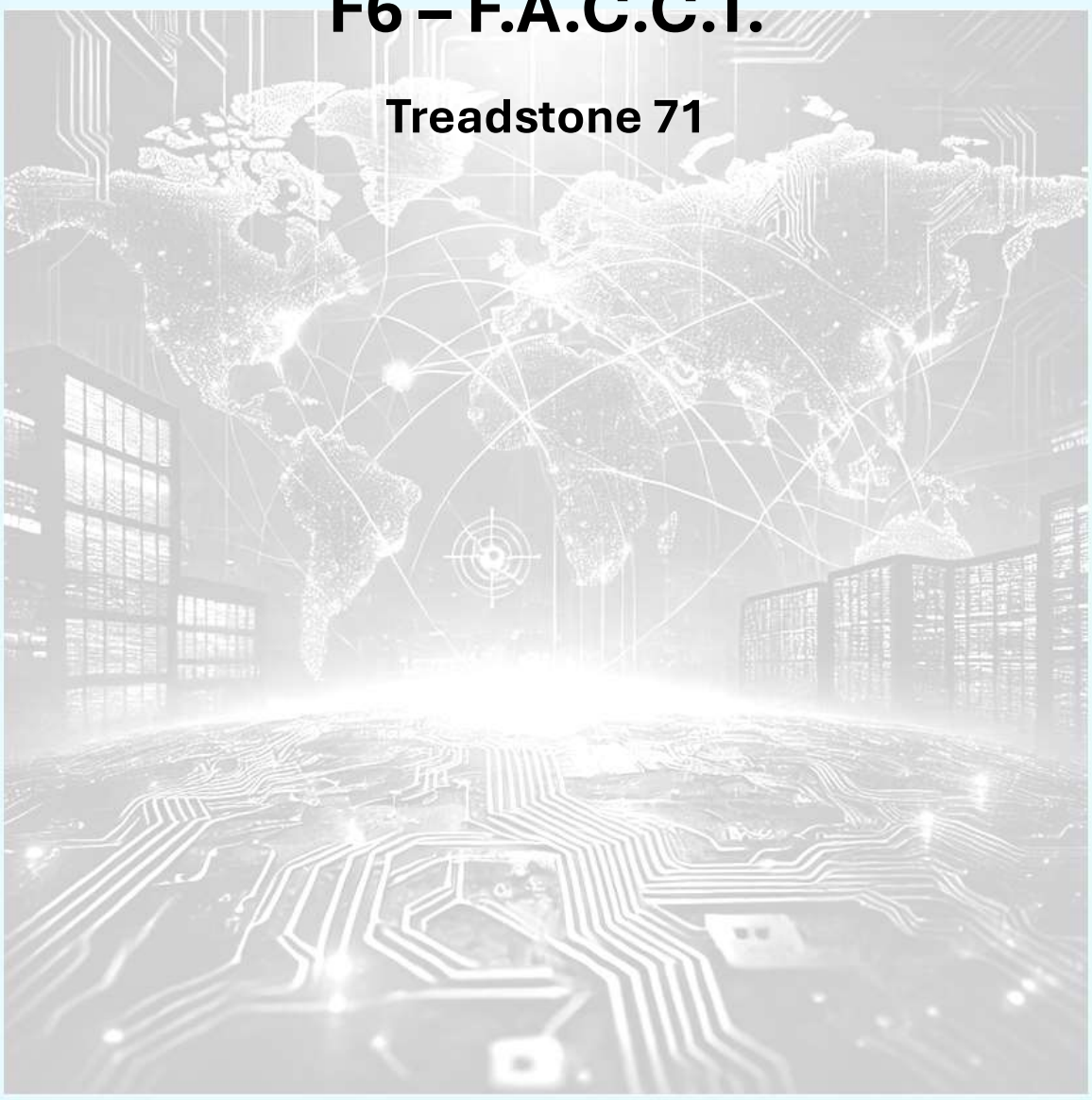
Review of the Russian Cybercrime Report (2024-2025)

F6 – F.A.C.C.T.



Treadstone 71

Summary Judgment

An Intelligence Failure Masquerading as Analysis[1]

Admiralty Scoring Model Assessment

Source Credibility: E4 – Doubtful Reliability ⬇

The F6 report fails fundamental credibility tests due to a lack of transparency, circular sourcing, and clear state-aligned bias. The authors rely primarily on their security tools and past reports, never referencing independent third-party verification or external validation. The glaring omission of Russian cyber operations while emphasizing foreign threats further erodes trust. A rating of E4 (Doubtful Reliability) is warranted, as the source appears strongly influenced by political motivations and lacks methodological rigor.

Source Validity: 3/10 – Inconsistent and Misleading ⬇

The information presented lacks verifiable sourcing, attribution remains ambiguous, and claims about cyber threats do not follow structured analytic methodologies. The report conflates different types of cyber actors without proper delineation, making its conclusions unreliable. Statistical figures lack transparency regarding data collection methods. Predictions for 2025 rely on speculation rather than structured forecasting techniques. The absence of competing hypotheses and adversarial scrutiny weakens its validity. A 3/10 rating reflects the document's inability to meet intelligence tradecraft standards.

Source Relevance: 5/10 – Selectively Useful ⟺

While the report contains some information that could be relevant to understanding Russian cybersecurity narratives, its selective framing and deliberate omissions severely limit its usefulness. Analysts seeking a genuine understanding of cyber threats must extract raw data cautiously while discarding biased interpretations. The document may provide insight into how Russian cybersecurity firms wish to frame external threats but fail as an objective intelligence product. A 5/10 rating reflects partial relevance but a high level of distortion.

Overall Rating: 3/10 – A Politicized Report with Minimal Intelligence Value ⬇

[1] No snaps, no twists, and no kisses – Hated It

The F6 cybercrime report lacks credibility, distorts analysis, and prioritizes state-aligned messaging over objective threat assessments. Methodological weaknesses, selective framing, and the absence of competing perspectives undermine its intelligence value. A score of 3/10 reflects its status as a narrative-driven document rather than a legitimate intelligence product.

Introduction

Russian cybersecurity firm F6, a rebranded successor to F.A.C.C.T., has released a report on cybercrime trends for 2024-2025. The document presents a sweeping assessment of ransomware, hacktivism, data breaches, and financially motivated cyber operations. Assertions of rising cyber threats, especially against Russian entities, drive the report's narrative. Claims of surging pro-Ukrainian cyber activity dominate the analysis, while the omission of Russian state-backed cyber operations raises immediate questions about credibility and intent.

Assertions about growing cyber risks lack transparency regarding data sources and collection methods. Reports of increased DDoS attacks and ransomware campaigns present numbers without detailing how those figures were obtained or whether biases influence the interpretation. Statements about threat actors merging tactics create an impression of convergence without dissecting the methodologies that distinguish state-backed cyber warfare from independent criminal enterprises. Analysts fail to distinguish correlation from causation, allowing speculation to masquerade as insight.

Gaps in attribution further weaken the report's integrity. Repeated mentions of specific APT groups without clear methodologies for linking them to nation-states leave conclusions unsubstantiated. The absence of alternative hypotheses about hacking incidents signals a failure in structured analytic techniques, particularly the Analysis of Competing Hypotheses. Intelligence tradecraft demands a rigorous approach to sourcing, validation, and competing interpretations, none of which appear in the report.

No attempt is made to examine how Russian cyber operations fit into global trends. Reports of leaked databases and compromised corporate infrastructures focus exclusively on Russia as a target, ignoring the extensive history of Russian cyber espionage, economic sabotage, and disinformation campaigns. The framing of foreign actors as aggressors while omitting Russia's role in cyber conflicts reflects a deliberate narrative designed to deflect scrutiny.

The transition from F.A.C.C.T. to F6 raises additional concerns about objectivity. The Cyberus Foundation, a shadowy entity now controlling the firm, remains an enigma, with no clarity about its investors or affiliations. Leadership continuity suggests an effort to maintain institutional memory while erasing inconvenient ties to Group-IB's previous leadership scandal. The restructuring positions F6 as a vehicle for state-aligned intelligence production rather than an independent cybersecurity research organization.

Failure to engage in rigorous analysis, reliance on unverified data, and omission of Russian cyber activities expose the report as a tool for narrative control. Instead of presenting a balanced, evidence-based examination of global cyber threats, the authors have produced a document that prioritizes geopolitical messaging over analytic integrity. Readers expecting an objective study of cybercrime will find a publication that obscures more than it reveals.

Cutting Edge?

The Russian Cybercrime Trends 2024-2025 Report by F6 claims to be a cutting-edge analysis of cyber threats, yet it reads like an overextended marketing brochure riddled with bias, poor sourcing, analytical failures, and outright propaganda. The document fails intelligence tradecraft standards at nearly every level, from collection and source validation to structured analytic techniques and critical thinking. It exhibits denial and deception, disinformation, and cognitive manipulation in an attempt to control the narrative about Russia's cybersecurity landscape.

Collection and Source Credibility

Self-Referential, Unverifiable, and Manipulated

- The report repeatedly cites its Threat Intelligence and Managed XDR systems as sources of data, presenting them as unimpeachable. No third-party validation, independent corroboration, or adversarial scrutiny is applied.
- Circular reporting is rampant. The authors reference past F6 reports as if they constitute new intelligence rather than recycled assumptions.
- Data reliability is unverifiable. The report makes sweeping statistical claims (e.g., number of attacks, ransomware campaigns, hacker group activities) without providing methodology, collection techniques, or even sampling transparency.
- The document assumes no Russian-sponsored cyber activity exists while painting Ukraine, Western nations, and independent hacktivists as omnipresent threats. This blatant omission of Russia's documented cyber operations reflects an intelligence distortion, not analysis.

Validity and Relevance

Haphazard Categorization, Baseless Forecasts

- Contradictory narratives plague the report. The authors claim a doubling of state-backed APT groups attacking Russia but fail to explain the methodology of attribution or why this growth allegedly occurred.
- The classification of cyber actors is a jumbled mess: hacktivists, APT groups, and financially motivated criminals are arbitrarily grouped without defined criteria, making trend analysis meaningless.
- The 2025 forecasts lack any methodological foundation. The authors list "more cyberattacks" and "rising threats" without any structured reasoning, probability assessment, or alternative outcomes analysis, posing as speculation disguised as intelligence.

Structured Analytic Techniques (SATs)

Nonexistent Application, Cognitive Biases Rampant

- No SATs (Analysis of Competing Hypotheses, Devil's Advocacy, Red Teaming, Key Assumptions, ACH) are evident. The entire report is a single-threaded narrative without consideration of alternative hypotheses.
- Confirmation bias dominates: The authors begin with the assumption that Russia is a victim of foreign cyber aggression, and every piece of information is filtered through this lens.
- Failure to consider deception: The report never evaluates the possibility of false-flag operations, attribution errors, or manipulated threat intelligence data—a fundamental failure in counterintelligence-grade analysis.

Critical Thinking and Cognitive Biases

A Case Study in Manipulation

- Appeal to fear is omnipresent: The authors push apocalyptic cyber scenarios (e.g., "digital chaos," "cosmic-scale financial losses") without quantifiable evidence.
- Straw man arguments define the adversarial framing: Ukraine and Western actors are depicted as well-coordinated, destructive forces, while Russian cyber operations are absent, aka blatant disinformation.

- False equivalency: The report equates random cybercriminals and state-sponsored groups without defining operational objectives, tactics, or capabilities, making the comparisons analytically useless.

Patterns, Trends, and Link Analysis

Nonexistent or Cherry-Picked

- The report claims "new APT groups" have emerged but provides zero longitudinal analysis of trends, operational overlaps, or indicators of persistence.
- No link analysis is applied—despite a vast dataset, there is no effort to examine relationships, common infrastructure, or shared TTPs among threat actors.
- Semiotic analysis is absent: The document discusses defacement attacks, political messaging, and hacktivist operations yet never assesses the psychological, cultural, or strategic impact of these campaigns.

Inductive, Abductive, and Deductive Reasoning

Lazy and Unstructured

- Inductive reasoning is misapplied: The authors take select incidents (e.g., a ransomware attack on a Russian company) and extrapolate broad, unsupportable trends about national security risks.
- Abductive reasoning is absent: The authors never explore competing explanations for trends, such as internal Russian corruption, insider threats, or Russia's history of cyber-enabled economic espionage.
- Deductive logic is flawed: The report claims APT threats are growing because more groups were "discovered," but this ignores detection bias, reporting changes, and geopolitical factors.

Denial, Deception, and Disinformation

A Masterclass in Narrative Control

- Complete omission of Russian cyber operations: Not a single mention of Russia's well-documented APT groups (e.g., Sandworm, Fancy Bear, Cozy Bear)—a glaring act of information suppression.
- Misinformation through overstatement: The report inflates threat actor numbers and activities without substantiating sources to create an illusion of crisis.

- Cognitive manipulation through selective framing: The cybercrime landscape is framed as an external problem when many Russian cyber threats are internally driven by corruption, state-aligned actors, and systemic weaknesses.

Analytic Writing

A Disgrace to Intelligence Standards

- Excessive fluff: The document reads more like a cybersecurity vendor's marketing whitepaper than a structured intelligence report.
- No executive summary that clearly conveys confidence levels, intelligence gaps, or structured estimates. Instead, breathless prose and alarmist rhetoric dominate.
- Overuse of passive voice and hedging language (e.g., "it is likely that," "we assume that"), which dilutes analytic rigor.

A Deliberate Misrepresentation of Cyber Threats

The Russian Cybercrime Trends 2024-2025 Report is an intelligence failure. It is methodologically unsound, analytically biased, strategically misleading, and operationally compromised. Denial and deception drive the narrative, omitting Russian cyber operations while manufacturing an external cyber threat crisis.

The report is not intelligence but a state-sanctioned attempt at cognitive control.

F6 – A Sham Intelligence Firm Built on Smoke and Mirrors

The transformation of F.A.C.C.T. into F6 under the Cyberus Foundation is nothing short of a farce, a desperate rebranding attempt to whitewash its compromised legacy, obscure its ties to state intelligence, and manufacture legitimacy in a cybersecurity industry that demands transparency and rigor. The change to F6 is not an evolution—it is a cynical ploy to cover up corruption, political purges, and a laughably weak intelligence apparatus.

F.A.C.C.T.: A Hollow Shell of a Firm Built on a Crumbling Foundation

- Born from a Fallen Empire: F.A.C.C.T. was nothing more than the discarded husk of Group-IB, a company gutted by internal strife, state intervention, and the spectacular downfall of its co-founder, Ilya Sachkov, who was jailed for treason. The only "fact" about F.A.C.C.T. is its utter failure to function independently without state control.

- Intelligence Integrity? Nonexistent. By 2024, F.A.C.C.T. was a neutered, domesticated version of its former self, stripped of its best talent, global credibility, and genuine analytic capabilities. What remains is a zombie company, staggering forward under new branding while pretending its past sins and failures no longer exist.

Cyberus Foundation: A State-Controlled Puppet Disguised as Private Investment

- Follow the Money: The Cyberus Foundation, owned by "businessman" Yuri Maximov, conveniently absorbs F.A.C.C.T.'s assets with zero transparency. How much did this "sale" cost? No one knows—because it is a façade, not a transaction.
- "Private Investors"? Laughable. The 53% stake allegedly held by private investors is deliberate misdirection—in Russia, "private" means "state-aligned oligarchs and intelligence proxies." This entire move reeks of a Kremlin-approved asset shuffle.
- Built for Narrative Warfare, Not Cybersecurity. The Cyberus Foundation is not funding cyber defense—it is consolidating state-friendly cyber operations under an entity that appears independent but is anything but. The ultimate goal? Perpetuating state-controlled cyber influence under the guise of combating cybercrime.

F6: A Branding Exercise for a Fraudulent Intelligence Operation

- Why the sudden rebranding? Because F.A.C.C.T. is a poisoned brand. Tied to treason scandals, broken trust, and compromised intelligence, F6 is a cheap attempt to scrub history.
- Valery Baulin: The Yes-Man in Charge. The newly anointed CEO of F6, Baulin, is not a visionary but a careerist bureaucrat tasked with making this sham operation appear legitimate while following strict commands.
- Inherited Staff = Inherited Mediocrity. The same "team" moving to F6 means the same group responsible for producing the weak, unverified, and misleading reports under F.A.C.C.T. Expect no new insights, no improved methodologies—just the same state-scripted disinformation.

Final Judgment: A Paper Tiger Lying About Its Strength

F6 is not a cybersecurity powerhouse—it is a repainted propaganda vehicle for the Russian state's cyber operations. Its analysts are not unbiased intelligence professionals—they are narrative engineers crafting reports that serve political objectives, not truth.

The Cyberus-backed transition of F.A.C.C.T. to F6 is a clear signal that Russian cyber intelligence is retreating into controlled, state-friendly institutions with no independent oversight. The rebranding is a joke; the leadership is a placeholder, and the intelligence output will remain as fraudulent, biased, and strategically compromised as ever.

F6 is not an evolution. It is a rebranded failure.

Wrap Up

The Russian cybercrime report from F6 claims to present a thorough analysis of emerging threats, yet it offers nothing more than a curated narrative designed to reinforce a singular viewpoint. Assertions about escalating attacks rely on opaque sourcing and unverifiable data, making broad claims without the analytical depth required for intelligence reporting. The selective framing of cyber operations as an external threat to Russia while ignoring the country's well-documented offensive activities exposes the report's true function as a controlled messaging tool rather than a neutral assessment.

A failure to apply structured analytic techniques leaves the report riddled with confirmation bias, leading to unsupported conclusions that cannot withstand scrutiny. The absence of alternative hypotheses, competing perspectives, or adversarial analysis further diminishes its credibility. Statements about cybercriminal organizations and state-backed groups collapse into vague generalizations, making it impossible to distinguish between independent criminal enterprises and intelligence-directed operations. Analysts present correlations as causal relationships, undermining any claim to rigor.

The transformation from F.A.C.C.T. to F6 signals more than a rebranding effort. The company's transition under the Cyberus Foundation suggests an intentional repositioning to align cybersecurity narratives with state interests. The continued presence of leadership from the previous organization ensures continuity in messaging, reinforcing the likelihood that future reports will maintain the same strategic omissions and misleading emphases.

A report of this nature should have engaged in a dispassionate assessment of cybercrime, drawing from diverse sources and methodologies to present a comprehensive view. Instead, the document reads as an instrument of information control designed to shape perception

rather than illuminate truth. A meaningful examination of cyber threats demands intellectual discipline, methodological precision, and a willingness to challenge assumptions. None of that exists here. However, it is Kremlin-generated.

Intelligence Methods Comparative Analysis

Russian Intelligence Analysis Standards & Methodologies

1. "Active Measures" (Активные мероприятия) Doctrine

- Russian intelligence integrates deception, influence operations, and disinformation directly into analysis, unlike Western agencies, which separate influence operations from objective intelligence assessments.
- Analysis focuses less on objective truth and more on shaping perceptions that align with strategic goals.

2. Reflexive Control Theory (Рефлексивное управление)

- Analysts develop forecasts and narratives designed to manipulate adversary decision-making rather than assess threats.
- Cyber threat analysis often blends real and fabricated information to distort an opponent's situational awareness.

3. GRU Military Doctrine & Intelligence Analysis (Военная доктрина ГРУ)

- Military cyber intelligence follows Soviet-style net assessment methodologies, focusing on asymmetrical and hybrid warfare strategies.
- Intelligence is action-oriented, often leading directly to cyber, electronic, or psychological warfare operations.

4. FSB & SVR Intelligence Reporting Methods

- Intelligence reports often emphasize geopolitical interpretations over data-driven assessments.
- No equivalent of the CIA's "Tradecraft Standards" exists—analysts operate under looser requirements for sourcing and validation.
- Analysis tends to be compartmentalized, meaning analysts receive only selective data to limit independent conclusions.

5. OSINT & Cyber Intelligence (Кибербразведка и Открытая разведка в России)

- Russian OSINT frameworks do not rely on Western validation models. Instead, analysis is shaped to support strategic state narratives.

- Cyber threat intelligence analysis focuses on foreign adversaries rather than self-assessment of Russian operations.

6. Forecasting & Strategic Foresight (Прогнозирование и Стратегическое Видение)

- Long-term intelligence planning aligns with national security strategies, often producing reports that justify state policy rather than objectively analyze cyber threats.
- Unlike Western foresight models (e.g., Pherson's Strategic Foresight), Russian forecasting integrates political warfare elements, allowing intelligence to guide influence campaigns.

7. KGB Legacy Methods (Наследие КГБ)

- Analysts are trained to view intelligence through a Marxist-Leninist dialectical lens, assessing threats not just in technical terms but as ideological and geopolitical conflicts.
- Compartmentalization and deception are core tenets, making Russian cyber intelligence reports difficult to verify against actual operational activity.

Russian intelligence analysis follows a different logic than NATO, Western intelligence agencies, or professional cyber threat intelligence firms. Reports are often crafted to serve state narratives rather than adhere to structured analytic techniques, validation processes, or adversarial challenge methodologies. The F6 cybercrime report aligns with this tradition—prioritizing perception management over analytical integrity.

US/NATO vs. Russian Intelligence Methods

Category	US/NATO (Bias & Fallacy Rating: 1-10)	Russia (Bias & Fallacy Rating: 1-10)
Source Credibility & Information Reliability	2	9
Structured Analytic Techniques	2	10
Intelligence Source Validation	3	9
Critical Thinking & Bias Mitigation	2	10
Intelligence Writing & Reporting Standards	2	10

Category	US/NATO (Bias & Fallacy Rating: 1-10)	Russia (Bias & Fallacy Rating: 1-10)
Cyber Threat Intelligence Standards	3	9
Active Measures & Disinformation	2	10
Forecasting & Strategic Foresight	3	9
Military Intelligence & Hybrid Warfare	4	10
OSINT & Attribution Standards	2	10
Legacy Intelligence Practices & Secrecy	3	10
Overall Bias Rating (Weighted Average)	2.7	9.7

The US/NATO intelligence model prioritizes analytic rigor, adversarial challenge, and independent validation, reducing bias to an average score of 2.7/10. The Russian intelligence model embeds disinformation, manipulation, and compartmentalization into its methodology, leading to an extreme bias score of 9.7/10.

Key Takeaways

1. US/NATO intelligence methods focus on transparency, independent validation, and structured methodologies to challenge assumptions. Bias mitigation techniques are formally embedded into the analytic process.
2. Russian intelligence analysis is fundamentally different—it integrates deception, state-controlled narratives, and reflexive control techniques into intelligence production. Objectivity is sacrificed in favor of political and strategic objectives.
3. US/NATO methods employ SATs, confidence level assignments, and alternative assessments to minimize errors. Russian methods, in contrast, deliberately use selective framing, omission, and controlled attribution to manipulate perception.
4. Cyber threat intelligence in the West follows rigorous attribution standards, while Russian cyber intelligence distorts attribution to serve geopolitical interests.

The F6 cybercrime report aligns entirely with Russian intelligence methods—it is a product of controlled messaging, omission, and strategic deception rather than an objective intelligence assessment.