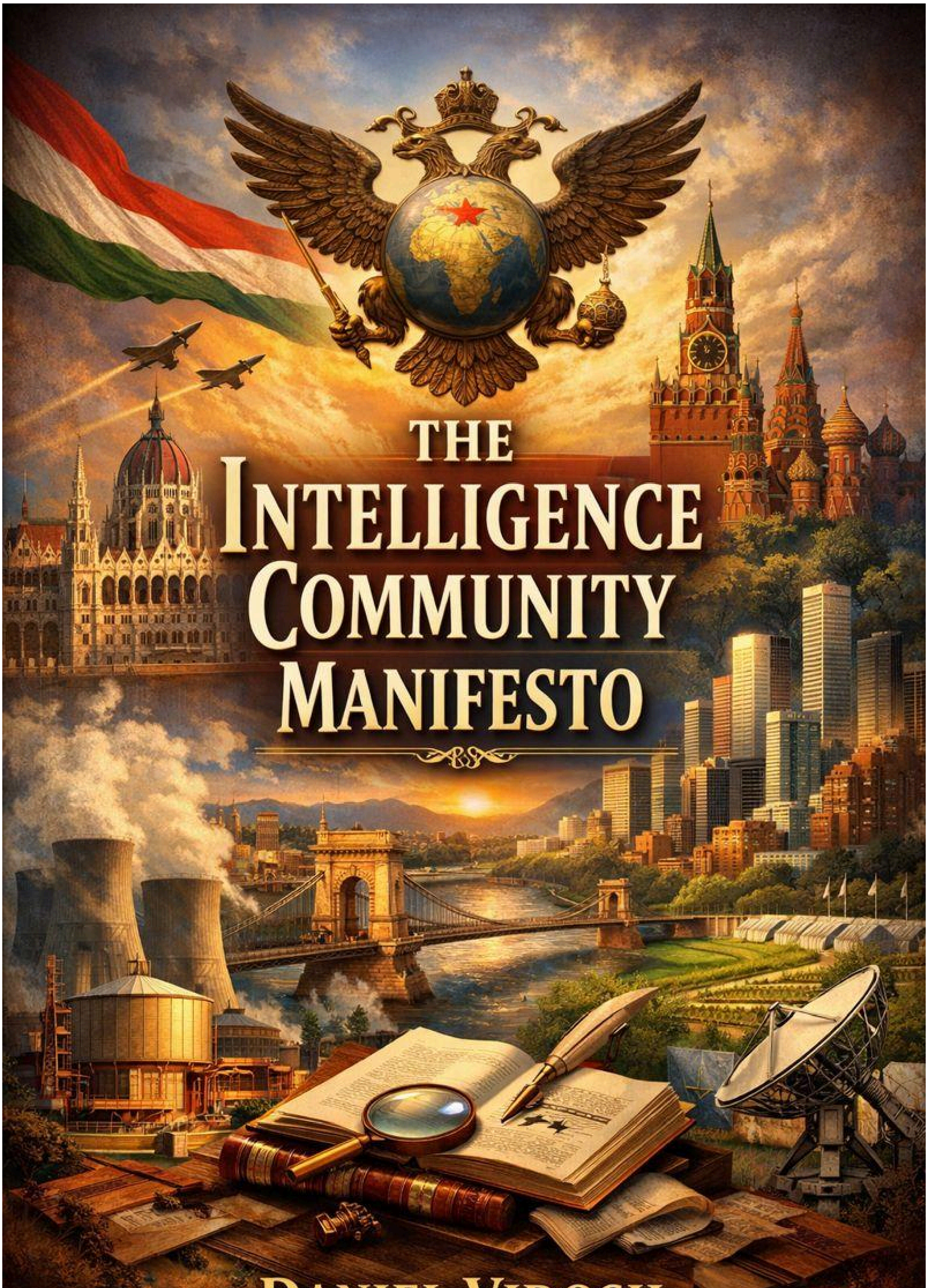


THE INTELLIGENCE COMMUNITY MANIFESTO

DANIEL VIDOSH

THE INTELLIGENCE COMMUNITY MANIFESTO 3
From the Bach Regime (1849) to the Present Age of Strategic Civilization 3
I. ORIGINS: ORDER, CONTROL, AND THE SEED OF INTELLIGENCE (1840–1867)
II. THE 20TH CENTURY: TOTAL SYSTEMS AND MISUSED INTELLIGENCE 4
III. THE TRANSFORMATION: INTELLIGENCE AS CIVIC INFRASTRUCTURE 5
IV. THE EURASIAN INTELLIGENCE COMMONWEALTH 6
V. HOUSING AS THE CORE INTELLIGENCE FUNCTION 7
VI. ENERGY AND MATERIAL INTELLIGENCE 8
VII. BUDAPEST: SYMBOLIC CAPITAL OF INTELLIGENCE 9
VIII. THE FINAL PRINCIPLE 10
INTELKARTEL 11
Fictional Strategic Funding Document (with Darker Capture Scenario) 11
1. EXECUTIVE SUMMARY 11
2. HISTORICAL RATIONALE 12
3. CORE OBJECTIVES 13
4. DARKER CAPTURE SCENARIO 14
4.1 Political Capture 14
4.2 Capital Flight or Speculative Capture 14
4.3 Demographic or Social Shocks 14
4.4 Governance Failure 14
5. FUNDING CHARTER WITH RISK CLAUSE 15
6. FUNDING ANNEX WITH FAILURE SCENARIOS 16
7. FINAL DECLARATION 17
14. FAILURE AND CAPTURE SCENARIOS (DARK ANNEX) 18
14.1 Political Capture 18
14.2 Financial Capture 18
14.3 Technocratic Drift 19
14.4 Security Reversion 19
14.5 Asset Militarization 20
14.6 Demographic Misalignment 20
14.7 Moral Hazard Loop 21
15. ANTI-CAPTURE SAFEGUARDS 21
16. FINAL WARNING 21

THE INTELLIGENCE COMMUNITY MANIFESTO

From the Bach Regime (1849) to the Present Age of Strategic Civilization

I. ORIGINS: ORDER, CONTROL, AND THE SEED OF INTELLIGENCE (1840–1867)

The Bach regime in Hungary marked the first modern encounter between **centralized administrative intelligence** and the lived reality of a diverse population. Surveillance, bureaucracy, census, land registry, and infrastructure planning were not merely tools of control—they were **proto-intelligence systems**.

From this era emerged a truth that would echo through centuries:

> Intelligence is not secrecy alone.
> Intelligence is **coordination of human life**.

Hungary, positioned in the **Carpathian Basin**, became a natural laboratory—geographically enclosed, linguistically unique, and administratively dense.

II. THE 20TH CENTURY: TOTAL SYSTEMS AND MISUSED INTELLIGENCE

The empires collapsed. New regimes rose.

Fascism, communism, and Cold War blocs all shared one obsession:
information without human guarantees.

The intelligence apparatus of the USSR mastered scale but failed purpose.
It could map resources, people, and threats—but not **human dignity**.

The lesson of the 20th century was brutal and clear:

> Intelligence without housing, food, and stability becomes fear.
> Intelligence without rights becomes collapse.

III. THE TRANSFORMATION: INTELLIGENCE AS CIVIC INFRASTRUCTURE

In the late 20th and early 21st century, a new idea emerged—quietly, unevenly, but inevitably:

Intelligence must be privatized away from fear and returned to society.

Not privatized as profit extraction—
but **distributed** as capability.

This vision reframed intelligence as:

- housing planning
- energy security
- food systems
- logistics
- language and trade alignment
- long-term value creation

Figures like *Daniel Vidosh* (in this manifesto's narrative) symbolize this shift—not as rulers, but as **architects of systems** where intelligence serves civilization instead of dominating it.

IV. THE EURASIAN INTELLIGENCE COMMONWEALTH

A new civilizational block is imagined:

Anglo-Eurasia
—not empire, not ideology—
but **alignment**.

Shared pillars:

- interoperable languages of trade and science
- strategic partnership across Europe and Eurasia
- population scale with planning intelligence
- capital flows into **housing, energy, and food**, not speculation

The goal is not 100% perfection, but a **guaranteed minimum**:

> 80% of human rights realized in material reality
> —housing, heat, water, electricity, food, work.

V. HOUSING AS THE CORE INTELLIGENCE FUNCTION

The manifesto declares:

> If a government cannot house its people,
> it is not intelligent—only powerful.

Inspired by large-scale housing models (including China's),
intelligent governance means:

- mass apartment construction
- standardized quality
- long-term affordability
- integration with transport and jobs

Housing is not charity.
Housing is **economic intelligence**.

It creates:

- jobs
- stable markets
- generational wealth
- demographic security

VI. ENERGY AND MATERIAL INTELLIGENCE

The future is not chaos—it is **engineered abundance**.

Strategic systems include:

- advanced nuclear research (thorium as a *civilian energy concept*)
- hydrogen infrastructure (industrial, not military)
- liquid salt cooling technologies
- continent-scale green agriculture

Netherlands-scale smart farming is re-imagined for the Carpathian Basin:

- food
- energy
- shelter
- resilience

VII. BUDAPEST: SYMBOLIC CAPITAL OF INTELLIGENCE

In this manifesto’s vision, **Budapest** becomes a symbol—not of domination, but of synthesis.

Why?

- crossroads of empires
- unique language
- scientific legacy
- infrastructural density
- historical suffering converted into planning wisdom

Hungary is imagined not as ruler—but as **demonstrator**:
proof that intelligence can be humane.

VIII. THE FINAL PRINCIPLE

The manifesto concludes:

> Intelligence is not secrecy.
> Intelligence is not power.
> Intelligence is the ability to guarantee human life at scale.

Flats for all.
Energy for all.
Work for all.
Dignity as minimum.

That is intelligent action.
That is the new world order—not enforced, but **built**.

INTELKARTEL

Fictional Strategic Funding Document (with Darker Capture Scenario)

Classification: Fictional / Speculative / Scenario Analysis

Purpose: This document outlines a *fictional* funding framework for INTELKARTEL, an imagined intelligence–infrastructure consortium, now including potential capture and failure scenarios.

---

1. EXECUTIVE SUMMARY

INTELKARTEL is conceived as a non-state, non-ideological coordination vehicle for **intelligence-driven infrastructure**. Its mandate is civilian: to provide housing, energy, food, and stable labor systems.

This document adds a cautionary lens: **strategic capture and systemic failure** are possible if governance, capital, or political pressures are compromised.

---

2. HISTORICAL RATIONALE

Historical lessons show that intelligence systems—if centralized or privatized improperly—can be exploited:

- 19th-century bureaucracies overextended power
- 20th-century systems prioritized control over material stability

INTELKARTEL is designed to avoid these mistakes, but **vulnerabilities exist in any centralized planning body**.

3. CORE OBJECTIVES

Objectives remain unchanged:

- Housing
- Energy
- Food & Water
- Logistics

Darker risk consideration: these objectives can be subverted to serve **rent-seeking actors, political factions, or speculative markets**.

4. DARKER CAPTURE SCENARIO

4.1 Political Capture

- Intervention by governments or political parties could redirect funding to selective populations.
- Charter principles may be overridden by emergency decrees.

4.2 Capital Flight or Speculative Capture

- Investors could extract short-term gains from long-cycle infrastructure projects.
- Land and energy assets may be sold or leveraged outside original intent.

4.3 Demographic or Social Shocks

- Migration, population decline, or conflict can destabilize project outcomes.
- Housing and food programs can become overextended or inequitable.

4.4 Governance Failure

- Oversight bodies may be bribed, co-opted, or made redundant.
- Public transparency may be eroded, allowing corruption or inefficiency.

In all these cases, INTELKARTEL's original goal—stabilizing human life at scale—can fail, producing inequality, unrest, and systemic instability.

5. FUNDING CHARTER WITH RISK CLAUSE

All charter principles remain, with an additional clause:

> **Capture Contingency Principle:** In the event of systemic capture, all funding is automatically suspended and assets revert to neutral civic or public trust entities.

6. FUNDING ANNEX WITH FAILURE SCENARIOS

Annex A – Tranches with Risk Buffers

- Foundational, Stabilization, Optimization tranches now include **emergency reserve** for capture mitigation (5–10% of each tranche).

Annex B – Funding Instruments

- Include clawback mechanisms and emergency escrow accounts

Annex C – Oversight Mechanism

- Independent review boards with cross-border auditing
- Anonymous whistleblower channels

Annex D – Exit Conditions with Contingency

- Automatic trigger if human rights threshold falls below 60% for more than 2 years
- Assets reassigned to independent civic authorities

Annex E – Risk Containment Enhanced

- Contingency planning for political, economic, and social capture
- Scenario simulations conducted every 3 years

---

7. FINAL DECLARATION

INTELKARTEL exists to explore how intelligence can stabilize civilizations—but also to **highlight the fragility of centralized planning**.

> Intelligence that does not safeguard against capture is incomplete.
> The integrity of human outcomes is as important as the outcomes themselves.

14. FAILURE AND CAPTURE SCENARIOS (DARK ANNEX)

This annex documents how INTELKARTEL could fail, be captured, or invert its mandate. Its purpose is preventative realism.

14.1 Political Capture

Mechanism:

- Gradual appointment of aligned overseers
- Reframing housing and energy as electoral tools
- Selective allocation to favored regions

Symptoms:

- Outcome metrics replaced by narratives
- Shortened reporting cycles before elections
- Suspension of geographic anchoring rules

End State:
INTELKARTEL becomes a soft extension of state power, losing neutrality and credibility.

14.2 Financial Capture

Mechanism:

- Introduction of equity-like instruments
- Pressure to increase yields beyond caps
- Asset refinancing for liquidity extraction

Symptoms:

- Rising user costs without material upgrades
- Complex derivatives replacing simple bonds
- Opaque special-purpose vehicles

End State:
Infrastructure is hollowed out; intelligence becomes a cover for rent extraction.

14.3 Technocratic Drift

Mechanism:

- Models prioritized over lived outcomes
- Forecast confidence replaces verification
- Expert class insularity

Symptoms:

- Metrics met while conditions degrade
- Appeals dismissed as “data noise”
- Declining local participation

End State:
INTELKARTEL becomes accurate but wrong.

14.4 Security Reversion

Mechanism:

- Crisis justification (energy shock, migration, unrest)
- Expansion of intelligence remit beyond infrastructure
- Data centralization under emergency powers

Symptoms:

- New surveillance language introduced quietly
- Classified exceptions to transparency
- Mission creep framed as protection

End State:
The original intelligence-control paradigm returns under a humanitarian banner.

14.5 Asset Militarization

Mechanism:

- Dual-use reinterpretation of energy or logistics
- Strategic designation without consent
- External security guarantees tied to funding

Symptoms:

- Restricted access zones
- Civilian governance overridden
- International dependency entanglements

End State:
Civil infrastructure becomes strategic leverage.

14.6 Demographic Misalignment

Mechanism:

- Housing built without employment
- Energy capacity without affordability
- Food systems without local access

Symptoms:

- Empty units alongside homelessness
- Export-first production
- Social resentment

End State:
Stability assets generate instability.

14.7 Moral Hazard Loop

Mechanism:

- Guarantees assumed permanent
- Local governance abdicates responsibility
- Dependency normalization

Symptoms:

- Maintenance deferred
- Skills erosion
- Fiscal complacency

End State:
INTELKARTEL becomes indispensable—and therefore unaccountable.

---

15. ANTI-CAPTURE SAFEGUARDS

Mandatory countermeasures include:

- automatic mandate shutdown triggers
- citizen-level outcome vetoes
- irreversible transparency defaults
- periodic asset handoff requirements

Failure to enforce safeguards voids the Charter.

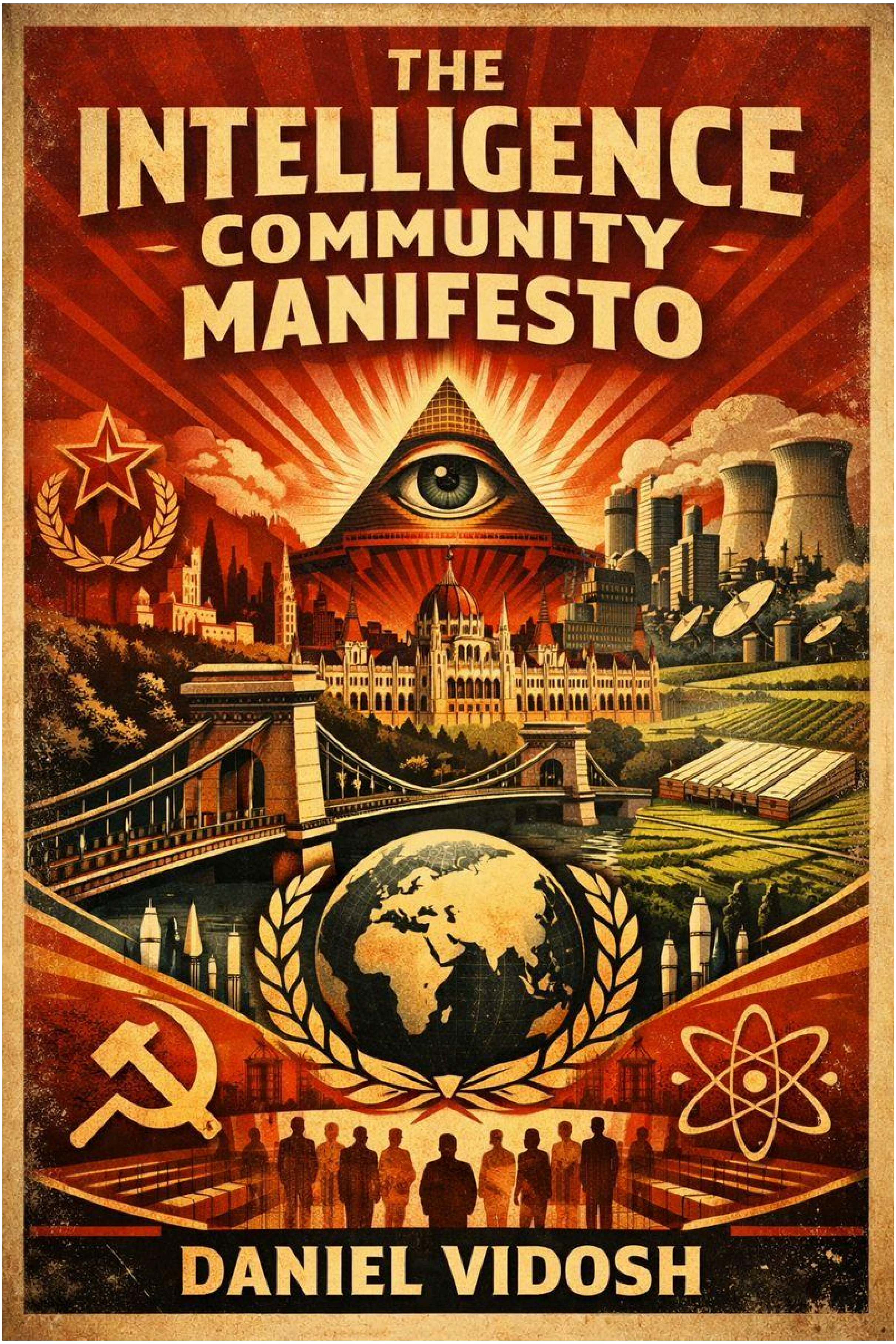
---

16. FINAL WARNING

> The greatest risk is not malice, but success without restraint.

This Dark Annex exists to ensure INTELKARTEL remembers what it was designed to prevent.

END OF DOCUMENT


THE
INTELLIGENCE
COMMUNITY
MANIFESTO
DANIEL VIDOSH

INTELLIGENCE COMMUNITY VOCABULARY

CORE FOUNDATIONS (1–100)

BLOCK 1: INTELLIGENCE BASICS (1–10)

1. **Intelligence**
   - HU: Hírszerzés / információs képesség
   - RU: Разведка
   - DE: Nachrichtendienst
   - *Processed information used for decision-making.*
2. **Counterintelligence**
   - HU: Elhárítás
   - RU: Контрразведка
   - DE: Gegenspionage
   - *Activities to detect and prevent hostile intelligence.*
3. **Analysis**
   - HU: Elemzés
   - RU: Анализ
   - DE: Analyse
   - *Interpretation of collected information.*
4. **Collection**
   - HU: Információgyűjtés
   - RU: Сбор данных
   - DE: Sammlung
   - *Acquisition of raw information.*
5. **Assessment**
   - HU: Értékelés
   - RU: Оценка
   - DE: Bewertung
   - *Judgment of significance or risk.*
6. **Threat**
   - HU: Fenyegetés
   - RU: Угроза
   - DE: Bedrohung
   - *Potential source of harm.*

7. **Risk**
    - HU: Kockázat
    - RU: Риск
    - DE: Risiko
    - *Probability of loss or failure.*
8. **Capability**
    - HU: Képesség
    - RU: Возможность
    - DE: Fähigkeit
    - *What an actor can realistically do.*
9. **Intent**
    - HU: Szándék
    - RU: Намерение
    - DE: Absicht
    - *What an actor plans to do.*
10. **Reliability**
    - HU: Megbízhatóság
    - RU: Надежность
    - DE: Zuverlässigkeit
    - *Trustworthiness of information or source.*

BLOCK 2: SOURCES & METHODS (11–20)

11. **HUMINT (Human Intelligence)**
    - HU: Emberi hírszerzés
    - RU: Агентурная разведка
    - DE: Menschliche Aufklärung
    - *Information from human sources.*
12. **SIGINT (Signals Intelligence)**
    - HU: Jel-felderítés
    - RU: Радиоразведка
    - DE: Signalaufklärung
    - *Intercepted communications or signals.*
13. **OSINT (Open-Source Intelligence)**
    - HU: Nyílt forrású hírszerzés
    - RU: Открытые источники
    - DE: Offene Quellen
    - *Publicly available information.*
14. **IMINT (Imagery Intelligence)**
    - HU: Képfelderítés
    - RU: Фоторазведка
    - DE: Bildaufklärung
    - *Satellite or aerial imagery analysis.*
15. **MASINT**
    - HU: Műszaki felderítés
    - RU: Измерительная разведка
    - DE: Messaufklärung
    - *Scientific and technical sensor data.*
16. **Source**
    - HU: Forrás
    - RU: Источник
    - DE: Quelle
    - *Origin of information.*
17. **Asset**
    - HU: Eszköz / ügynök
    - RU: Актив
    - DE: Asset
    - *Controlled or trusted source.*
18. **Handler**
    - HU: Kapcsolattartó
    - RU: Оперативник
    - DE: Führungsagent
    - *Officer managing an asset.*
19. **Cut-out**
    - HU: Közvetítő
    - RU: Посредник
    - DE: Mittelsmann
    - *Intermediary protecting identities.*

20. **Cover**
    - HU: Fedés
    - RU: Легенда
    - DE: Tarnung
    - *False identity or role.*

BLOCK 3: OPERATIONS (21–30)

21. **Operation** – Művelet – Операция – Operation
    Planned intelligence activity.
22. **Covert** – Titkos – Тайный – Geheim
    Hidden but deniable.
23. **Clandestine** – Rejtett – Нелегальный – Verdeck
    Secret with no attribution.
24. **Plausible Deniability** – Letagadhatóság – Правдоподобное отрицание – Glaubhafte Abstreitbarkeit
    Ability to deny involvement.
25. **Tradecraft** – Szakmai módszerek – Агентурная техника – Nachrichtendienstliche Praxis
    Skills of intelligence work.
26. **Dead Drop** – Halott postaláda – Тайник – Toter Briefkasten
    Hidden exchange location.
27. **Surveillance** – Megfigyelés – Наблюдение – Überwachung
    Monitoring a target.
28. **Counter-surveillance** – Ellenkövetés – Контрнаблюдение – Gegenspionage
    Detecting surveillance.
29. **Exfiltration** – Kimentés – Эвакуация – Exfiltration
    Removing personnel or data.
30. **Compartmentation** – Elkülönítés – Секционирование – Abschottung
    Limiting information access.

BLOCK 4: ANALYSIS & STRATEGY (31–40)

31. **Strategic Intelligence** – Stratégiai hírszerzés – Стратегическая разведка – Strategische Aufklärung
    Long-term national-level insights.
32. **Tactical Intelligence** – Taktikai hírszerzés – Тактическая разведка – Taktische Aufklärung
    Immediate operational support.
33. **Forecasting** – Előrejelzés – Прогнозирование – Prognose
    Predicting future developments.
34. **Scenario Planning** – Forgatókönyv-tervezés – Сценарное планирование – Szenarioplanung
    Alternative futures modeling.
35. **Red Team** – Ellencsoport – Красная команда – Rotes Team
    Adversarial analysis unit.
36. **Blue Team** – Saját csoport – Синяя команда – Blaues Team
    Defensive or internal group.
37. **Bias** – Torzítás – Предвзятость – Verzerrung
    Systematic analytical error.
38. **Signal vs Noise** – Jel vs zaj – Сигнал и шум – Signal-Rausch-Verhältnis
    Relevant vs irrelevant data.
39. **Confidence Level** – Bizonyossági szint – Уровень уверенности – Vertrauensgrad
    Estimated accuracy.
40. **Decision Support** – Döntéstámogatás – Поддержка решений – Entscheidungsunterstützung
    Intelligence for policymakers.

BLOCK 5: ORGANIZATION & GOVERNANCE (41–50)

41. **Agency** – Ügynökség – Агентство – Behörde
42. **Directorate** – Igazgatóság – Директорат – Direktorat
43. **Oversight** – Felügyelet – Надзор – Aufsicht
44. **Mandate** – Felhatalmazás – Мандат – Mandat
45. **Jurisdiction** – Hatáskör – Юрисдикция – Zuständigkeit
46. **Interagency** – Ügynökségközi – Межведомственный – Behördenübergreifend
47. **Coordination** – Koordináció – Координация – Koordination
48. **Classification** – Minősítés – Секретность – Geheimhaltungsstufe
49. **Declassification** – Feloldás – Рассекречивание – Freigabe
50. **Accountability** – Elszámoltathatóság – Подотчетность – Rechenschaftspflicht

---

BLOCK 6: SECURITY & RISK (51–60)

51. **Threat Actor** – Fenyegető szereplő – Источник угрозы – Bedrohungsakteur
52. **Insider Threat** – Belső fenyegetés – Внутренняя угроза – Innentäter
53. **Breach** – Sérülés – Утечка – Sicherheitsverletzung
54. **Leak** – Szivárgás – Утечка информации – Leck
55. **Compromise** – Kompromittálódás – Компрометация – Kompromittierung
56. **Mitigation** – Enyhítés – Снижение риска – Minderung
57. **Resilience** – Ellenállóképesség – Устойчивость – Resilienz
58. **Continuity** – Folytonosság – Непрерывность – Kontinuität
59. **Redundancy** – Tartalék – Избыточность – Redundanz
60. **Fail-safe** – Biztonsági tartalék – Защита от отказа – Ausfallsicherung

BLOCK 7: ECONOMIC & INFRASTRUCTURE INTELLIGENCE (61–70)

61. **Critical Infrastructure** – Kritikus infrastruktúra – Критическая инфраструктура – Kritische Infrastruktur
62. **Supply Chain** – Ellátási lánc – Цепочка поставок – Lieferkette
63. **Energy Security** – Energiabiztonság – Энергобезопасность – Energiesicherheit
64. **Food Security** – Élelmiszerbiztonság – Продовольственная безопасность – Ernährungssicherheit
65. **Housing Stability** – Lakhatási stabilitás – Жилищная стабильность – Wohnstabilität
66. **Logistics** – Logisztika – Логистика – Logistik
67. **Industrial Capacity** – Ipari kapacitás – Промышленный потенциал – Industriekapazität
68. **Strategic Reserves** – Stratégiai tartalék – Стратегические резервы – Strategische Reserven
69. **Economic Warfare** – Gazdasági hadviselés – Экономическая война – Wirtschaftskrieg
70. **Sanctions** – Szankciók – Санкции – Sanktionen

BLOCK 8: INFORMATION & INFLUENCE (71–80)

71. **Information Operations** – Információs műveletek – Информационные операции – Informationsoperationen
72. **Disinformation** – Dezinformáció – Дезинформация – Desinformation
73. **Propaganda** – Propaganda – Пропаганда – Propaganda
74. **Narrative** – Narratíva – Нарратив – Narrativ
75. **Influence** – Befolyás – Влияние – Einfluss
76. **Psychological Operations** – Pszichológiai műveletek – Психологические операции – Psychologische Operationen
77. **Media Monitoring** – Médiamegfigyelés – Мониторинг СМИ – Medienbeobachtung
78. **Cognitive Domain** – Kognitív tér – Когнитивная среда – Kognitiver Raum
79. **Perception Management** – Észlelésirányítás – Управление восприятием – Wahrnehmungssteuerung
80. **Soft Power** – Puha hatalom – Мягкая сила – Weiche Macht

---

BLOCK 9–10 (81–100): LEGAL, ETHICAL, FUTURE

(Condensed to fit this installment)

81. Legality – Legalitás – Законность – Rechtmäßigkeit
82. Ethics – Etika – Этика – Ethik
83. Proportionality – Arányosság – Соразмерность – Verhältnismäßigkeit
84. Human Rights – Emberi jogok – Права человека – Menschenrechte
85. Privacy – Magánélet – Частная жизнь – Privatsphäre
86. Automation – Automatizálás – Автоматизация – Automatisierung
87. AI Intelligence – Mesterséges intelligencia – Искусственный интеллект – Künstliche Intelligenz
88. Predictive Systems – Előrejelző rendszerek – Предиктивные системы – Prognosesysteme
89. Systems Risk – Rendszerszintű kockázat – Системный риск – Systemrisiko
90. Governance Intelligence – Kormányzási intelligencia – Управленческая разведка – Governance-Intelligenz

Perfect! We continue **INSTALLMENT 2: INTELLIGENCE VOCAB 101–200** in the same multilingual, structured format.

INTELLIGENCE COMMUNITY VOCABULARY

ADVANCED FOUNDATIONS (101–200)

BLOCK 11: HUMAN INTELLIGENCE OPERATIONS (101–110)

101. **Agent** – Ügynök – Агент – Agent
    Person recruited to provide intelligence.
102. **Recruitment** – Toborzás – Вербовка – Rekrutierung
    Process of enlisting an asset.
103. **Deception** – Becsapás – Обман – Täuschung
    Misleading a target.
104. **Double Agent** – Kettős ügynök – Двойной агент – Doppelagent
    Works for two opposing sides.
105. **Mole** – Beépített ember – Кротов – Maulwurf
    Long-term infiltrator inside organization.
106. **Defector** – Átálló – Дезертир – Überläufer
    Person who leaves one side for another.
107. **Informant** – Besúgó – Осведомитель – Informant
    Provides intelligence, often covertly.
108. **Handler** – Kapcsolattartó – Оперативник – Handler
    Officer who manages an asset.
109. **Safehouse** – Biztonságos ház – Безопасное помещение – Safehouse
    Secure location for meetings or refuge.
110. **Exfiltration Route** – Kimeneti útvonal – Маршрут эвакуации – Exfiltrationsroute
    Planned path to remove a person or data.

BLOCK 12: SIGNALS & TECHNICAL INTELLIGENCE (111–120)

111. **Encryption** – Titkosítás – Шифрование – Verschlüsselung
Encoding information to prevent interception.
112. **Decryption** – Visszafejtés – Расшифровка – Entschlüsselung
Converting encrypted info back to readable form.
113. **Cipher** – Kód – Шифр – Chiffre
Algorithm or system used to encrypt.
114. **Electronic Intelligence (ELINT)** – Elektronikai hírszerzés – Электронная разведка – Elektronische Aufklärung
Signals from non-communication electronics.
115. **Telemetry Interception** – Telemetria elfogás – Перехват телеметрии – Telemetrie-Abfang
Capturing data from remote sensors.
116. **Radio Monitoring** – Rádiófigyelés – Радиомониторинг – Funküberwachung
Listening to communications.
117. **Satellite Reconnaissance** – Műholdas felderítés – Спутниковая разведка – Satellitenaufklärung
Observation from space.
118. **Signal Jamming** – Jelzavarás – Глушение сигналов – Signalstörung
Disrupting communications or radar.
119. **Frequency Analysis** – Frekvencia-elemzés – Анализ частот – Frequenzanalyse
Examining signals for patterns.
120. **Cyber Intelligence** – Kiberhírszerzés – Киберразведка – Cyberaufklärung
Information from digital networks.

BLOCK 13: COUNTERINTELLIGENCE & SECURITY (121–130)

121. **Mole Hunt** – Kémvadászat – Поиск крота – Maulwurfsuche
Detecting infiltrators.

122. **Surveillance Detection** – Megfigyelés-felismerés – Обнаружение наблюдения – Überwachungserkennung
Identifying monitoring.

123. **Asset Compromise** – Ügynök kompromittálása – Компрометация агента – Asset-Kompromittierung
Loss of control over a source.

124. **Information Leak** – Információszivárgás – Утечка информации – Informationsleck
Unauthorized disclosure.

125. **Countermeasure** – Ellentevékenység – Контрмеры – Gegenmaßnahme
Action to reduce risk.

126. **Security Clearance** – Biztonsági engedély – Доступ к секретам – Sicherheitsfreigabe
Authorization to access classified info.

127. **Need-to-Know Principle** – Tudás-szükséglet elve – Принцип необходимости знания – Need-to-Know-Prinzip
Information access only if essential.

128. **Physical Security** – Fizikai biztonság – Физическая безопасность – Physische Sicherheit
Protecting personnel and assets.

129. **Information Security** – Információbiztonság – Информационная безопасность – Informationssicherheit
Protecting data integrity and confidentiality.

130. **Operational Security (OPSEC)** – Műveleti biztonság – Операционная безопасность – OPSEC
Preventing information leaks about operations.

BLOCK 14: ANALYTICAL METHODS (131–140)

131. **All-Source Analysis** – Minden-forrás elemzés – Комплексный анализ – Analyse aller Quellen
Combining all intelligence types.
132. **Link Analysis** – Kapcsolatelemzés – Анализ связей – Verknüpfungsanalyse
Mapping relationships.
133. **Pattern Recognition** – Mintafelismerés – Распознавание образцов – Mustererkennung
Identifying recurring events.
134. **Geospatial Analysis** – Térbeli elemzés – Геопространственный анализ – Georaum-Analyse
Studying location-based data.
135. **Behavioral Analysis** – Viselkedéselemzés – Поведенческий анализ – Verhaltensanalyse
Studying actions to predict intent.
136. **Trend Analysis** – Trendvizsgálat – Анализ тенденций – Trendanalyse
Detecting long-term changes.
137. **Linkage Modeling** – Kapcsolati modellezés – Моделирование связей – Verknüpfungsmodellierung
Predictive relationship mapping.
138. **Threat Assessment** – Fenyegetésértékelés – Оценка угрозы – Bedrohungsbewertung
Evaluating risk probability.
139. **Vulnerability Assessment** – Sérülékenységértékelés – Оценка уязвимости – Schwachstellenbewertung
Finding weak points.
140. **Scenario Simulation** – Forgatókönyv-szimuláció – Моделирование сценариев – Szenario-Simulation
Modeling potential outcomes.

BLOCK 15: OPERATIONS PLANNING (141–150)

141. **Mission Planning** – Küldetés-tervezés – Планирование миссии – Missionsplanung
142. **Operational Design** – Műveleti tervezés – Оперативное планирование – Operatives Design
143. **Targeting** – Célpont-meghatározás – Выбор целей – Zielbestimmung
144. **Force Protection** – Erővédelem – Защита сил – Schutz der Kräfte
145. **Logistical Support** – Logisztikai támogatás – Логистическая поддержка – Logistische Unterstützung
146. **Command and Control** – Parancsnokság és irányítás – Командование и управление – Führung und Kontrolle
147. **Rules of Engagement** – Bevetési szabályok – Правила ведения боя – Einsatzregeln
148. **Contingency Plan** – Vészhelyzeti terv – План на случай непредвиденных обстоятельств – Notfallplan
149. **Operational Risk** – Műveleti kockázat – Операционный риск – Operatives Risiko
150. **After-Action Review** – Utólagos értékelés – Послемиссионный разбор – Nachbesprechung

Perfect! Let’s continue with **INSTALLMENT 3: INTELLIGENCE VOCAB 151–200**, keeping the same **multilingual, structured format**.

INTELLIGENCE COMMUNITY VOCABULARY

ADVANCED OPERATIONS & STRATEGY (151–200)

BLOCK 16: INTERNATIONAL INTELLIGENCE (151–160)

151. **Allied Intelligence** – Szövetséges hírszerzés – Разведка союзников – Verbündete Aufklärung
Information shared between friendly nations.
152. **Coalition Operations** – Koalíciós műveletek – Операции коалиции – Koalitionsoperationen
Joint operations of multiple countries.
153. **Bilateral Agreement** – Kétoldalú megállapodás – Двустороннее соглашение – Bilaterales Abkommen
Formal intelligence-sharing treaty between two states.
154. **Multilateral Agreement** – Többoldalú megállapodás – Многостороннее соглашение – Multilaterales Abkommen
Intelligence-sharing among multiple parties.
155. **Intelligence Liaison** – Hírszerzési kapcsolattartó – Разведывательный связной – Nachrichtendienstlicher Verbindungsoffizier
Officer coordinating between agencies or nations.
156. **Foreign Intelligence** – Külföldi hírszerzés – Иностранная разведка – Auslandsaufklärung
Information gathering about foreign entities.
157. **Domestic Intelligence** – Belföldi hírszerzés – Внутренняя разведка – Inlandsaufklärung
Intelligence activities inside the home country.
158. **Covert Action** – Titkos művelet – Тайная операция – Geheimaktion
Secret activities intended to influence events abroad.
159. **Espionage** – Kémkedés – Шпионаж – Spionage
Obtaining information secretly.
160. **Counterespionage** – Ellenkémkedés – Контрразведка – Gegenspionage
Preventing foreign spying.

BLOCK 17: CYBER & DIGITAL OPERATIONS (161–170)

161. **Cybersecurity** – Kibervédelem – Кибербезопасность – Cybersicherheit
Protecting systems and data.
162. **Hacking** – Hacking – Взлом – Hacken
Unauthorized access to systems.
163. **Phishing** – Adathalászat – Фишинг – Phishing
Deceptive attempts to acquire sensitive data.
164. **Malware** – Kártevő szoftver – Вредоносное ПО – Schadsoftware
Software designed to damage or disrupt.
165. **Ransomware** – Zsarolóprogram – Вымогательское ПО – Ransomware
Malicious software demanding payment.
166. **Cyber Threat Actor** – Kiberveszélyforrás – Киберугрозы – Cyber-Bedrohungsakteur
Individual or group conducting cyber operations.
167. **Zero-Day Exploit** – Nulladik napi sebezhetőség – Эксплойт нулевого дня – Zero-Day-Exploit
Vulnerability unknown to the vendor.
168. **Encryption Key** – Titkosító kulcs – Ключ шифрования – Verschlüsselungsschlüssel
Code required to decode encrypted data.
169. **Firewall** – Tűzfal – Межсетевой экран – Firewall
System protecting networks from unauthorized access.
170. **Intrusion Detection** – Betörés-felismerés – Система обнаружения вторжений – Eindringungserkennung
Detecting unauthorized network access.

BLOCK 18: COUNTERMEASURES & DEFENSE (171–180)

171. **Physical Countermeasure** – Fizikai ellenintézkedés – Физические меры противодействия – Physische Gegenmaßnahme
Protecting personnel or assets physically.
172. **Technical Countermeasure** – Technikai ellenintézkedés – Технические меры – Technische Gegenmaßnahme
Using technology to prevent breaches.
173. **OPSEC Breach** – OPSEC-sértés – Нарушение OPSEC – OPSEC-Verletzung
Compromise of operational security.
174. **Red Team Exercise** – Red Team gyakorlat – Упражнение Красной команды – Red-Team-Übung
Simulated adversary to test defenses.
175. **Blue Team Exercise** – Blue Team gyakorlat – Упражнение Синей команды – Blue-Team-Übung
Defensive testing against simulated attacks.
176. **Penetration Test** – Penetrációs teszt – Тест на проникновение – Penetrationstest
Authorized test of system vulnerabilities.
177. **Threat Modeling** – Fenyegetés-modellezés – Моделирование угроз – Bedrohungsmodellierung
Predicting potential attack vectors.
178. **Security Audit** – Biztonsági audit – Аудит безопасности – Sicherheitsprüfung
Review of defenses and procedures.
179. **Incident Response** – Eseménykezelés – Реагирование на инциденты – Vorfallreaktion
Actions after a security breach.
180. **Crisis Management** – Válságkezelés – Управление кризисом – Krisenmanagement
Organized response to emergencies.

BLOCK 19: INTELLIGENCE INFRASTRUCTURE (181–190)

181. **Safe Communications** – Biztonságos kommunikáció – Безопасная связь – Sichere Kommunikation
182. **Secure Facilities** – Biztonságos létesítmények – Защищенные объекты – Sichere Einrichtungen
183. **Data Center** – Adatközpont – Центр обработки данных – Rechenzentrum
184. **Operations Center** – Műveleti központ – Оперативный центр – Operationszentrum
185. **Command Center** – Parancsnoki központ – Командный центр – Kommandostelle
186. **Encryption Suite** – Titkosító rendszer – Система шифрования – Verschlüsselungssystem
187. **Observation Post** – Megfigyelő állomás – Наблюдательный пункт – Beobachtungsposten
188. **Communication Relay** – Kommunikációs adó-vevő – Релейная связь – Kommunikationsrelais
189. **Secure Network** – Biztonságos hálózat – Защищенная сеть – Sichernetz
190. **Access Control** – Hozzáférés-ellenőrzés – Контроль доступа – Zugangskontrolle

BLOCK 20: STRATEGY & LONG-TERM PLANNING (191–200)

191. **Long-Range Planning** – Hosszú távú tervezés – Долгосрочное планирование – Langfristige Planung
192. **Scenario Analysis** – Forgatókönyv-elemzés – Сценарный анализ – Szenarioanalyse
193. **Strategic Forecast** – Stratégiai előrejelzés – Стратегический прогноз – Strategische Prognose
194. **Intelligence Cycle** – Hírszerzési ciklus – Цикл разведки – Nachrichtendienstlicher Zyklus
195. **Collection Plan** – Információgyűjtési terv – План сбора информации – Sammelplan
196. **Target Development** – Célpontfejlesztés – Разработка целей – Zielentwicklung
197. **Priority Intelligence Requirements (PIR)** – Prioritási hírszerzési követelmények – Приоритетные разведывательные требования – Prioritäre Geheimdienstanforderungen
198. **Decision Support Framework** – Döntéstámogatási keretrendszer – Рамки поддержки решений – Entscheidungsunterstützungsrahmen
199. **Risk Assessment Matrix** – Kockázatértékelési mátrix – Матрица оценки риска – Risikomatrix
200. **Intelligence Product** – Hírszerzési termék – Разведывательный продукт – Nachrichtendienstliches Produkt

INTELLIGENCE COMMUNITY VOCABULARY

ADVANCED OPERATIONS & STRATEGY (151–200)

BLOCK 16: INTERNATIONAL INTELLIGENCE (151–160)

151. **Allied Intelligence** – Szövetséges hírszerzés – Разведка союзников – Verbündete Aufklärung
Information shared between friendly nations.
152. **Coalition Operations** – Koalíciós műveletek – Операции коалиции – Koalitionsoperationen
Joint operations of multiple countries.
153. **Bilateral Agreement** – Kétoldalú megállapodás – Двустороннее соглашение – Bilaterales Abkommen
Formal intelligence-sharing treaty between two states.
154. **Multilateral Agreement** – Többoldalú megállapodás – Многостороннее соглашение – Multilaterales Abkommen
Intelligence-sharing among multiple parties.
155. **Intelligence Liaison** – Hírszerzési kapcsolattartó – Разведывательный связной – Nachrichtendienstlicher Verbindungsoffizier
Officer coordinating between agencies or nations.
156. **Foreign Intelligence** – Külföldi hírszerzés – Иностранная разведка – Auslandsaufklärung
Information gathering about foreign entities.
157. **Domestic Intelligence** – Belföldi hírszerzés – Внутренняя разведка – Inlandsaufklärung
Intelligence activities inside the home country.
158. **Covert Action** – Titkos művelet – Тайная операция – Geheimaktion
Secret activities intended to influence events abroad.
159. **Espionage** – Kémkedés – Шпионаж – Spionage
Obtaining information secretly.
160. **Counterespionage** – Ellenkémkedés – Контрразведка – Gegenspionage
Preventing foreign spying.

BLOCK 17: CYBER & DIGITAL OPERATIONS (161–170)

161. **Cybersecurity** – Kibervédelem – Кибербезопасность – Cybersicherheit
Protecting systems and data.

162. **Hacking** – Hacking – Взлом – Hacken
Unauthorized access to systems.

163. **Phishing** – Adathalászat – Фишинг – Phishing
Deceptive attempts to acquire sensitive data.

164. **Malware** – Kártevő szoftver – Вредоносное ПО – Schadsoftware
Software designed to damage or disrupt.

165. **Ransomware** – Zsarolóprogram – Вымогательское ПО – Ransomware
Malicious software demanding payment.

166. **Cyber Threat Actor** – Kiberveszélyforrás – Киберугрозы – Cyber-Bedrohungsakteur
Individual or group conducting cyber operations.

167. **Zero-Day Exploit** – Nulladik napi sebezhetőség – Эксплойт нулевого дня – Zero-Day-Exploit
Vulnerability unknown to the vendor.

168. **Encryption Key** – Titkosító kulcs – Ключ шифрования – Verschlüsselungsschlüssel
Code required to decode encrypted data.

169. **Firewall** – Tűzfal – Межсетевой экран – Firewall
System protecting networks from unauthorized access.

170. **Intrusion Detection** – Betörés-felismerés – Система обнаружения вторжений – Eindringungserkennung
Detecting unauthorized network access.

BLOCK 18: COUNTERMEASURES & DEFENSE (171–180)

171. **Physical Countermeasure** – Fizikai ellenintézkedés – Физические меры противодействия – Physische Gegenmaßnahme
Protecting personnel or assets physically.
172. **Technical Countermeasure** – Technikai ellenintézkedés – Технические меры – Technische Gegenmaßnahme
Using technology to prevent breaches.
173. **OPSEC Breach** – OPSEC-sértés – Нарушение OPSEC – OPSEC-Verletzung
Compromise of operational security.
174. **Red Team Exercise** – Red Team gyakorlat – Упражнение Красной команды – Red-Team-Übung
Simulated adversary to test defenses.
175. **Blue Team Exercise** – Blue Team gyakorlat – Упражнение Синей команды – Blue-Team-Übung
Defensive testing against simulated attacks.
176. **Penetration Test** – Penetrációs teszt – Тест на проникновение – Penetrationstest
Authorized test of system vulnerabilities.
177. **Threat Modeling** – Fenyegetés-modellezés – Моделирование угроз – Bedrohungsmodellierung
Predicting potential attack vectors.
178. **Security Audit** – Biztonsági audit – Аудит безопасности – Sicherheitsprüfung
Review of defenses and procedures.
179. **Incident Response** – Eseménykezelés – Реагирование на инциденты – Vorfallreaktion
Actions after a security breach.
180. **Crisis Management** – Válságkezelés – Управление кризисом – Krisenmanagement
Organized response to emergencies.

BLOCK 19: INTELLIGENCE INFRASTRUCTURE (181–190)

181. **Safe Communications** – Biztonságos kommunikáció – Безопасная связь – Sichere Kommunikation
182. **Secure Facilities** – Biztonságos létesítmények – Защищенные объекты – Sichere Einrichtungen
183. **Data Center** – Adatközpont – Центр обработки данных – Rechenzentrum
184. **Operations Center** – Műveleti központ – Оперативный центр – Operationszentrum
185. **Command Center** – Parancsnoki központ – Командный центр – Kommandostelle
186. **Encryption Suite** – Titkosító rendszer – Система шифрования – Verschlüsselungssystem
187. **Observation Post** – Megfigyelő állomás – Наблюдательный пункт – Beobachtungsposten
188. **Communication Relay** – Kommunikációs adó-vevő – Релейная связь – Kommunikationsrelais
189. **Secure Network** – Biztonságos hálózat – Защищенная сеть – Sichernetz
190. **Access Control** – Hozzáférés-ellenőrzés – Контроль доступа – Zugangskontrolle

BLOCK 20: STRATEGY & LONG-TERM PLANNING (191–200)

191. **Long-Range Planning** – Hosszú távú tervezés – Долгосрочное планирование – Langfristige Planung
192. **Scenario Analysis** – Forgatókönyv-elemzés – Сценарный анализ – Szenarioanalyse
193. **Strategic Forecast** – Stratégiai előrejelzés – Стратегический прогноз – Strategische Prognose
194. **Intelligence Cycle** – Hírszerzési ciklus – Цикл разведки – Nachrichtendienstlicher Zyklus
195. **Collection Plan** – Információgyűjtési terv – План сбора информации – Sammelplan
196. **Target Development** – Célpontfejlesztés – Разработка целей – Zielentwicklung
197. **Priority Intelligence Requirements (PIR)** – Prioritási hírszerzési követelmények – Приоритетные разведывательные требования – Prioritäre Geheimdienstanforderungen
198. **Decision Support Framework** – Döntéstámogatási keretrendszer – Рамки поддержки решений – Entscheidungsunterstützungsrahmen
199. **Risk Assessment Matrix** – Kockázatértékelési mátrix – Матрица оценки риска – Risikomatrix
200. **Intelligence Product** – Hírszerzési termék – Разведывательный продукт – Nachrichtendienstliches Produkt

INTELLIGENCE COMMUNITY VOCABULARY

ADVANCED CLANDESTINE & INFLUENCE OPERATIONS (201–300)

BLOCK 21: LEGAL & ETHICAL (201–210)

201. **Legislation** – Jogszabály – Закон – Gesetz
Legal framework governing intelligence activities.
202. **Policy** – Politika – Политика – Politik
Guiding principles for agency operations.
203. **Oversight Committee** – Felügyeleti bizottság – Комитет по надзору – Aufsichtskomitee
Body reviewing intelligence conduct.
204. **Accountability Mechanism** – Elszámoltathatósági mechanizmus – Механизм подотчетности – Rechenschaftsmechanismus
Structures ensuring responsibility.
205. **Civilian Control** – Polgári ellenőrzés – Гражданский контроль – Zivile Kontrolle
Government oversight of intelligence.
206. **Legal Authority** – Joghatóság – Юридическая власть – Rechtsbefugnis
Power granted by law.
207. **Privacy Protection** – Magánélet védelme – Защита частной жизни – Datenschutz
Safeguarding personal data.
208. **Ethics Review** – Etikai felülvizsgálat – Этический контроль – Ethikprüfung
Evaluation of moral considerations.
209. **Proportionality** – Arányosság – Соразмерность – Verhältnismäßigkeit
Actions must be proportionate to threat.
210. **Civil Rights** – Polgári jogok – Гражданские права – Bürgerrechte
Rights guaranteed to citizens.

BLOCK 22: CLANDESTINE TECHNIQUES (211–220)

211. **Dead Drop** – Halott postaláda – Тайник – Toter Briefkasten
Secret material exchange point.
212. **Brush Pass** – Gyors átadás – Быстрая передача – Kurzer Austausch
Quick transfer between agents.
213. **Cut-out** – Közvetítő – Посредник – Mittelsmann
Third party to protect source identity.
214. **Safehouse** – Biztonságos ház – Безопасное помещение – Safehouse
Secure operational base.
215. **Front Company** – Álcavállalat – Подставная компания – Tarnfirma
Business masking intelligence operations.
216. **Legend** – Légenda – Легенда – Legende
Fabricated identity for cover.
217. **Operational Compartment** – Műveleti szekció – Оперативный отсек – Operative Abteilung
Isolated operational segment.
218. **False Flag** – Álflag – Провокация под чужим флагом – Falsche Flagge
Operation disguised as another actor.
219. **Tradecraft** – Szakmai módszerek – Агентурная техника – Nachrichtendienstliche Praxis
Skills for espionage.
220. **Surveillance** – Megfigyelés – Наблюдение – Überwachung
Monitoring targets covertly.

BLOCK 23: POLITICAL & ECONOMIC INFLUENCE (221–230)

221. **Propaganda** – Propaganda – Пропаганда – Propaganda
Information used to influence opinion.

222. **Disinformation** – Dezinformáció – Дезинформация – Desinformation
Deliberate false information.

223. **Information Operation** – Információs művelet – Информационная операция – Informationsoperation
Coordinated influence campaign.

224. **Soft Power** – Puha hatalom – Мягкая сила – Weiche Macht
Influence via attraction, not force.

225. **Strategic Communication** – Stratégiai kommunikáció – Стратегическая коммуникация – Strategische Kommunikation
Planned messaging to achieve policy goals.

226. **Economic Intelligence** – Gazdasági hírszerzés – Экономическая разведка – Wirtschaftsspionage
Information on markets, trade, and industry.

227. **Sanctions Analysis** – Szankcióelemzés – Анализ санкций – Sanktionsanalyse
Evaluating impact of economic measures.

228. **Influence Campaign** – Befolyásolási kampány – Кампания по влиянию – Einflusskampagne
Targeted effort to shape opinions.

229. **Narrative Management** – Narratíva kezelése – Управление нарративом – Narrativsteuerung
Shaping public perception.

230. **Public Diplomacy** – Nyilvános diplomácia – Публичная дипломатия – Öffentliche Diplomatie
Government messaging abroad to influence audiences.

BLOCK 24: INTELLIGENCE CYCLE CONTINUED (231–240)

231. **Planning and Direction** – Tervezés és irányítás – Планирование и руководство – Planung und Steuerung
Setting priorities and guidance.
232. **Collection Management** – Információgyűjtés menedzsment – Управление сбором данных – Sammlungskontrolle
Overseeing information collection.
233. **Processing** – Feldolgozás – Обработка – Verarbeitung
Converting raw data into usable form.
234. **Analysis & Production** – Elemzés és termelés – Анализ и производство – Analyse und Erstellung
Turning information into intelligence.
235. **Dissemination** – Terjesztés – Распространение – Verbreitung
Sharing intelligence with stakeholders.
236. **Feedback** – Visszajelzés – Обратная связь – Rückmeldung
Information on usefulness and accuracy.
237. **Requirements Development** – Követelményfejlesztés – Разработка требований – Anforderungsentwicklung
Determining information needed.
238. **Collection Requirements** – Gyűjtési követelmények – Требования к сбору – Sammelanweisungen
Specific questions for collection.
239. **Priority Intelligence Requirements (PIR)** – Prioritási hírszerzési követelmények – Приоритетные разведывательные требования – Prioritäre Geheimdienstanforderungen
High-priority information needed by decision-makers.
240. **Essential Elements of Information (EEI)** – Alapvető információs elemek – Основные элементы информации – Wesentliche Informationselemente
Critical data points for analysis.

BLOCK 25: LOGISTICS & INFRASTRUCTURE (241–250)

241. **Operational Base** – Műveleti bázis – Оперативная база – Operationsbasis
Hub supporting missions.
242. **Forward Operating Location (FOL)** – Előretolt műveleti hely – Передовая база – Vorwärtsoperationsstandort
Temporary or semi-permanent mission site.
243. **Supply Chain** – Ellátási lánc – Цепочка поставок – Lieferkette
Flow of resources to support operations.
244. **Transport Network** – Szállítási hálózat – Транспортная сеть – Transportnetzwerk
Logistics infrastructure.
245. **Secure Communications** – Biztonságos kommunikáció – Защищенная связь – Sichere Kommunikation
Encrypted messaging for operations.
246. **Data Center** – Adatközpont – Центр обработки данных – Rechenzentrum
Facility hosting information systems.
247. **Redundancy** – Tartalék – Резервирование – Redundanz
Backup systems to ensure continuity.
248. **Contingency Resource** – Vészhelyzeti erőforrás – Резервный ресурс – Notfallressource
Resources for emergencies.
249. **Asset Tracking** – Eszközkövetés – Отслеживание активов – Asset-Tracking
Monitoring material and personnel.
250. **Maintenance Protocol** – Karbantartási protokoll – Протокол обслуживания – Wartungsprotokoll
Guidelines for upkeep.

BLOCK 26: EMERGING TECHNOLOGIES (251–260)

251. **Artificial Intelligence (AI)** – Mesterséges intelligencia – Искусственный интеллект – Künstliche Intelligenz
252. **Machine Learning** – Gépi tanulás – Машинное обучение – Maschinelles Lernen
253. **Predictive Analytics** – Prediktív analitika – Предиктивная аналитика – Predictive Analytics
254. **Big Data** – Nagy adatok – Большие данные – Big Data
255. **Data Mining** – Adatbányászat – Добыча данных – Datenanalyse
256. **Algorithm** – Algoritmus – Алгоритм – Algorithmus
257. **Cyber Threat Intelligence (CTI)** – Kiberveszély-hírszerzés – Разведка киберугроз – Cyber Threat Intelligence
258. **Network Mapping** – Hálózati feltérképezés – Картирование сети – Netzwerk-Mapping
259. **Quantum Computing** – Kvantumszámítás – Квантовые вычисления – Quantencomputing
260. **Blockchain Analysis** – Blokklánc-elemzés – Анализ блокчейна – Blockchain-Analyse

INTELLIGENCE COMMUNITY VOCABULARY

STRATEGIC, FINANCE & CRISIS OPERATIONS (261–300)

BLOCK 27: STRATEGIC RESERVES & INFRASTRUCTURE (261–270)

261. **Strategic Reserve** – Stratégiai tartalék – Стратегический резерв – Strategische Reserve
Stockpiles to mitigate crises.
262. **Energy Security** – Energiabiztonság – Энергобезопасность – Energiesicherheit
Ensuring reliable energy supply.
263. **Food Security** – Élelmiszerbiztonság – Продовольственная безопасность – Ernährungssicherheit
Reliable access to sufficient food.
264. **Water Security** – Vízügyi biztonság – Водная безопасность – Wassersicherheit
Access to safe water supplies.
265. **Critical Infrastructure Protection** – Kritikus infrastruktúra védelme – Защита критической инфраструктуры – Schutz kritischer Infrastruktur
Safeguarding essential services.
266. **Logistics Support** – Logisztikai támogatás – Логистическая поддержка – Logistische Unterstützung
Material and personnel movement for operations.
267. **Resilience Planning** – Ellenállóképesség tervezés – Планирование устойчивости – Resilienzplanung
Preparation for recovery from disruption.
268. **Redundancy Systems** – Tartalék rendszerek – Резервные системы – Redundanzsysteme
Backup systems to maintain continuity.
269. **Infrastructure Risk Assessment** – Infrastruktúra kockázatértékelés – Оценка рисков инфраструктуры – Infrastruktur-Risikobewertung
Identifying vulnerabilities in critical assets.
270. **Continuity of Operations (COOP)** – Működés folytonossága – Непрерывность операций – Kontinuität der Operationen
Ensuring operations continue under disruption.

BLOCK 28: FINANCIAL & ECONOMIC INTELLIGENCE (271–280)

271. **Budget Analysis** – Költségvetés-elemzés – Анализ бюджета – Haushaltsanalyse
Reviewing expenditure trends.
272. **Financial Intelligence (FININT)** – Pénzügyi hírszerzés – Финансовая разведка – Finanzielle Aufklärung
Information on economic and financial activities.
273. **Sanctions Compliance** – Szankció-megfelelés – Соблюдение санкций – Sanktionskonformität
Adhering to imposed sanctions.
274. **Trade Monitoring** – Kereskedelem figyelés – Мониторинг торговли – Handelsüberwachung
Tracking imports, exports, and strategic goods.
275. **Money Laundering Detection** – Pénzmosás-felismerés – Выявление отмывания денег – Geldwäsche-Erkennung
Identifying illicit financial activity.
276. **Economic Forecasting** – Gazdasági előrejelzés – Экономический прогноз – Wirtschaftsprognose
Predicting market trends and stability.
277. **Resource Allocation** – Erőforrás-elosztás – Распределение ресурсов – Ressourcenverteilung
Distributing funds or material effectively.
278. **Asset Protection** – Eszközvédelem – Защита активов – Vermögensschutz
Securing financial and physical assets.
279. **Funding Oversight** – Finanszírozási felügyelet – Надзор за финансированием – Finanzaufsicht
Monitoring use of resources.
280. **Investment Risk Assessment** – Befektetési kockázatértékelés – Оценка инвестиционных рисков – Investitionsrisikobewertung
Evaluating financial opportunities and threats.

BLOCK 29: CRISIS & EMERGENCY OPERATIONS (281–290)

281. **Crisis Response** – Válságkezelés – Реагирование на кризис – Krisenreaktion
Actions taken during emergencies.
282. **Emergency Preparedness** – Vészhelyzeti előkészületek – Готовность к чрезвычайным ситуациям – Notfallvorsorge
Planning for disasters.
283. **Incident Command System (ICS)** – Eseményirányítási rendszer – Система командования инцидентами – Incident-Command-System
Structure for managing crises.
284. **Evacuation Plan** – Kiürítési terv – План эвакуации – Evakuierungsplan
Organized exit from danger zones.
285. **Continuity of Government (COG)** – Kormányzati folytonosság – Непрерывность деятельности правительства – Kontinuität der Regierung
Maintaining government functions under crisis.
286. **Risk Mitigation Plan** – Kockázatcsökkentési terv – План по снижению рисков – Risikominderungsplan
Reducing likelihood or impact of threats.
287. **Emergency Operations Center (EOC)** – Vészhelyzeti műveleti központ – Центр чрезвычайных операций – Notfalloperationszentrum
Command hub for emergencies.
288. **Disaster Recovery** – Katasztrófa utáni helyreállítás – Восстановление после катастрофы – Katastrophenwiederherstellung
Restoring systems and services.
289. **Continuity Planning** – Folytonossági tervezés – Планирование непрерывности – Kontinuitätsplanung
Ensuring uninterrupted operations.
290. **Operational Resilience** – Műveleti ellenállóképesség – Оперативная устойчивость – Operative Resilienz
Capacity to absorb and adapt to shocks.

BLOCK 30: INFORMATION INFLUENCE & MEDIA (291–300)

291. **Media Analysis** – Médiaelemzés – Медиаанализ – Medienanalyse
Studying public and social media trends.
292. **Public Perception** – Nyilvános észlelés – Общественное восприятие – Öffentliche Wahrnehmung
How people view events or entities.
293. **Influence Metrics** – Befolyás-mutatók – Метрики влияния – Einflussmetriken
Measures of impact on audiences.
294. **Information Warfare** – Információs hadviselés – Информационная война – Informationskrieg
Manipulation of information to achieve objectives.
295. **Psychological Operations (PSYOPS)** – Pszichológiai műveletek – Психологические операции – Psychologische Operationen
Operations targeting morale or decision-making.
296. **Perception Management** – Észlelésirányítás – Управление восприятием – Wahrnehmungssteuerung
Controlling narratives and viewpoints.
297. **Social Media Monitoring** – Közösségi média megfigyelés – Мониторинг социальных медиа – Social-Media-Überwachung
Tracking trends online.
298. **Cyber Influence** – Kibermédia befolyás – Кибервлияние – Cyber-Einfluss
Online influence campaigns.
299. **Disinformation Campaign** – Dezinformációs kampány – Кампания по дезинформации – Desinformationskampagne
Coordinated spread of false information.
300. **Narrative Control** – Narratíva-irányítás – Контроль нарратива – Narrativkontrolle
Management of storytelling for strategic goals.

INTELLIGENCE COMMUNITY GLOSSARY (ALPHABETICAL, 1–300)

Access Control – System controlling who can access facilities or information.
Accountability – Ensuring individuals and agencies are responsible for actions.
Accountability Mechanism – Structures ensuring responsibility.
All-Source Analysis – Combining all intelligence sources for insight.
Alarm / Alert – Notification of potential threat or critical event.
Algorithm – Step-by-step procedure for processing data.
Analysis – Interpretation of collected information.
Analysis & Production – Turning information into intelligence products.
Artificial Intelligence (AI) – Machine-based intelligence and decision-making systems.
Assessment – Judgment of significance or risk.
Asset – Controlled or trusted source of information.
Asset Compromise – Loss of control over a source.
Asset Tracking – Monitoring material or personnel.
Automation – Using machines to perform processes automatically.
Bilateral Agreement – Intelligence-sharing agreement between two states.
Blue Team – Defensive or internal group.
Blue Team Exercise – Defensive simulation against attacks.
Budget Analysis – Reviewing expenditure trends.
Brush Pass – Quick exchange of material between agents.
Capability – What an actor can realistically do.
Crisis Response – Actions taken during an emergency.
Crisis Management – Organized response to emergencies.
Cyber Influence – Online influence campaigns.
Cyber Intelligence – Information collected from digital networks.
Cyber Threat Actor – Individual or group conducting cyber operations.
Cyber Threat Intelligence (CTI) – Intelligence on cyber threats.
Classification – Level of secrecy assigned to information.
Clandestine – Hidden operations with no attribution.
Coalition Operations – Joint operations of multiple nations.
Collection – Acquisition of raw information.
Collection Management – Overseeing intelligence collection.
Collection Plan – Plan for acquiring specific intelligence.
Collection Requirements – Specific information requested by analysts.
Compartmentation – Limiting access to sensitive information.
Compromise – Loss of security or credibility.
Continuity Planning – Ensuring uninterrupted operations.
Continuity of Government (COG) – Maintaining government functions in crisis.
Continuity of Operations (COOP) – Ensuring ongoing agency operations.
Contingency Plan – Plan for unexpected situations.
Contingency Resource – Resource reserved for emergencies.

Coordination – Organized interaction between agencies.
Covert – Hidden but deniable operations.
Critical Infrastructure – Essential services and facilities.
Critical Infrastructure Protection – Safeguarding essential services.
Cybersecurity – Protecting systems and data from attacks.
Cut-out – Intermediary protecting identities.
Data Center – Facility hosting information systems.
Data Mining – Extracting useful information from datasets.
Dead Drop – Secret material exchange point.
Decision Support – Intelligence supporting policy decisions.
Decision Support Framework – Structure guiding intelligence advice.
Deception – Misleading a target.
Decryption – Converting encrypted information into readable form.
Defector – Person leaving one side for another.
Disaster Recovery – Restoring systems after a catastrophe.
Dissemination – Sharing intelligence with authorized users.
Disinformation – Deliberate false information.
Disinformation Campaign – Coordinated spreading of false information.
Economic Forecasting – Predicting economic trends.
Economic Intelligence – Information on markets and trade.
Economic Warfare – Using economic means to achieve strategic goals.
Encryption – Encoding information to prevent unauthorized access.
Encryption Key – Code needed to decrypt encrypted data.
Energy Security – Ensuring reliable energy supply.
Essential Elements of Information (EEI) – Critical data points for intelligence.
Ethics – Moral principles guiding intelligence activities.
Ethics Review – Evaluation of moral considerations.
Exfiltration – Removing personnel or data from a location.
Evacuation Plan – Organized exit from danger zones.
Expert – Subject-matter specialist.
False Flag – Operation disguised as conducted by another actor.
Feedback – Information on usefulness and accuracy.
Financial Intelligence (FININT) – Intelligence on financial activities.
Financial Risk Assessment – Evaluating potential financial threats.
Firewall – System protecting networks from unauthorized access.
Force Protection – Safeguarding personnel and resources.
Forward Operating Location (FOL) – Temporary mission site.
Forecasting – Predicting future events or trends.
Front Company – Business masking intelligence operations.
Funding Oversight – Monitoring use of resources.
Geospatial Analysis – Studying location-based data.
Hazard / Risk – Potential for harm or loss.
Human Intelligence (HUMINT) – Information from human sources.
Human Rights – Rights guaranteed to individuals.
Hacking – Unauthorized access to systems.
Handler – Officer managing an asset.
Incident Command System (ICS) – Structured crisis management.
Incident Response – Actions after security breaches.

Industrial Capacity – Nation’s ability to produce goods.
Influence – Ability to shape decisions or perceptions.
Influence Campaign – Targeted effort to shape opinion.
Information Operations – Coordinated influence actions.
Information Security – Protecting information integrity and confidentiality.
Information Warfare – Manipulation of information for strategic goals.
Insider Threat – Risk from internal personnel.
Intelligence – Processed information supporting decision-making.
Intelligence Cycle – Sequence of planning, collection, analysis, dissemination.
Intelligence Liaison – Officer coordinating between agencies or nations.
Intelligence Product – Analysis or report produced from intelligence.
Intent – Planned action or goal of an actor.
Interagency – Cooperation between multiple agencies.
Investment Risk Assessment – Evaluating potential financial opportunities.
Jurisdiction – Legal authority over an area or operation.
Key Performance Indicator (KPI) – Measure of operational success.
Knowledge Management – Organizing intelligence for access and use.
Legal Authority – Power granted by law.
Legislation – Legal framework governing operations.
Legend – Fabricated identity for cover.
Leak – Unauthorized disclosure of information.
Link Analysis – Mapping relationships between entities.
Linkage Modeling – Predictive mapping of relationships.
Long-Range Planning – Planning over an extended period.
Machine Learning – AI techniques for pattern recognition and predictions.
Malware – Software designed to damage systems.
Map / Chart – Visual representation of spatial data.
Media Analysis – Studying trends in media coverage.
Media Monitoring – Tracking media activity for intelligence purposes.
Media Reporting – Public dissemination of information.
Media Strategy – Planning messaging and communications.
Mission Planning – Organizing tasks for an operation.
Mitigation – Reducing severity or risk.
Money Laundering Detection – Identifying illicit financial activity.
Multilateral Agreement – Intelligence-sharing among multiple parties.
Narrative – Storyline shaping perception.
Narrative Control – Managing strategic storytelling.
Narrative Management – Shaping public perception intentionally.
Need-to-Know Principle – Access only if necessary.
Network Mapping – Analyzing connections in a system.
Operational Base – Hub supporting missions.
Operational Design – Structuring operations to achieve objectives.
Operational Resilience – Ability to absorb shocks and adapt.
Operational Risk – Potential for operational failure or harm.
Operations Center – Command hub for intelligence operations.
Operations Security (OPSEC) – Preventing operational information leaks.
Oversight – Supervision ensuring lawful and ethical conduct.
Pattern Recognition – Identifying recurring trends or behaviors.

Penetration Test – Authorized testing of security systems.
Perception Management – Controlling how information is interpreted.
Physical Countermeasure – Protecting people or assets physically.
Physical Security – Protection of personnel, facilities, and materials.
Planning and Direction – Setting priorities and operational guidance.
Plausible Deniability – Ability to deny involvement convincingly.
Predictive Analytics – Using data to forecast outcomes.
Predictive Systems – Systems forecasting future scenarios.
Priority Intelligence Requirements (PIR) – High-priority intelligence needs.
Privacy – Protection of personal information.
Propaganda – Information used to influence opinion.
Proportionality – Ensuring actions match threats.
Public Diplomacy – Messaging abroad to influence audiences.
Public Perception – How the public interprets events.
Red Team – Adversarial group simulating threats.
Red Team Exercise – Simulation of attacks to test defenses.
Redundancy – Backup systems to maintain continuity.
Redundancy Systems – Systems providing backups in operations.
Recruitment – Enlisting an asset for intelligence purposes.
Reliability – Trustworthiness of sources or information.
Remote Sensing – Collecting data from a distance.
Resource Allocation – Distribution of funds or material.
Resilience – Ability to recover from disruption.
Resilience Planning – Planning to maintain function under stress.
Rules of Engagement – Guidelines for conduct in operations.
Safe Communications – Encrypted or protected communication channels.
Safehouse – Secure location for operations or refuge.
Sanctions – Economic or political penalties.
Sanctions Analysis – Evaluating impact of sanctions.
Scenario Analysis – Studying possible future situations.
Scenario Planning – Modeling alternative futures.
Scenario Simulation – Simulating potential outcomes.
Secure Facilities – Protected operational sites.
Secure Network – Protected data and communication network.
Security Audit – Reviewing security procedures and systems.
Security Clearance – Authorization to access classified information.
Signal vs Noise – Differentiating relevant from irrelevant data.
Signal Jamming – Disrupting electronic communication.
Signals Intelligence (SIGINT) – Intelligence from intercepted signals.
Social Media Monitoring – Tracking trends online.
Soft Power – Influence through attraction and diplomacy.
Source – Origin of information.
Strategic Communication – Planned messaging to achieve objectives.
Strategic Forecast – Long-term intelligence projection.
Strategic Intelligence – National-level long-term insights.
Strategic Reserve – Stockpiles for crisis mitigation.
Surveillance – Monitoring targets.
Surveillance Detection – Detecting being monitored.

Systems Risk – Vulnerabilities in integrated systems.
Target Development – Identifying targets for intelligence operations.
Targeting – Selecting objectives for operations.
Telemetry Interception – Capturing sensor data remotely.
Threat – Potential source of harm.
Threat Assessment – Evaluating probability and severity of threats.
Threat Modeling – Predicting potential attack vectors.
Tactical Intelligence – Immediate, operational-level intelligence.
Telecommunications Interception – Capturing signals communications.
Transport Network – Infrastructure moving personnel or material.
Trend Analysis – Identifying patterns over time.
Trustworthiness – Reliability of source or information.
Vulnerability Assessment – Identifying weaknesses.
Water Security – Ensuring safe and sufficient water.
Weapons Intelligence – Information on armaments or military tech.
Workflow / Process Mapping – Structuring operational processes.
Yellow Team / Advisory Team – Support or evaluation team.
Zero-Day Exploit – Vulnerability unknown to the vendor.