

<https://doi.org/10.70265/IVEB3293>

**ЕВОЛЮЦИЯ НА ВОЕННОТО РАЗУЗНАВАНЕ ПОД
ВЪЗДЕЙСТВИЕТО НА ТЕХНИЧЕСКИЯ ПРОГРЕС:
АНАЛИЗ НА МЕТОДИТЕ И ФОРМИТЕ ЗА
ПРИДОБИВАНЕ НА РАЗУЗНАВАТЕЛНА
ИНФОРМАЦИЯ**

Огнян Костадинов

**EVOLUTION OF MILITARY INTELLIGENCE UNDER
THE INFLUENCE OF TECHNOLOGICAL PROGRESS:
ANALYSIS OF METHODS AND FORMS OF
INTELLIGENCE GATHERING**

Ognyan Kostadinov

***Резюме:** Военното разузнаване добива информация и изготвя аналитична оценка чрез съчетание на конспиративни практики и научно-технически прогрес. Разкриването на намеренията и способностите на противника служи за ранно предупреждение и вземане на решения в интерес на сигурността. Анализирани са основните форми за събиране на информация: чрез човешки източници (HUMINT), технически средства (SIGINT, IMINT/GEOINT, MASINT) и открити източници (OSINT).*

***Ключови думи:** OSINT, HUMINT, SIGINT, IMINT/GEOINT, MASINT*

***Abstract:** Military intelligence acquires information and produces analytical assessments through a combination of clandestine practices and scientific and technological progress. Revealing the intentions and capabilities of an adversary serves early warning and decision-making in the interest of security. The main forms of intelligence collection are analyzed: human sources (HUMINT), technical means (SIGINT, IMINT/GEOINT, MASINT), and open sources (OSINT).*

***Keywords:** OSINT, HUMINT, SIGINT, IMINT/GEOINT, MASINT*

УВОД

Разузнаването се използва в различни сфери на обществения живот, но в междудържавните отношения има особено важно значение

като средство за защита на националната сигурност и отбраната. В този смисъл то представлява форма на противоборство, осъществявана главно чрез прикрити способности, конспиративни дейности и технически средства.

Исторически разузнаването може да се проследи още при пра човека – в поведението му при борбата за оцеляване, лова и съперничеството за поминък. Наблюдението, разпознаването на заплахи и възможности, изборът на подходящ момент за действие и използването на хитрост са елементарни форми на събиране и използване на информация за постигане на превъзходство. В този смисъл разузнаването е функционално проявление на човешкия бит и част от живота: човекът намалява неизвестността чрез сведения, тълкуване и предвиждане. Подобни модели се наблюдават и в животинския свят: търсене и ориентиране, наблюдение и откриване на възможност, преследване и действие за оцеляване чрез осигуряване на храна. При човека тези първични модели на наблюдение, преценка и действие по-късно прерастват в съзнателна дейност по събиране и използване на сведения срещу противника.

За ранни организирани форми на разузнаване има сведения и в Библията. Един от примерите е описанието как Исус Навин „изпрати от Ситим двама мъже да съгледват тайно ... Ерихон“ (Исус Навин 2:1; Библия, 1982а, ред 1). Двамата намират укритие при жена на име Раав; властите узнават за присъствието им, но не успяват да ги заловят (Исус Навин 2; Библия, 1982а, ред 2-3). Този сюжет съдържа класически елементи на проникване, прикритие и използване на местен сътрудник във враждебна среда.

Подобен пример е и изпращането на дванадесет съгледвачи от Моисей в земята Ханаан (Числа 13–14; Библия, 1982b). По Божия заповед Моисей „Изпрати мъже, за да съгледат Ханаанската земя.... по един мъж от всяко племе...“ (Числа 13; Библия, 1982b, ред 2). Поставената задача е с ясно изразен разузнавателен характер и включва събиране на сведения за природните условия, населените места, силата на местните народи, укрепленията и плодородието на земята (Числа 13–14; Библия, 1982b, ред 17-24). В съвременни условия това се доближава до стратегическо разузнаване, включващо оценка на територията, човешките ресурси и икономическия потенциал преди евентуално въоръжено нападение.

Още в древността разузнаването се разглежда като ключов елемент на военното изкуство. В трактата „Изкуството на войната“ Сун Дзъ подчертава, че „шпионажът е същностен във война – чрез него именно се определя всеки ход“ (Сун Дзъ, 2023, с. 109). Тази ранна концепция поставя акцент върху предварителната осведоменост, човешките

източници и стратегическото значение на информацията за постигане на превъзходство над противника.

През Ренесанса разузнаването постепенно придобива институционализирани форми. Според Ioanna Iordanou Венецианската република създава *„една от най-ранните в света централно организирани държавни разузнавателни служби“* (Iordanou, 2019, p. 41), основана на систематизирано събиране, анализ и защита на чувствителна информация. Това бележи прехода от епизодични разузнавателни практики към организирани държавни структури за сигурност и стратегическо управление на информацията

Основните задачи на съвременните военни разузнавания са добиването и анализът на чувствителна чуждестранна информация, важна за сигурността на държавата и за защитата на въоръжените сили – намерения, способности и потенциални заплахи от потенциалния противник. В официалното описание на задачите на уебсайта на Служба „Военно разузнаване“ е посочено като задачи: *„добиване и анализ на стратегическа разузнавателна информация, необходима за отбраната на страната и защитата на националната сигурност от външни посегателства, рискове и заплахи;“* (Служба „Военно разузнаване“, n.d.).

Изследването разглежда три форми на разузнавателна дейност:

- **Разузнаване чрез човешки източници (HUMINT)** – добиване и проверка на разузнавателна информация чрез хора (агенти, информатори, доверителни контакти), включително чрез конспиративни способности и контролирани комуникации; резултатът се оформя като сведения и оценъчни изводи, които подпомагат планирането и вземането на решения. (Лазаров, 2012, с. 101–104; Лазаров, Гюров, 2012, с. 202 – 210)

- **Разузнаване чрез технически средства (PTC – вкл. SIGINT, IMINT/GEOINT, MASINT)** – обединява дисциплини за добив и анализ на разузнавателна информация чрез технически средства и сензори, независимо от използваната платформа-носител, основани на: (1) комуникации и електромагнитни излъчвания; (2) изображения и геопространствени данни; и (3) измерими физични „сигнатури“ (подписи) на обекти и процеси (Arbus, 2025). В рамките на PTC ключови направления според U.S. Naval War College са: **Signals Intelligence (SIGINT)** – прихващане, локализиране и анализ на сигнали и електромагнитни излъчвания, включително комуникационни и некомуникационни; **Imagery Intelligence / Geospatial Intelligence (IMINT/GEOINT)** – добив и интерпретация на информация от

въздушни, спътникови и други изображения и последващ геопропространствен анализ; и **Measurement and Signature Intelligence (MASINT)** – разузнаване по измервания и сигнатури, насочено към откриване, локализиране, проследяване и идентифициране на цели чрез техните специфични измерими характеристики (U.S. Naval War College). Според U.S. Army MASINT е технически производна разузнавателна информация, която открива, локализира, проследява, идентифицира и/или описва специфични характеристики на цели (U.S. Army, 2004, Chapter 9, para. 9-1). Важна особеност е, че MASINT включва и разширена обработка и използване на данни, получени по линии на IMINT и SIGINT (U.S. Army, 2004, Chapter 9, para. 9-2, 9-3, 9-4). На практическо ниво MASINT използва спектър от сензори – например радарни, електрооптични/инфрачервени, спектрометрични, акустични и радиочестотни, както и ядрено-радиационни и сеизмични средства и техники за събиране на **CBRN**¹-релевантни материални проби. Както посочва U.S. Army, системите за събиране на MASINT включват „... акустични, RF², ядрено-детекционни и сеизмични сензори...“ (U.S. Army, 2004). Поради това MASINT има пряка приложимост и за откриване и характеризиране на ядрени събития чрез комбиниране на сеизмични, хидроакустични, инфразвукови и радионуклидни данни в глобални мониторингови мрежи. „*CTBTO: Международната мониторингова система включва сеизмични, хидроакустични, инфразвукови и радионуклидни станции.*“ (CTBTO, n.d.)

• **Разузнаване от открити източници (OSINT)** – добиване и анализ на информация с легитимни средства от публични медии, академични и институционални публикации, бази данни и дигитални източници. Критичен етап е верификацията и оценката на надеждността на източниците, за да се ограничат дезинформацията и манипулациите (Yotova, 2024, pp. 305–311; Gill, 2023).

За целите на анализа се въвежда авторски оперативен модел – „*движение – наблюдение – комуникация – анализ*“ – за описание на добива и анализа на информация в рамките на конкретна ситуация. В най-елементарния си вид той отразява човешкия модел на разузнаване: субектът се придвижва, наблюдава, съобщава установеното и

¹ CBRN (Chemical, Biological, Radiological, Nuclear) – химическо, биологично, радиологично и ядрено

² RF (Radio Frequency) – радиочестотен/радиочестотни.

анализира полученото, за да намали неопределеността и да подпомогне вземането на решение.

- **Движение**

Движението е „логистиката“ на разузнаването: достъп до хора, обекти и ситуации и управление на риска. В технически план то включва маневреност на разузнавателни средства и платформи и бързо разгръщане или преместване на сензори и станции.

- **Наблюдение**

Наблюдението се извършва от хора и чрез технически средства. То включва забелязване на важното, откриване на повтарящи се признаци и отклонения, проверка на детайлите и преценка на тяхното значение според обстановката. При техническото наблюдение са важни изборът на начин на засичане и познаването на ограниченията на използваните средства.

- **Комуникация**

Комуникацията е критична, защото човекът може да бъде едновременно източник, канал и филтър. Тя включва отношенията между разузнавателния офицер и агента-информатор, основани на доверие, мотивация и манипулация, както и техническите аспекти на разузнавателните средства – обхват, устойчивост на връзките и криптиране.

- **Анализ**

Анализът превръща информацията в оценка, която подпомага вземането на решение в условия на неяснота. Той включва проверка на източника и съдържанието, отделяне на фактите от тълкуванията, откриване на противоречия и липсващи данни и преценка на вероятните намерения и действия. В цифрова среда анализът включва и работа с големи масиви от данни и алгоритми/AI, без да отпада значението на човешката преценка.

Ключови преломи в развитието на военното разузнаване са: *двигателят с вътрешно горене; развитието на оптиката, геодезията и картографията; въздушните платформи и фотографията; радиовръзките, прихващането на съобщения, дешифрирането и последващата цифровизация, както и спътниковите канали; радиолокацията и акустичните средства; космическите системи; безпилотните летателни и плавателни средства; мрежовата дигитализация, киберинструментите, електронната борба, машинната обработка на данни и изкуственият интелект.*

Общият извод е, че устойчивият оперативен модел „**движение – наблюдение – комуникация – анализ**“ се запазва, докато средствата и методите се променят и повишават ефективността на добива, верификацията и оценката на информацията.

Настоящото изследване анализира формите и методите за придобиване и оценка на стратегическа разузнавателна информация относно военните способности, инфраструктурата и системите за управление на потенциалния противник в условията на съвременния технически прогрес и свързаните с него еволюционни процеси.

1. ЕТАПИ В РАЗВИТИЕТО НА ВОЕННОТО РАЗУЗНАВАНЕ

Развитието на съвременното военно разузнаване може да се проследи като поредица от етапи, започнали с въвеждането на нови технически средства и от разширяването на възможностите по веригата **TCPED/ISR**³. В литературата се подчертава значението на платформите по суша, море, въздух и в космоса, на различните сензори, комуникационните мрежи и средствата за обработка, използване и анализ на данни, включително автоматизирани решения (Henry, 2017; Kimmons & Gilmer, 2017, pp. 3–5). Това съответства на разбирането за **C4ISR**⁴ като мрежово интегрирана и **service-oriented** система, която свързва разузнавателно-добивните, командно-управленските и оръжейните системи в обща мрежа, така че участниците да изграждат споделена картина на обстановката и да обменят своевременно оперативната информация (Wang & Cao, 2020, p. 55).

1.1. Ранна „индустриално-комуникационна“ фаза (края на XIX в. – Първата световна война)

Първият голям технологичен прелом е свързан с преминаването от конска към двигателна тяга в транспорта на военна техника. Двигателят с вътрешно горене има особено важно значение, защото повишава подвижността и автономията на разузнавателните формирования, и позволява „да придвижва хора и предмети на големи разстояния с повишени скорости, освободено от ограниченията на железопътните линии“ (Horowitz & Resnick Samotin, 2025, p. 15, lines 1–3).

Успоредно с това ранните радио- и безжични връзки поставят началото на далечните комуникации извън кабелната мрежа. Както пише Bigelow: „Първият човек, който изпраща съобщение през въздуха без проводници, е сър Томас Прийс, през 1885 г.“ (Bigelow, 1951, para. 1).

Съществена роля имат и геодезията, топографските заснемания и прецизната оптика. Stefanova подчертава, че „точните геодезически данни са от решаващо значение за навигацията и ориентацията на

³ TCPED/ISR = Tasking, Collection/Capture, Processing, Exploitation, Dissemination / Intelligence, Surveillance, Reconnaissance — информационният цикъл на разузнаването, наблюдението и разпознаването (Henry, 2017, pp. 1–2).

⁴ ISR = „събирам и доставям разузнавателна информация“ / C4ISR = „събирам + предавам + обработвам + разпределям + използвам в командването и управлението“ (интегрирана система/мрежа).

военните сили, тъй като без надеждни карти войниците и превозните средства лесно могат да се изгубят или да попаднат в опасни райони“ (Stefanova, 2025, p. 217). Според *Report on Survey on the Western Front 1914–1918* полевите топографски заснемания „като общо правило“ са извършвани с „призматичен компас“, а понякога и с „мензула“ (Geographical Section, General Staff, War Office, 1920, p. 20, lines: 4-5). В този период далекомерите вече се утвърждават като важно средство за наблюдение и целеуказване. Russell отбелязва, че „до 1914 г. на всеки британски боен и линеен крайцер са били използвани до девет такива уреда“ (Russell, 2001, p. 2, lines 3-7).

1.2. Въздушно-наблюдателна и фотограметрична фаза (Първата световна война – междувоенен период)

Втората фаза се характеризира с превръщането на въздушното пространство в основна среда за разузнаване. Развитието преминава от използването на балони за корекция на артилерийския огън към специализирани витлови самолети, които превръщат въздушното наблюдение и фоторазузнаването в системна практика. Ключова роля има камерата – ускореното развитие на фото- и оптичните средства утвърждава авиационната фотография като важно средство за разузнаване и картографиране. (Quagliati, N., 2020, pp. 96). В този контекст се налага „фотointерпретацията“ (*photointerpretation*) като метод за аналитично разчитане и извличане на информация от аерофотографски изображения (Campbell, 2008, pp 77).

Паралелно с това се развиват и полевите комуникации чрез телеграф, телефон и безжични средства. Както отбелязва Bruton, „към края на войната пилотите са били оборудвани с радиотелефония и са могли да комуникират на къси разстояния с други самолети и на по-големи разстояния с наземни безжични станции“ (Bruton, 2014, p. 2, lines 9–14). Въпреки че това улеснява командването, то създава и нов риск, защото радиопредаванията могат лесно да бъдат прихващани. Tworek подчертава тази уязвимост, като посочва, че армиите са търсели сигурни средства за свързка, а „безжичната връзка е можела лесно да бъде прихващана“ (Tworek, 2014, p. 2, lines 1–3 of the section “Wireless on the Battlefield”). Това формира предпоставките за утвърждаването на COMINT⁵ като важен елемент на SIGINT.

1.3. Радиолокационно-електронна и криптологична фаза (Втората световна война)

Втората световна война бележи голям технологичен скок, при който радиолокацията се утвърждава като основа на ранното предупреждение и поставя началото на радарното разузнаване (**RADINT**, *Radar Intelligence*) като самостоятелен компонент на

⁵ COMINT – разузнаване от комуникации: телефони, радио, електронни съобщения

техническото разузнаване. Изграждането на интегрирани радарни мрежи, като британската **Chain Home Low (CHL)** и допълващите я нисковисочинни елементи, позволява откриване и проследяване на цели на големи разстояния. Това осигурява ценно време за реакция и по-точно управление на отбраната (Kovács, 2020, pp. 102).

Успоредно с това се развива и криптологичният компонент. Прихванатите радиосъобщения придобиват оперативно значение едва след механизираното им дешифриране. Полската „**bomba kryptologiczna**“, създадена като полуавтоматично средство за криптоаналитична атака срещу Enigma, показва как електромеханичната обработка ускорява установяването на настройки и прави възможно системното разчитане на противниковата кореспонденция (Link, 2009, pp. 166–168). От съюзническа страна този процес се развива в големи центрове като **Bletchley Park**, където криптоанализът се превръща в постоянен ресурс за ръководене на операциите (Kovács, 2020, pp. 101–102). В морската среда важно предимство дават акустичните средства като **ASDIC/сонар** (D'Amico & Pittenger, 2009, pp. 426–429), които поставят началото на акустичното разузнаване (**ACINT, Acoustic Intelligence**), основано на ехо-локация за откриване на подводници чрез определяне на разстояние и пеленг.

Наред с радиолокацията, криптоанализа и сонара, Втората световна война утвърждава и средства за скрито проникване с двойно предназначение: парашутът позволява въвеждане на малки групи в дълбочина, а апаратите за подводно дишане – прикрито приближаване по море. И в двата случая техническото средство служи едновременно за бойни и разузнавателни задачи.

1.4. Височинно-авиационна и сензорна фаза (Студената война – до началото на космическата доминация)

След 1945 г. акцентът се измества към разузнаването чрез научно-технически средства и към анализа на стратегическите комуникации. В този контекст **SIGINT** придобива особено значение, тъй като британският **JIC** (Joint Intelligence Committee) дава най-висок приоритет на добива на сведения за „...*съветски атомни, химически или биологични оръжия; други нови съветски оръжия; съветските военновъздушни сили; и управляеми оръжия.*“ (Aldrich & Coleman, 1989, pp. 536). Потребността от надеждно наблюдение в дълбочина води до създаването на самолета **U-2** – „...*специализирана разузнавателна платформа...оперираща до височина 70000 фута...*“, която осигурява изображения с много висока разделителна способност за стратегически анализ (Caddell, 2016, pp. 420).

През този период започва и възходът на **MASINT** (*Measurement and Signature Intelligence*) – дисциплина, която работи с технически данни от сензори, за да открива специфични характеристики, или

„сигнатури“, на обекти и събития. Dr. Aaron Chia Eng Seng определя MININT като „разузнаването на бъдещето“ (Chia Eng Seng, 2007, с. 118). Според *U.S. Army MASINT* е „технически производна разузнавателна информация“, която „открива, локализира, проследява, идентифицира и/или описва“ специфичните характеристики на целите и източниците (U.S. Army, 2004, Chapter 9, para. 9-1). Това позволява да се откриват признаци, които не винаги се виждат при обикновеното фотографско разузнаване, включително инфрачервени, спектрални и други емисии, свързани с ракетни, ядрени и технически дейности.

Устойчивата стойност на тези данни личи и от факта, че разсекретени **U-2** изображения от 50-те и 60-те години и днес се използват за прецизен ретроспективен анализ. Както отбелязват Hammer и Ur, тези изображения „улавят с висока разделителна способност облика на горещите точки на Студената война от 50-те и 60-те години“ (Hammer & Ur, 2019, p. 107).

1.5. Космическа (спътникова) фаза – IMINT/SIGINT от орбита (1960–1991)

От края на 50-те години разузнаването от орбита се превръща в ключов инструмент на глобалната сигурност. Спътниковите платформи позволяват мащабна оценка на военните способности чрез изображенческо разузнаване (**IMINT/GEOINT**) и сигнално разузнаване (**SIGINT**), включително **COMINT** – прихващане на съобщения, и **ELINT** – прихващане на излъчвания от технически средства (Galliford, 2024, p. 2-3).

Ранен пример за орбитално **IMINT** са програмите **Corona** и **Midas** на САЩ, които дават първото поколение системни разузнавателни изображения. След декласификацията част от тези масиви започват да се използват и за ретроспективен анализ на територии и инфраструктура (Jiang & Liu, 2023, p. 760-761; Muszyński-Sulima, 2023, pp. 9, 10, 14, 15).

Важен елемент на орбиталното наблюдение е и използването на **MASINT** сензори за засичане на ядрени детонации и балистични изстрелвания. Според *U.S. Army* това включва и ядрено разузнаване (**NUCINT**) – данни за ядрена радиация и други физични явления, свързани с ядрени оръжия, материали и съоръжения (U.S. Army, 2004, Chap. 9, para. 9-1–9-4). Тази линия по-късно става важна и за верификацията на ядрените договори чрез Международната система за мониторинг на **СТВТО**, която използва сеизмични, хидроакустични, инфразвукови и радионуклидни станции (СТВТО, n.d.). Така „националните технически средства за проверка“ утвърждават орбиталното наблюдение като фактор за международната стабилност (Muszyński-Sulima, 2023, pp. 14–15).

1.6. Мрежова/цифрова фаза: интернет, GPS, цифрова обработка и GEOINT като стандарт (1991–2014)

След Студената война разузнавателните технологии се развиват бързо под влияние на интернет, цифровите връзки и GPS⁶. Както отбелязват Kröpfl, Buchmüller и Leberl, онлайн картите, „облакът“ и GNSS⁷ „се съчетават в напълно нова инфраструктура“ за нови геопространствени приложения (Kröpfl, Buchmüller & Leberl, 2012, p. 151). Това променя начина, по който се събират, споделят и използват пространствени данни (Czaplewski & Goward, 2016).

През този период разузнаването става мрежово: данните идват от повече източници, предават се по цифров път и се обработват в обща среда. Същите автори подчертават, че онлайн картите вече „са напуснали света на настолните и преносимите компютри“ и са преминали към мобилните устройства, които са „отлична платформа“ за услуги, свързани с местоположението (Kröpfl, Buchmüller & Leberl, 2012, p. 151). Така геопространствената информация става по-достъпна и по-бърза за използване.

GEOINT и GIS⁸ се утвърждават като основна среда за обединяване на данни. Crampton, Roberts и Poorthuis пишат за „силен растеж“ на техническия GEOINT, свързан с обработката на големи масиви данни от въздушни сензори, а сред използваните средства са EO/IR⁹ сензори, синтетична апертурна радиолокация и сензори за химически и радиационни следи (Crampton, Roberts & Poorthuis, 2014, p. 11). Същият модел се вижда и при WIMAAS¹⁰, където данните идват от „различни източници на информация“, а после „се съпоставят с данни от други източници и разузнавателна информация“ (Gonçalves da Silva et al., 2012, pp. 38–39).

Това показва, че към 2010-те години се налага ясен модел: мрежово събиране, цифрова обработка и геопространствено обединяване на данни.

1.7. Тактическа безпилотна и електронно-борбена фаза (2014–2022)

След 2014 г. се наблюдава „демократизация“ на ISR¹¹ на

⁶ (Global Positioning System) - Глобална система за позициониране

⁷ GNSS (глобална навигационна спътникова система)

⁸ GIS (Geographic Information System) - Географска информационна система

⁹ EO/IR (Electro-Optical / Infrared) – електрооптични и инфрачервени сензори.

¹⁰ WIMAAS (JRC) – Wide Maritime Area Airborne Surveillance; експериментална „system-of-systems“ архитектура за широкозоново въздушно наблюдение на морски райони, разработвана/описвана от JRC (Joint Research Centre на Европейската комисия).

¹¹ ISR – Intelligence, Surveillance and Reconnaissance; разузнаване, наблюдение и рекогносцировка (комплекс от дейности и системи за събиране, обработка и използване на информация за обстановката).

тактическо ниво. Според автора малките **FPV**¹² дроне, безекипажните платформи и полевите **SIGINT** средства скъсяват цикъла „сензор–канал–анализ–тактическо действие“ и чрез ускорени **PED**¹³ процеси осигуряват разузнавателна информация в реално време за тактически решения (Kimmons, 2019, pp. 2–5; Europol, 2025, pp. 17–18). Kimmons свързва модернизацията на **PED** с по-бързото превръщане на видео, аудио и други масиви данни в основа за оперативни решения в реално време, а Europol подчертава, че след 2022 г. безпилотните системи вече се използват във всички домейни (среди), а натрупаните умения и технологии се разпространяват бързо (Kimmons, 2019, pp. 2, 4–5; Europol, 2025, pp. 17–18).

Това развитие налага и по-цялостен подход към противодействието (**C-UAS**)¹⁴. Вместо отделни средства все по-често се използват многосензорни решения, които съчетават радарно, **RF**, акустично и оптично откриване с **AI**, както и различни мерки за неутрализация, като **RF** заглушаване, **GPS spoofing**¹⁵, кинетично прихващане и насочена енергия. Hansen и Pinto Faria подчертават, че ефективните **C-UAS** решения се основават на комбиниране на различни сензори и на тяхното сливане в обща картина за откриване и проследяване в реално време (Hansen & Pinto Faria, 2023, pp. 49–50).

Електронната война се превръща в ежедневна задача и ускорява цикъла „мярка–контрмярка“. Появяват се и РЕБ-устойчиви решения, а **HPM**¹⁶ се утвърждават като важен способ за пряко въздействие върху противниковата електроника, особено срещу автономни или предварително програмирани дроне, при които класическото **RF** заглушаване не винаги е достатъчно (Chaari, 2021, pp. 69–70, 81–82).

1.8. Съвременна **AI**/автономна фаза: сливане на данни, рояци и устойчиви спътникови мрежи (2022–2025)

Най-новият етап в развитието на военното разузнаване се характеризира с автоматизирано сливане на големи масиви от данни, получени чрез **MASINT**, **IMINT** и **SIGINT**, както и с нарастващата роля на автономни системи и рояци от безекипажни платформи (Chandran & Vipin, 2024). Чрез **AI** може да се обработва по-голям обем информация и да се съпоставят данни от различни източници (Gao et al., 2020, pp. 831–833). **AI** моделите разширяват възможностите за наблюдение, като позволяват разпознаване на обекти не само по

¹² FPV – *First-Person View*; „първоличен“ видеоканал/управление (обикн. при дроне) чрез камера и пряко видеопредаване към оператор (екран/очила), създаващо ефект на „поглед от борда“.

¹³ PED (Processing, Exploitation and Dissemination) - обработка, аналитично използване и разпространение на разузнавателната информация

¹⁴ C-UAS (Counter-Unmanned Aircraft Systems) – противодействие на безпилотни летателни системи (ангидрон/контрадрон).

¹⁵ GPS spoofing - сигналът се подменя с подвеждащ

¹⁶ HPM (High-Power Microwaves) - високомощни микровълни (за въздействие)

външен вид, но и по физически следи в реално време, например термичен отпечатък или акустичен профил (Semerikov et al., 2025, p. 18).

Нараства и значението на **OSINT**. В съчетание с **AI** то подпомага откриването на аномалии, информационни отклонения и дезинформация и дава по-широк контекст на оперативната обстановка (Yotova, 2024; Julan & Togan, 2023).

Стратегическата устойчивост на разузнаването все повече се свързва с **LEO** мегаконстелациите¹⁷. Тези спътникови мрежи в ниска околоземна орбита осигуряват свързаност и пренос на данни дори при загуба на част от инфраструктурата, макар че отслабването на междуспътниковите връзки може да увеличи закъсненията и да намали капацитета (Chen et al., 2024, p. 1).

В тази фаза анализът се превръща в ключов фактор за ефективността. Интегрирането на **AI** в цикъла на **MASINT** изисква подход **security-by-design** и спазване на принципи за киберсигурност при високорискови **AI** системи, за да се ограничат враждебните манипулации и да се гарантира надеждността на автоматизирания анализ (Junklewitz et al., 2023, pp. 5–10). Въпреки това **HUMINT** запазва важна роля, защото съчетаването на технически данни и човешка оценка позволява разузнаването не само да реагира, но и да предвижда заплахи.

Таблица 1. Техническа периодизация на съвременното военно разузнаване

№	ПЕРИОД	ТЕХНИЧЕСКИ НОВОВЪВЕДЕНИЯ
1	1890-1914	ДВГ + МОТОРИЗАЦИЯ; РАННИ РАДИО/БЕЗЖИЧНИ + ОПТИКА/КАРТОГРАФИЯ
2	1914-1939	БАЛОНИ + ВИТЛОВИ САМОЛЕТИ; ФОТОКАМЕРА + ФОТОГРАМЕТРИЯ + МОБИЛНО РАДИО
3	1939-1945	РАДАР (МОРЕ/ВЪЗДУХ) + EW ЗАЧАТЪЦИ; СОНАР/ASDIC + КРИПТО/КРИПТОАНАЛИЗ + ПАРАШУТ; АПАРАТ ЗА ПОДВОДНО ДИШАНЕ
4	1945-1960	РЕАКТИВНА АВИАЦИЯ; ЕЛЕКТРОННИ СЕНЗОРИ + ВИСОЧИННО РАЗУЗНАВАНЕ (U-2)
5	1960-1991	СПЪТНИЦИ (IMINT/SIGINT); РАННИ КОМПЮТРИ + ЦИФРОВА КРИПТОГРАФИЯ
6	1991-2014	ИНТЕРНЕТ + GPS + ЦИФРОВИ ВРЪЗКИ; MALE/HALE UAV + ГИС/ПЛАТФОРМИ
7	2014-2022	ТАКТИЧЕСКИ/FPV ДРОНОВЕ; USV/UUV + РЕБ + ТЪРГ. САТ. НАБЛЮДЕНИЕ + OSINT/СОЦИАЛНИ МРЕЖИ + МОБИЛНИ ПРИЛОЖЕНИЯ
8	2022-2025	AI АНАЛИТИКА + АВТОНОМНИ РОЯЦИ; СПЪТНИКОВИ МРЕЖИ + АВТОНОМНИ ПЛАТФОРМИ

Източник: авторска разработка (синтез) по използваната литература в т. 1.1–1.8.

¹⁷ LEO мегаконстелации – Спътникови мрежи в ниска орбита (напр. Starlink).

Извод: Периодизацията показва, че еволюцията не е линейно натрупване, а „скокове“, при които нови платформи, сензори, канали и аналитични инструменти започват да работят съвместно и променят темпа и надеждността на разузнавателния цикъл.

2. СРАВНИТЕЛЕН АНАЛИЗ НА ОСНОВНИТЕ ФОРМИ И НАПРАВЛЕНИЯ НА РАЗУЗНАВАНЕТО

Разузнавателната дейност включва събиране, обработване и анализ на информация, необходима за военно-тактически и стратегически решения. М. Kamiński подчертава, че отделните канали за информация се комбинират и допълват (Kamiński, 2019). Те се различават по бързина, цена, риск, възможност за проверка и уязвимост.

2.1. Разузнаване чрез човешки източници (HUMINT)

Предимства: дава достъп до намерения, мотиви, планове и решения; позволява проникване в затворени среди и тила на противника; подпомага проверката на информацията; висока мобилност.

Недостатъци: крие висок риск за източниците и каналите; уязвимо е към дезинформация; изисква време, доверие и защитени връзки.

2.2. Разузнаване чрез технически средства

2.2.1. Разузнаване чрез прихващане и анализ на сигнали (SIGINT)

Предимства: осигурява достъп до комуникации и електромагнитни излъчвания; осигурява информация близка до реалното време.

Недостатъци: изисква сериозна техническа база; има пространствени и технически ограничения; уязвимо е към заглушаване и подвеждане.

2.2.2. Образно и геопространствено разузнаване (IMINT/GEOINT)

Предимства: дава зрително потвърждение и пространствена картина; подпомага планирането и ориентирането в обстановката.

Недостатъци: зависи от атмосферните условия, камуфлажа и заблуждаването; изисква експертна обработка и надеждна проверка.

2.2.3. Разузнаване чрез измерване и анализ на сигнатура (MASINT)

Предимства: открива обекти и дейности чрез техните измерими „подписи“; особено е полезно при откриване на ядрени материали и изпитания.

Недостатъци: скъпо и сложно; зависи от научна експертиза; само по себе си е рядко достатъчно.

Richelson посочва, че **MASINT** извлича разузнавателна стойност от измерими „сигнатури“ и е най-полезен като допълнение към други канали (Richelson, 2001, p. 1).

2.3. Разузнаване от открити източници (OSINT)

Предимства: нисък риск и сравнително ниска цена; бърз достъп до големи обеми информация; полезно за политически, икономически и научно-технически цели; полезно при изучаването на разузнаваната среда

Недостатъци: възможни са манипулации, неточности и дезинформация.

Van Puyvelde & Tabarez Rienzi отбелязват, че **OSINT** често служи като основа за първоначална ориентация и за проверка на данни от човешки и технически източници (Van Puyvelde & Tabarez Rienzi, 2024, p. 534).

Извод: Разузнавателните канали не действат изолирано. Най-надеждната картина се получава, когато **OSINT** дава първоначална насока и индикатори, **TECHINT** осигурява измеримо потвърждение и покритие, а **HUMINT** добавя контекст, намерения и вътрешен смисъл, обединени чрез анализа.

3. ИНТЕГРАЦИЯ НА РАЗУЗНАВАТЕЛНИТЕ ФОРМИ В СЪВРЕМЕННАТА СРЕДА

Разузнавателните дисциплини се припокриват, допълват и понякога си съперничат в рамките на един общ процес. Надеждността на разузнавателния продукт нараства чрез кръстосана верификация и включване на данните в обща оперативна картина (Wang & Cao, 2020, p. 55).

- **Взаимодействие и синергия:** HUMINT осигурява сведения и подпомага тяхната проверка, SIGINT показва признаци на активност, IMINT/GEOINT дава пространствена рамка и зрително потвърждение, MASINT позволява идентификация по сигнатури, а OSINT осигурява насочваща информация и ранни сигнали (NATO, 2002).

- **Конкуренция и съпоставка:** Между дисциплините възниква напрежение при разминаване на данните, различна преценка за достоверност или когато техническите средства временно изместват значението на агентурната проверка. То се преодолява чрез аналитично съпоставяне и оценка на източниците.

- **Интеграция в съвременни условия:** Днес интеграцията се постига чрез общи платформи, автоматизация и анализ, подпомаган от AI. Това улеснява обработката на информацията, а безпилотните системи допълнително ускоряват връзката между откриването, предаването и въздействието. Нараства и значението на C-UAS

средствата и на решенията, устойчиви на РЕБ (Percivall, 2010; Junklewitz et al., 2023, pp. 5–6; Gao et al., 2020, pp. 831–833; Europol, 2025, pp. 10–11, 20; Hansen & Pinto Faria, 2023, pp. 7–8).

Извод: Интеграцията е оперативна необходимост, а техническите средства допълват, но не заменят човешката преценка.

ЗАКЛЮЧЕНИЕ

Съвременното военно разузнаване се развива под динамичното влияние на научно-техническия прогрес, който фундаментално разширява възможностите за добив, проверка и анализ на информация (U.S. Joint Chiefs of Staff, 2013, p. 1). Тази трансформация не отменя класическите форми на разузнаване, а променя тяхното съотношение и засилва нуждата от взаимодействие. В условията на мирно време задачата за следене на въоръжението и потенциала на вероятния противник остава водеща, като се потвърждава принципът, че инвестицията в разузнаване е по-икономична от компенсирането на предотвратими щети.

Трансформацията на методите изисква разузнавателният продукт да се изгражда чрез синергия и взаимна проверка (cross-validation), особено в контекста на информационни операции и манипулации (UK Ministry of Defence, 2023, p. 4; NATO Standardization Office, 2023). Теорията и практиката доказват, че най-добри резултати се постигат, когато различните източници се съчетават и взаимно се допълват (UK Ministry of Defence, 2023, p. 91). Това се потвърждава и в академичния анализ, където изрично се подчертава, че отделните дисциплини не функционират изолирано (Henrico & Putter, 2024, p. 22, lines 1–2).

Техническият прогрес преобразява всяка дисциплина по различен начин:

- **OSINT** се разширява чрез AI инструменти за превод и обработка на големи масиви от данни, което подпомага откриването на аномалии и дезинформация (NATO OSINT Reader, 2002, p. 2).
- **HUMINT** запазва своята водеща роля за установяване на намерения, мотиви и планове, но става все по-уязвим на съвременното наблюдение, което налага по-строги мерки за сигурност и защита на източниците.
- При **SIGINT**, **IMINT/GEOINT** и **MASINT** модернизацията е най-видима чрез използването на дронове и спътникови системи за стратегическо покритие, макар че данните остават зависими от

условията и правилната интерпретация (Space Training and Readiness Command, 2023, p. 17).

Авторската теза е, че съвременното военно разузнаване изисква задължителна синергия между неговите форми. Най-устойчив разузнавателен продукт се получава чрез многоизточников подход: първоначално насочване чрез OSINT; последващо наблюдение и измерване чрез технически средства; и финализиране чрез човешки източници (HUMINT), които допълват картината с информация за намеренията и подпомагат верификацията. Именно тази синергия превръща суровите данни в надеждно проверено знание. Важно е да се отчете, че техническите данни сами по себе си не водят до автоматични изводи. Без контекст и качествена интерпретация дори точните измервания могат да доведат до погрешни оценки, тъй като „*дори най-добрата разузнавателна информация може да подлежи на различни интерпретации*“ (UK Ministry of Defence, 2023, p. 3, lines 153–155). В условията на хибридни заплахи и информационно пренасищане решаващо значение има качественият анализ, основан на интердисциплинарен подход и критична преценка (Nilsson, Weissmann и Palmertz, 2025).

В обобщение, съвременното военно разузнаване трябва да се разбира като високотехнологична, но преди всичко аналитична дейност. Неговата надеждност се основава на интеграцията на различните форми за добив, взаимната проверка на информацията и безусловното запазване на аналитичния приоритет.

ЛИТЕРАТУРА:

- Библия. (1982a). Синодално издание (Книга Исус Навин 2:1–24). Налично: <https://biblia.bg/index.php?k=6&g=2>
- Библия. (1982b). Синодално издание (Книга Числа 13:1–33). Налично: <https://biblia.bg/index.php?k=4&g=13>
- Лазаров, В. (2012). *Новите реалности и разузнаване с хора*. София: „Изток-Запад“. ISBN: 978-619-152-051-0.
- Лазаров, Гюров, (2012). *Матрични решения на националната сигурност*, София: „Изток-Запад“. ISBN: 978-619-152-096-1
- Служба „Военно разузнаване“. (n.d.). Министерство на отбраната на Република България. Налично: <https://dis.mod.bg/>
- Сун Дзъ. (2023). *Изкуството на войната*. София: Фама, ISBN 978-619-218-080-5
- Aldrich, R., Coleman, M. (1989). The cold war, the JIC and British signals intelligence, 1948. *Intelligence and National Security*, 4(3), 535–549. DOI: 10.1080/02684528908432015. Available from:

- https://warwick.ac.uk/fac/soc/pais/people/aldrich/publications/jic_1948.pdf
- <http://dx.doi.org/10.1080/02684528908432015> ;
<http://www.tandfonline.com/page/terms-and-conditions>
- Arbus, G. (2025). Decoding the world: An overview of modern intelligence disciplines. *Medium*. Available from: <https://medium.com/@guyarbus/decoding-the-world-an-overview-of-modern-intelligence-disciplines-775415bedbbd>
- Bigelow, R. P. (1951). Wireless in warfare, 1885–1914. *Proceedings*, 77(2) Available from: <https://www.usni.org/magazines/proceedings/1951/february/wireless-warfare-1885-1914>
- Bruton, E. (2014). Communication Technology. In: *1914-1918-online. International Encyclopedia of the First World War* (issued by Freie Universität Berlin). Berlin, 2014-12-09. DOI: 10.15463/ie1418.10504 Available from: <https://encyclopedia.1914-1918-online.net/article/communication-technology/?format=pdf>
- Caddell Jr., J. W. (2016). Corona over Cuba: The Missile Crisis and the Early Limitations of Satellite Imagery Intelligence. *Intelligence and National Security*, 31(3), 416–438. DOI: 10.1080/02684527.2015.1005495 Available from: https://www.researchgate.net/publication/273520282_Corona_over_Cuba_The_Missile_Crisis_and_the_Early_Limitations_of_Satellite_Imagery_Intelligence
- Campbell, James B. (2008). Origins of Aerial Photographic Interpretation, U.S. Army, 1916 to 1918. – *Photogrammetric Engineering & Remote Sensing*, 1, 77–93. American Society for Photogrammetry and Remote Sensing. DOI: 10.14358/PERS.74.1.77.
- Chaari, M. Z. (2021). High power microwave for knocking out programmable suicide drones. *Security and Defence Quarterly*, 34(2), 68–84. DOI: 10.35467/sdq/135068. Available from: <https://securityanddefence.pl/pdf-135068-66456?filename=66456.pdf>
- Chandran, I.; Vipin, K. (2024). Network analysis of decentralized fault-tolerant UAV swarm coordination in critical missions. *Drone Systems and Applications*, 12, 1–15. DOI: 10.1139/dsa-2023-0101 Available from: <https://cdnsiencepub.com/doi/10.1139/dsa-2023-0101>
- Chen, X.; Zhang, J.; Wang, X.; Li, Y. (2024). 3-ISL topology: Routing properties and performance in LEO mega-constellation networks. *IEEE Transactions on Aerospace and Electronic Systems*. DOI: 10.1109/TAES.2024.3512535. Available from: https://ese.nju.edu.cn/_upload/article/files/d3/14/3d3cb65f4899ba528ce4cce37733/ca5af812-88cd-4ccc-8352-5d775cfb9cbf.pdf

- CHIA ENG SENG, Aaron. (2007). MASINT: The Intelligence of the Future [online]. *DSTA Horizons*, 118–126. Le from: www.bpb-us-e1.wpmucdn.com/sites.psu.edu/dist/f/5180/files/2014/10/Reading_from_Cory_Botti.pdf (bpb-us-e1.wpmucdn.com)
- Crampton, J. W., Roberts, S. M., Poorthuis, A. (2014). The New Political Economy of Geographical Intelligence. *Annals of the Association of American Geographers*, 104(1), 196–214. DOI: 10.1080/00045608.2013.843436. Available from: https://geography.as.uky.edu/sites/default/files/faculty_publications/Crampton%20Roberts%20Poorthuis%202013%20Annals.pdf
- CTBTO. (n.d.). Comprehensive Nuclear-Test-Ban Treaty Organization. *The International Monitoring System*. Available from: <https://www.ctbto.org/our-work/international-monitoring-system>
- Czaplewski, K.; Goward, D. (2016). Global Navigation Satellite Systems – Perspectives on Development and Threats to System Operation. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 10(2), 183–192. DOI: 10.12716/1001.10.02.01. Available from: https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-95853a7c-210a-44c4-9be7f65ab6f6b9a2/c/Global_Navigation_Satellite_Systems___Perspectives_on_Development_and_Threats_to_System_Operation.pdf (PDF)
- D’Amico, A.; Pittenger, R. (2009). A Brief History of Active Sonar. *Aquatic Mammals*, 35(4), 426–434. DOI: 10.1578/AM.35.4.2009.426. Available from: https://www.aquaticmammalsjournal.org/wp-content/uploads/2010/10/35_4_D_Amico-Pittenger.pdf
- Europol. (2025). *The Unmanned Future(s): The impact of robotics and unmanned systems on law enforcement*. Luxembourg: Publications Office of the European Union. DOI: 10.2813/0022284. Available from: <https://www.europol.europa.eu/cms/sites/default/files/documents/The-Unmanned-Future-Report.pdf>
- Galliford, K. (2024). Legalities of Spying From Satellites and High Altitude Balloons. *Contemporary Issues in Air and Space Power*, 2(1), bp35753434. DOI: 10.58930/bp35753434 Available from: <https://ciasp.scholasticahq.com/article/91182.pdf>
- Gao, J.; Li, P.; Chen, Z.; Zhang, J. (2020). A survey on deep learning for multimodal data fusion. *Neural Computation*, 32(5), 829–864. DOI: 10.1162/neco_a_01273. Available from: https://www.mitpressjournals.org/doi/pdf/10.1162/neco_a_01273
- Gill, R. (2023). What is Open-Source Intelligence? *SANS Institute* (23 February 2023). Available from: <https://www.sans.org/blog/what-is-open-source-intelligence>

- Geographical Section, General Staff, War Office (1920). *Report on Survey on the Western Front 1914–1918*. October 1920. Available on: <https://1stmiddlesex.com/report/reportonsurveyonwesternfrontmodern text.pdf>
- Gonçalves da Silva, V., Jurquet, G., Marchalot, G., Gomez Calzado, M. T., Soroa, T., Sancho, J., Koubek, A., Van Wimersma Greidanus, H., Savarino, C. (2012). *Wide Maritime Area Airborne Surveillance (WIMAAS) WP5 Final Report*. (EUR 25183 EN; JRC68160). Luxembourg: Publications Office of the European Union. DOI: 10.2788/6952. Available on: <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC68160/lbna25183enn.pdf>
- Hammer, E., Ur, J. (2019). Near Eastern Landscapes and Declassified U2 Aerial Imagery. *Advances in Archaeological Practice*, 7(2), 107–126. DOI: 10.1017/aap.2018.38. Available from: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/A16A04FB4990B74B9FF750DCCF31A141/S2326376818000384a.pdf/near-eastern-landscapes-and-declassified-u2-aerial-imagery.pdf>
- Hansen, P., Pinto Faria, R. (2023). *Protection against Unmanned Aircraft Systems: Handbook on UAS protection of Critical Infrastructure and Public Space: A five Phase approach for C-UAS stakeholders* (EUR 31454 EN; JRC132714). Luxembourg: Publications Office of the European Union. DOI: 10.2760/18569. Available from: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC132714/JRC132714_01.pdf
- HENRICO, Susan, PUTTER, Dries (2024). Intelligence Collection Disciplines—A Systematic Review. *Journal of Applied Security Research*. Published online: 08 Jan 2024. DOI: 10.1080/19361610.2023.2296765. ISSN 1936-1610 (Print); ISSN 1936-1629 (Online). Available on 6 March 2026 on LinkPDF: <https://www.tandfonline.com/doi/epdf/10.1080/19361610.2023.2296765>
- Henry, Daniel J. (2017). *ISR Systems – Past, Present, and Future*. Rockwell Collins Inc., Cedar Rapids, IA 52498. Available: <https://rockwellcollinsthoughtleadership.wordpress.com/wp-content/uploads/2017/07/isr-systems-past-present-and-future.pdf>
- Horowitz, M. C.; Resnick Samotin, L. (2025, March 01). Driving Too Fast or Too Slow: Analyzing Military Adoption of the Combustion Engine. *SSRN*. DOI: 10.2139/ssrn.5238304. Available from: <https://ssrn.com/abstract=5238304>

- Jordanou, I. (2019). *Venice's Secret Service: Organizing Intelligence in the Renaissance*. Oxford University Press. <https://doi.org/10.1093/oso/9780198791317.001.0001>
- Jiang, P., Liu, Y. (2023). Echoes of Declassified Intelligence Satellite Photographs: Their Role and Application in the Research and Preservation of China's Built Vernacular Heritage. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVIII-M-2-2023*, 759–765. DOI: 10.5194/isprs-archives-XLVIII-M-2-2023-759-2023. Available from: <https://isprs-archives.copernicus.org/articles/XLVIII-M-2-2023/759/2023/isprs-archives-XLVIII-M-2-2023-759-2023.pdf>
- Julan, C. I., & Togan, M. (2023). Methodologies for Retrieving and Processing Information from Open Sources (OSINT). *Journal of Military Technology*, 6(1), 39–44. <https://doi.org/10.32754/jmt.2023.1.05>
- Junklewitz, H.; Hamon, R.; André, A.-A.; Evas, T.; Soler Garrido, J.; Sanchez Martin, J. I. (2023). *Cybersecurity of Artificial Intelligence in the AI Act: Guiding principles to address the cybersecurity requirement for high-risk AI systems* (EUR 31643 EN; JRC134461). Luxembourg: Publications Office of the European Union. DOI: 10.2760/271009. Available from: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC134461/JRC134461_01.pdf
- Kamiński, M. A. (2019). Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community. *Security Dimensions*, 32, 82–105. DOI: 10.5604/01.3001.0014.0988.
- Kimmons, Jeff; Gilmer, Graham (2019). *Remaking Intelligence Processing, Exploitation and Dissemination*. Thought piece. Booz Allen Hamilton. Available from: <https://www.defenseone.com/media/ped-thought-piece-presentedby-booz-allen.pdf>
- Kovács, P. (2020). A brit radarrendszer működése az angliai csata idején (The Operation of the British Radar System during the Battle of Britain). *Hadtudományi Szemle*, 13(4), 99–105. DOI: 10.32563/hsz.2020.4.8. Available from: <https://folyoirat.ludovika.hu/index.php/hsz/article/download/3236/4303/16291> (PDF)
- Kröpfl, M.; Buchmüller, D.; Leberl, F. (2012). Online maps and cloud-supported location-based services across a manifold of devices. *ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences, I-4*, 151–156. DOI: 10.5194/isprsannals-I-4-151-2012. Available from: <https://isprs-annals.copernicus.org/articles/I-4/151/2012/isprsannals-I-4-151-2012.pdf>

- Link, D. (2009). Resurrecting Bomba Kryptologiczna: Archaeology of Algorithmic Artefacts, I. *Cryptologia*, 33(2), 166–182. DOI: 10.1080/01611190802562809. Available from: https://alpha60.de/research/bomba_krypt/DavidLink_BombaCryptologiczna_Cryptologia2009.pdf
- Muszyński-Sulima, W. (2023, Summer). Cold War in Space: Reconnaissance Satellites and US-Soviet Security Competition. *European Journal of American Studies*, 18-2. DOI: 10.4000/ejas.20427. Available from: <https://journals.openedition.org/ejas/pdf/20427>
- NATO (2002, February). *Prepared by the staff of the Supreme Allied Commander Atlantic, Intelligence Branch, in collaboration with the Supreme Allied Command Europe (SACEUR)*. NATO Open Source Intelligence Reader. PDF: <https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20ct2002.pdf>
- NATO Standardization Office. (2023). *Allied Joint Publication AJP-10.1: Allied Joint Doctrine for Information Operations* (Edition A Version 1). Available from: https://assets.publishing.service.gov.uk/media/650c03bf52e73c000d9425bb/AJP_10_1_Info_Ops_UK_web.pdf
- NILSSON, Niklas; WEISSMANN, Mikael; PALMERTZ, Björn (2025). *Hybrid Threats and the Intelligence Community: Priming for a Volatile Age*. International Journal of Intelligence and CounterIntelligence. DOI: 10.1080/08850607.2024.2435265
- NORTH ATLANTIC TREATY ORGANIZATION (2002). *Open Source Intelligence Reader*. Brussels: NATO. Available from: <https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20ct2002.pdf>
- Percivall, G. (2010). The application of open standards to enhance the interoperability of geospatial information. *International Journal of Digital Earth*, 3(S1), 14–30. DOI: 10.1080/17538941003792751. Available from: <https://www.tandfonline.com/doi/pdf/10.1080/17538941003792751> (PDF)
- Quagliati, N. (2020). Training the eye: production and reception of aerial photography during the World Wars. *AUC Geographica*, 55(1), 93–111. DOI: 10.14712/23361980.2020.6. Available from: https://karolinum.cz/data/clanek/8001/Geogr_55_1_0093.pdf
- Richelson, J. T. (2001). MASINT: The new kid in town. *International Journal of Intelligence and CounterIntelligence*, 14(4), 541–548. DOI:

- 10.1080/088506001300063136. [online]. Available from: <https://www.tandfonline.com/doi/pdf/10.1080/088506001300063136>
- Russell, S. (n.d.). *Technical Transfer in the British Optical Industry 1888–1914*. The Case of Barr & Stroud, University of Glasgow, Available on: 3 March 2026 at <https://eprints.gla.ac.uk/302/1/BStech.pdf>.
- Semerikov, S. O., Nechypurenko, P. P., Vakaliuk, T. A.; Mintii, I. S., Kolhatin, A. O. (2025). Vision-based autonomous UAV landing: A comprehensive review of technologies, techniques, and applications. *Journal of Intelligent & Robotic Systems*, 111, 115. DOI: 10.1007/s10846-025-02314-4. Available from: <https://link.springer.com/content/pdf/10.1007/s10846-025-02314-4.pdf>
- Space Training and Readiness Command (STARCOM). (2023). *Space Doctrine Publication 2-0: Intelligence*. Available from: https://www.starcom.spaceforce.mil/Portals/2/SDP%202-0%20Intelligence%20%2819%20July%202023%29_1.pdf (PDF)
- Stefanova, A. (2025). The role of geodesy in military operations: Historical development and modern use. *Security and Defense*, (1), 213–221. DOI: 10.70265/PXBB9124. Available from: <https://institute.nvu.bg/en/statia/role-geodesy-military-operations-historical-development-and-modern-use>
- Tworek, H. J. S. (2014). Wireless Telegraphy. In: *1914-1918-online. International Encyclopedia of the First World War* (issued by Freie Universität Berlin). Berlin, 2014-10-08. DOI: 10.15463/ie1418.10347. Available from: https://encyclopedia.1914-1918-online.net/pdf/1914-1918-Online-wireless_telegraphy-2014-10-08.pdf
- UK Ministry of Defence. (2023). *Joint Doctrine Publication 2-00: Intelligence, Counter-intelligence and Security Support to Joint Operations*. Fourth Edition. London: UK Ministry of Defence. Available on 5 March 2026 from: https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf or https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf
- U.S. Army. (2004). *Field Manual 2-0: Intelligence. Chapter 9: Measurement and Signature Intelligence*. Washington, DC: Department of the Army. Available from: <https://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap9.htm>
- <https://www.globalsecurity.org/intell/library/policy/army/fm/2-0/fm2-0.pdf>
- U.S. Joint Chiefs of Staff (2013). *Joint Intelligence (Joint Publication 2-0)*. Washington, D.C.: Joint Chiefs of Staff.

- Available at:
https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf
- U.S. Naval War College, (n.d.). Intelligence Studies: Types of Intelligence Collection; Available on 6 March'26 at
<https://usnwc.libguides.com/c.php?g=494120&p=3381426>
- Van Puyvelde, D.; Tabarez Rienzi, F. (2024). Rise of open-source intelligence. *European Journal of International Security*, 9(4), 533–547. DOI: 10.1017/eis.2024.61. Available from:
https://resolve.cambridge.org/core/services/aop-cambridge-core/content/view/21122432399ECB8078BF0D89A76D0586/S2057563724000610a.pdf/rise_of_opensource_intelligence.pdf
- Wang, M.; Cao, S. (2020). A survey on C4ISR system architecture technique. *Global Journal of Engineering and Technology Advances*, 2(3), 54–66. DOI: 10.30574/gjeta.2020.2.3.0019. Available from:
<https://scispace.com/pdf/a-survey-on-c4isr-system-architecture-technique-3r0hefwakj.pdf>
- Yotova, R. (2024). Conceptual model of an automated system for processing information from open sources and detecting information deviations. *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, 4, 305–311. DOI: <https://doi.org/10.17770/etr2024vol4.8230> . ISBN: 978-619-185-593-3. Print ISSN: 1691-5402; ISSN: 2256-070X. Available from:
<https://archive-journals.rtu.lv/etr/article/view/5085>