РЕЗЮМЕТА НА НАУЧНИТЕ ТРУДОВЕ

на гл. ас. д-р Владимир Огнянов Бабанов

представени за участие в конкурс за заемане на академична длъжност „Доцент“ по професионално направление 9.1. „Национална сигурност“, Югозападен университет „Неофит Рилски“ – Благоевград, обявен в ДВ бр. 107 от 12.12.2025 г.

1.Хабилитационен труд - монография

Бабанов, В. (2026), “Въздействие на генеративния изкуствен интелект върху концепцията за киберсигурност”, Университетско издателство „Неофит Рилски“, Благоевград, **ISBN: 978-954-00-0446-4**

Монографията „Въздействие на генеративния изкуствен интелект върху концепцията за киберсигурност“ представлява интердисциплинарно изследване, посветено на трансформационното влияние на генеративния изкуствен интелект (ИИ) върху теоретичните основи, стратегическите измерения и практическите механизми на киберсигурността. Разработката се позиционира в контекста на ускорената дигитална трансформация след 2022 г., когато широката публична достъпност на големи езикови модели показа, че ИИ се превръща в структуроопределящ фактор за икономиката, управлението и сигурността. Основната изследователска теза е, че генеративният ИИ не представлява просто нов инструмент в киберсредата, а фактор, който променя самата философия на сигурността и изисква преоценка на установените принципи и подходи.

Целта на изследването е да се изясни въздействието на генеративния ИИ върху фундаменталните принципи на киберсигурността и върху динамиката на киберпрестъпността от ново поколение, както и да се очертаят възможностите за интегриране на тази технология в архитектурата на съвременната киберотбрана. Обект на изследване е киберпространството като среда на взаимодействие между интелигентни системи, институции и злонамерени субекти, а предмет – ефектът на генеративните модели върху принципите, практиките и баланса между настъпателни и отбранителни способности. Методологически се прилагат сравнителен анализ на

регулаторни рамки и стратегии, критичен преглед на научна и експертна литература, казусен метод и концептуално моделиране.

В първата глава се разглеждат класическите концепции за киберсигурност и тяхната еволюция под въздействието на генеративния ИИ. Анализира се триадата конфиденциалност, интегритет и наличност (КИН) като фундамент на информационната сигурност. Посочва се, че генеративните модели създават нови рискове за конфиденциалността чрез възможността за възпроизвеждане на чувствителни данни, за интегритета чрез генериране на убедително фалшиво съдържание и за наличността чрез автоматизирана експлоатация на уязвимости. Наред с това се подчертава, че същата технология може да подпомага динамичното управление на риска, симулационното моделиране и ранното идентифициране на аномалии.

Разглеждат се и принципите „защита в дълбочина“ и „нулево доверие“, които се поставят в нов контекст на висока свързаност и автоматизация. Отбелязва се, че нарастващата интеграция на ИИ в облачни и хибридни среди увеличава атакуемата повърхност, като същевременно предоставя възможности за непрекъснат мониторинг и адаптивна реакция. Анализира се и необходимостта от прецизиране на принципите за минимални привилегии и отграничаване на задълженията в условията на автономни ИИ агенти. Въвежда се идеята за „машинно отграничаване на отговорностите“, което цели да ограничи рисковете от прекомерна концентрация на достъп и функционалности в автоматизирани системи.

Особено внимание се отделя на принципите „сигурност по дизайн“ и „поддържане на опростеност и сигурност“ (KISS), които придобиват ново значение в среда на нарастваща сложност. Подчертава се, че внедряването на генеративен ИИ изисква предварително проектиране на защитни механизми и ясна регламентация на ролята на алгоритмите в организационните процеси. В тази връзка се обсъждат и въпросите за отговор при инциденти, непрекъснатост на бизнеса и възстановяване от бедствия, като се очертават възможности за използване на ИИ при симулации на сценарии, анализ на въздействието и ускорено възстановяване.

Втората глава е посветена на генеративния ИИ като катализатор на киберпрестъпления от ново поколение. Изяснява се, че технологията предоставя

стратегическо предимство на злонамерени актьори чрез висока адаптивност, автоматизация и нисък праг за достъп. Анализират се конкретни форми на злоупотреба, включително фишинг и социално инженерство с повишена степен на персонализация, генериране и оптимизация на зловреден софтуер, създаване на дълбоки фалшификати и използване на ИИ за разузнаване и сканиране на уязвимости. Отбелязва се, че в нелегалната онлайн среда вече съществуват структурирани пазари за инструменти и услуги, базирани на ИИ, което допълнително улеснява киберпрестъпната дейност.

Разглеждат се и сложните настойчиви заплахи (APT), включително взаимодействието между държавно подкрепяни групи и криминални мрежи. Генеративният ИИ се интерпретира като фактор, който усилва асиметрията в киберпространството и размива границите между държавни и недържавни субекти. Подчертава се геополитическото измерение на технологичната надпревара и необходимостта от стратегическа адаптация на националните политики за сигурност.

Третата глава разглежда потенциала на генеративния ИИ в практиките по киберсигурност. Анализират се възможности за автоматизация на аналитичната дейност, подпомагане на „лова на заплахи“, анализ на аномалии и интеграция със системи за управление на събития и автоматизирана реакция. Подчертава се, че оптималният модел на приложение предполага сътрудничество между човешкия експертен фактор и алгоритмичните системи, при което ИИ изпълнява подпомагаща и ускоряваща функция, без да елиминира необходимостта от стратегическа и етична преценка.

Като основен научно-приложен принос се предлага концептуална рамка за автоматизирано асоцииране на зловредна дейност с известни хакерски групи чрез използване на генеративен ИИ и киберразузнавателни данни. Рамката цели да съкрати времето за атрибуция на атаки и да повиши ефективността на аналитичните процеси, като комбинира алгоритмична обработка на големи обеми информация с експертна верификация.

В заключение се формулира необходимостта от нова парадигма на киберсигурността, основана на адаптивност, прозрачност и стратегическа интеграция на ИИ. Генеративният изкуствен интелект се разглежда като двойнствен феномен –

едновременно източник на нови рискове и инструмент за тяхното ограничаване. Изследването очертава посоки за бъдещи научни разработки и практически политики в условията на ускорена алгоритмична трансформация на дигиталната среда и нарастваща зависимост на националната сигурност от интелигентни технологични системи.

2. Статии и доклади, публикувани в научни издания, реферирани и индексирани в световноизвестни бази данни с научна информация

1. G. Belova, G. Georgieva, Y. Kochev, A. Yankov, and **V. Babanov**, "COVID-19, INFODEMIC AND CYBER SECURITY", ETR, vol. 5, pp. 57–61, Jun. 2025, doi: 10.17770/etr2025vol5.8479. https://archive-journals.rtu.lv/etr/article/view/5290

Статията има за цел да проследи въздействието на някои процеси, свързани с пандемията от COVID-19, върху отделни сфери на обществения живот и върху националната сигурност. Анализът се фокусира върху два основни аспекта – инфодемията и киберсигурността, тъй като по време на COVID-19 те се откроиха като проблеми с дългосрочен характер. Пандемията от COVID-19 представляваше предизвикателство, което изискваше международната общност, правителствата и политическите елити да се справят с множество измерения, надхвърлящи последиците за общественото здраве и оказващи влияние върху сигурността. Изходна точка на анализа са социалните детерминанти на правото на здраве, които утвърждават общественото здраве едновременно като елемент на сигурността и като една от целите на устойчивото развитие. Именно част от тези детерминанти на правото на здраве се оказаха обект на инфодемията – разпространението на невярна или подвеждаща информация, съзнателно създавана с цел да навреди на отделен човек, социална група, организация или държава. Наред с това слабостите, разкрити по време на пандемията, подчертаха необходимостта от по-силна международна рамка, способна да противодейства както на разпространението на дезинформация, така и на нарастващата сложност на кибератаките. Това налага разработването на всеобхватна стратегия, включваща засилено международно сътрудничество, повишаване на обществената осведоменост и прилагане на съвременни технически решения. Предвид чувствителния характер на здравната проблематика, която става още по-уязвима при

въздействието на инфодемия или киберпрестъпност, е използвана подходяща методология. Основният извод е, че освен усъвършенстване на международното законодателство с оглед подготовката за и предотвратяването на бъдещи пандемии, следва да се обърне по-голямо внимание и на съпътстващите ги явления, като инфодемията и киберпрестъпността. Това е от изключителна важност, тъй като при евентуални бъдещи пандемии може да се очаква тяхното развитие в значително по-голям мащаб. Международната общност и националните елити следва да обсъдят и предприемат конкретни мерки за справяне с тези явления.

2. **Статии и доклади, публикувани в нереферирани списания с научно рецензиране или публикувани в редактирани колективни томове:**

1. Babanov, **V.** (2024). "Internals of Defense-In-Depth Strategy in Cybersecurity," *Security and Defense, vol. 2, pp. 37-42, Dec. 2024.* https://doi.org/10.70265/PNEZ3158 DOI: https://doi.org/10.70265/PNEZ3158

Разработката изследва основите на стратегията „защита в дълбочина“ в киберсигурността, като акцентира върху нейното значение за противодействие на заплахи в динамичната среда на сигурността. Чрез прилагането на множество слоеве от независими защитни контроли в рамките на физически, технически, управленски и оперативни домейни организациите могат ефективно да ограничават рисковете и да предотвратяват кибератаки. Адаптивността на стратегията я превръща в устойчива рамка за справяне с развиващите се предизвикателства в областта на киберсигурността, като предлага цялостен подход за защита срещу широк спектър от заплахи.

2. **Бабанов, В.**, (2023). „Военният конфликт в Украйна – към нов световен ред или борба за оцеляване на Русия.“ *Сигурност и отбрана*, (1), 212-222. , ISSN 2815-4584 (Online), ISSN 2815-388X (Print); https://doi.org/10.70265/RXAG6807; DOI:https://doi.org/10.70265/RXAG6807

Статията обръща внимание на влиянието на войната в Украйна върху световния ред и върху съдбата на Русия. Възможно ли е конфликтът да предизвика верижна реакция на други места по света и да доведе до рухване на „американския свят“, до залеза на Запада, или дилемите пред Руската федерация ще се задълбочат и ще направят съдбата ѝ неясна? Съществуват индикации за развитие и на двата сценария, но е възможен само един. Действията на Русия в Украйна подкопават основни принципи на съвременните международни отношения, които или ще бъдат защитени, или ще възникне опасен прецедент, който ще дестабилизира глобалната сигурност. За България това са въпроси от изключително значение.

3. **Бабанов, В.** (2025) “Дигитален суверенитет и ООН – между защита на националната сигурност и международното сътрудничество в киберпространството.” Сб. „Съвременните международни общувания и защита на правата на човека. Ролята на ООН.“ УИ „За буквите – О писменехь“, С. 2025, стр. 61.; ISBN 978-619-185-735-7; https://drive.google.com/file/d/1iLzqeAI4_jHwLd5CNn0YO6cMt3RflVUS/view

Настоящата статия изследва концепцията за дигитален суверенитет в контекста на международната система и ролята на Организацията на обединените нации (ООН) в управлението на киберпространството. В епохата на глобална дигитализация, националният суверенитет придобива ново значение, свързано с управлението на интернет и защитата на киберсигурността. Документът разглежда противоречивите подходи на водещи геополитически сили, като Русия, Китай, Северна Корея, от една страна, и демократичните държави – от друга, и как те влияят върху международното сътрудничество.

4. **Бабанов, В.** (2021). “Глобалната среда за сигурност и съвременни характеристики на системата на международните отношения”; сп. *Национална сигурност* (9), 37-41. https://nacionalna-sigurnost.bg/broi-9/. ISSN 2682-941X & ISSN 2682-9983.

Темата за ефектите на Ковид-19 върху света са безспорен тематичен акцент пред държавите и обществата. Вирусът усложнява глобалната среда за сигурност, но големите процеси, присъщи за системата на международните отношения, не са престанали своето развитие. Статията обръща поглед върху отношенията между големите сили на 21-и век, йерархията в системата и нейния характер- наченките на многополюсен свят съвсем не са гаранция за подобно развитие. Наред с взаимодействието между големите центрове на сила съществуват значителен брой глобални процеси, влияещи на международната сигурност.

5. **Бабанов, В.** & Насева, Йо. (2022). Ефекти от пандемията от COVID-19 върху националната и международна сигурност. *Право, Политика, Администрация, 9(2),* 1-7. https://lpajournal.swu.bg/wp-content/uploads/2022/09/Vladimir-Babanov-summary-BG.pdf

Пандемията от COVID-19 продължава да нанася щети върху всички системи на националните държави. От самото й начало, обществата по света избраха проактивен подход за превенция и ограничаване на заболеваемостта, което доведе до редица очаквани и неочаквани ефекти. Трудно е да се изчисли истинската стойност на материалните и нематериални поражения в глобален мащаб, затова тази статия поставя акцент върху три основни сфери с огромна важност за националната сигурност- икономика, здравеопазване и дигитализация. Всяка от тези области претърпява разнородни ефекти, включително положителни, но едно може да се каже със сигурност- пандемията от COVID-19 предизвика мащабна глобална трансформация.

6. **Бабанов, В.** (2021). „Изграждане на цялостна система за киберсигурност-приоритет на България през настоящото десетилетие“; Електронно списание „Право, Политика, Администрация”, том 8, бр. 2/2021 г., с. 46-52, ISSN 2367-4601 (Online); Retrieved from https://lpajournal.swu.bg/wp-content/uploads/2021/12/Vladimir-Babanov-br8-2.pdf

Киберсигурността вече е неделима част от общото изследване за сигурността. Настоящата публикация обръща внимание на процеса на изграждане на система за

киберсигурност на Р. България. Целта е до 2030 г. страната да изгради цялостна киберзащита, която да е интегрална част от системата за киберсигурност на ЕС. Тази обща мрежа за киберсигурност е отправната точка на страните от общността в стремежа им да отговорят на новите заплахи в електронна среда.

7. **Babanov, V.** (2025) "Artificial Intelligence and Cybersecurity in Space Warfare", сп. „Международна политика", бр. 2, стр. 105-110; Retrieved from http://ip.swu.bg/mod/data/view.php?d=1&rid=739&filter=1 ; ISSN 2367-5373;

Космическите операции са дълбоко повлияни от бързото навлизане на изкуствения интелект (ИИ) в сферата на киберсигурността. Настоящата статия разглежда водещи съвременни изследвания по темата и анализира неизбежната двойна роля на ИИ както в отбраната, така и в нападението при космическа война. Разкриват се начините, по които ИИ се прилага за усъвършенствано откриване и реагиране на заплахи в орбита, с цел защита на критични космически апарати от кибератаки. Става очевидно, че мощни и гъвкави технологии като ИИ представляват сериозна заплаха за космическата инфраструктура, изграждана преди десетилетия. Злонамерени актьори и определени държави се стремят едновременно да получат предимство над своите противници и да защитят собственото си уязвимо космическо оборудване. Основавайки се на значимите разработки в областта, статията разглежда технологичните предизвикателства, стратегическите императиви и липсата на международна нормативна рамка, необходими за изясняване на сложните последици от въздействието на ИИ върху космическата сигурност и това, което все по-ясно се очертава като форма на война. Анализът подчертава належащата необходимост от технически и правни механизми, които да регулират опасния баланс между ИИ, киберсигурността и растящите залози в последната граница на стратегическото съперничество.

8. **Бабанов, В.,** (2024) „Дезинформацията в киберпространството- заплаха за демократичните процеси в Югоизточна Европа", Сборник с доклади от Кръгла маса, организирана от Югозападен университет „Неофит Рилски" и Университет по библиотекознание и информационни технологии (УниБИТ) „СЪВРЕМЕННИ ИЗМЕРЕНИЯ НА СИГУРНОСТТА В ЮГОИЗТОЧНА ЕВРОПА", ISBN 978-954-

00-0356-6, Благоевград, ЮЗУ „Неофит Рилски“, с. 51-58, Достъпно на: http://press.swu.bg/images/conf/collection_security_unibit.pdf

Дезинформацията се използва като основно оръжие в борбата за геополитическо надмощие между големите сили. Развитието на интернет и високите технологии улесниха изключително много нейното разпространение, а изкуственият интелект допринесе за почти цялостното автоматизиране на процеса на дезинформация на обществата. Възможността интернет да се окаже доминиран от ботове, дезинформация и злонамерени играчи е напълно реална- обстоятелство, което тревожи страните от Югоизточна Европа поради тяхната особена уязвимост. В тази статия се обръща внимание именно на тези процеси.

9. **Babanov, V.** (2025), Strategic Considerations for AI-Enhanced Cybercrime, сп. „Право, Политика, Администрация”, том 13, бр. 2/2025 г., с. 46-52, ISSN 2367-4601 (Online); Retrieved from https://lpajournal.swu.bg/wp-content/uploads/2025/12/1-Vladimir-Babanov.pdf

Статията цели да подчертае някои способи, чрез които киберпрестъпниците използват изкуствения интелект (ИИ) за извършване на киберпрестъпления. Ефектите на ИИ върху киберпрестъпността е също основен фокус, наравно с причините за бързото разпространение на моделите на ИИ в киберпространството. Резултатът от подобно сливане на технологии, криминални интереси и икономически мотиви е невъзможно да бъде предвиден, но обмислянето на основни съображения спрямо киберпрестъпността, подсилена от ИИ, би могло да послужи като важна отправна точка за последващи дискусии.

10. **Babanov, V.** (2026) “AI-Enabled predictive diplomacy: data-driven approach to foreign policy”, сборник „Международната система в преход. Нови парадигми на сигурността и дипломацията в дигиталната епоха.“ Издателство „За буквите-О писменехь“, 2026 г., ISBN 978-619-185-793-7, (под печат, представена служебна бележка)

Настоящата разработка изследва концепцията за дипломация, подпомагана от изкуствен интелект с предиктивни възможности, като нов феномен в сферата на

външната политика. Чрез използването на нови и мощни технологии държавите могат да извеждат латентни интереси и поведенчески модели на своите партньори на основата на големи обеми на пръв поглед несвързана информация. Предложената рамка измества фокуса на преговорите от пасивното разчитане на BATNA към проактивна стратегия, усилена чрез изкуствен интелект. Изследването демонстрира потенциалните ползи от използването на ИИ в преговорния процес, като същевременно отчита и етичните граници, които подобен подход поставя под въпрос.

11. **Babanov, V.** (2026) "OSINT with AI for geopolitical conflict forecasting", сборник „Международната система в преход. Нови парадигми на сигурността и дипломацията в дигиталната епоха." Издателство „За буквите- О писменехь", 2026 г., ISBN 978-619-185-793-7, (под печат, представена служебна бележка)

Настоящата разработка представлява обзор на теорията за OSINT, базирана на изкуствен интелект, във връзка със системите за стратегическо ранно предупреждение. Разглежда се по какъв начин ИИ може да подобри всички етапи от разузнавателния цикъл – от събирането и обработката на данни до изготвянето на прогнози – както и потенциалът му да повиши способността за стратегическо предупреждение при конфликти. Анализирани са и ключови предизвикателства пред ИИ-базираната OSINT, включително пристрастия в данните, ограничения на моделите, липса на прозрачност и обяснимост на алгоритмичните методи, както и т.нар. „разрив между предупреждението и реакцията" в контекста на моделирането на геополитическа нестабилност. В заключение се подчертава, че макар OSINT, подпомагана от изкуствен интелект, да притежава потенциала да трансформира моделирането на геополитическа нестабилност, реализирането на този потенциал изисква стриктна интеграция на човешка експертна преценка и внимателно съобразяване с техническите и институционалните ограничения.

12. **Babanov, V.** (2026). **„**Synthetic reality as a strategic threat: from disinformation to predictive manipulation". E-Journal VFU, 25, 84-93. Издателски център на ВСУ

"Черноризец Храбър", ISSN 1313-7514, https://ejournal.vfu.bg/index.php/vfu/article/view/261

Статията разглежда потенциала на изкуствения интелект да трансформира дезинформацията в усъвършенстван тип синтетична реалност, основана на хиперперсонализирана манипулация и когнитивна експлоатация. Синтетичната реалност се различава съществено от традиционните форми на пропаганда, тъй като е дълбоко потапяща, значително по-устойчива във времето и притежава способността да влияе върху решенията и поведението както на отделни индивиди, така и на цели общества. Анализира се начинът, по който синтетичните медии подкопават стратегическото доверие, създавайки дълготрайна заплаха, която заобикаля конвенционалните механизми за откриване и защита. Идентифицират се съществени пропуски в готовността по отношение на правната рамка, технологичните инструменти и доктриналните подходи. В заключение се формулират насоки за политики и решения, основани на повишаване на устойчивостта, с цел справяне с тези еволюиращи предизвикателства.

13. **Бабанов, В.** (2026). „Ai-enhanced counter-offensive decision-making in hybrid warfare.“ E-Journal VFU, 25, 94-102. Издателски център на ВСУ "Черноризец Храбър",ISSN1313-7514, https://ejournal.vfu.bg/index.php/vfu/article/view/262

В настоящата статия се изследва използването на изкуствения интелект (ИИ) като средство за усъвършенстване на контранастъпателното вземане на решения в среда на хибридна война. Хибридната война се дефинира като пространство, в което се пресичат конвенционални военни тактики и други форми на водене на война, като кибервойна, информационна война и психологическа война. Тази среда създава условия на несигурност, неотложност и висока степен на асиметрия, които изискват ефективно и навременно вземане на решения. Изследването показва, че прилагането на ИИ може да предостави съществена подкрепа при планирането на контранастъпателни действия чрез съкращаване на времето за вземане на решения, подпомагане на интеграцията на данни от множество домейни и повишаване на ситуационната осведоменост посредством аналитични инструменти и системи за подпомагане на решенията. Идентифицират се както ползите от ИИ-базираните

процеси на вземане на решения, така и съществуващите ограничения. В заключение се подчертава, че изкуственият интелект би бил най-ефективен като част от балансирана система човек–машина, при която ИИ подпомага процесите на вземане на решения, основани на данни, а човешкият фактор запазва стратегическата преценка и отговорността.

14. **Babanov, V.** (2026). „Artificial intelligence in anti-money laundering and the questions of explainability, privacy and trust.“ сп. „Право, Политика, Администрация”, том 13, бр. 1/2026 г., ISSN 2367-4601 (Online); (под печат, представена служебна бележка)

Настоящата статия има за цел да изследва трансформиращите възможности на изкуствения интелект за подобряване разкриването и предотвратяването на прането на пари. Тя синтезира изследванията върху разкриването на финансови измами, в контекста на изкуствения интелект, и се фокусира върху ролята на обяснимия изкуствен интелект за прозрачност и съответствие с регулаторните изисквания. Акцентира се върху нуждата от правна координация между технологичните иновации, финансовия надзор и международните принципи за прозрачност и отчетност в защита на основните човешки права в контекста на автоматизирания финансов анализ и контрол. Статията също обръща внимание на федерираното обучение за анализа на данни и опазването на поверителността. Обсъждат се факторите, балансиращи връзката между разкриването на незаконни парични потоци, поверителността на данните и доверието на потребителите в законните практики по пресичане на прането на пари чрез автономни системи. В заключение са обобщени ключовите ползи и предизвикателства пред интегрирането на изкуствения интелект в рамките на борбата с прането на пари, заедно с основни препоръки.

15. **Babanov, V.** (2026). The ascending techno-nationalism in the U.S.– China rivalry and the EU’s technological independence., сп. „Международна политика“, бр. 1, 2026 г.; ISSN 2367-5373; (под печат, представена служебна бележка)

Възходът на технонационализма е ключов фактор за оформянето на технологическото съперничество между САЩ и Китай и влияе върху начина, по който Европейският съюз преследва технологическа независимост. Технонационализмът определя подхода, чрез който САЩ и Китай се стремят към стратегическо доминиране чрез нововъзникващи технологии като изкуствен интелект, полупроводници и облачни изчисления. Настоящото изследване аргументира, че макар ЕС да се стреми към постигане на дигитален суверенитет, той е изправен пред редица предизвикателства, произтичащи от фрагментираната индустриална база, бавния иновационен цикъл и зависимостта от чуждестранно разработени технологии в критични области. Изводите подчертават необходимостта от укрепване на индустриалната политика на ЕС и повишаване на иновационния капацитет, наред с реализирането на регулаторните цели, за да бъде запазена стратегическата автономия в условията на бързо променящ се световен технологичен ред.

16. **Babanov, V.** (2026). **„**Fractured cyberspace and digital disorder as a strategic threat to international security“, сп. сп. „Международна политика“, бр. 2, 2026 г.; ISSN 2367-5373; CEEOL; Национален референтен списък; (под печат, представена служебна бележка)

Статията очертава възможно по-нататъшно развитие на явлението „Сплинтернет“, при което дигиталният хаос нараства експоненциално. Акцентът е поставен върху неконтролируемия ръст на киберпрестъпността, както и върху изкривяването на реалността чрез дезинформация и използване на синтетични идентичности. Изследването разглежда стремежа на държавите към дигитален суверенитет, който често се осъществява за сметка на глобалната свързаност. Фрагментацията на интернет пространството увеличава възможностите на злонамерени актьори да подкопават неговата стабилност. Подчертава се, че липсата на ефективно международно сътрудничество допълнително задълбочава съществуващите негативни тенденции.

17. **Babanov, V.** (2026). „Automated threat actor profiling with AI in cyber threat intelligence: a framework for real-time extraction and attribution“, сп. „Образование, научни изследвания и иновации“, година 4, книжка 1, март 2026, ISSN 2815-4630, CEEOL, CrossRef, Национален референтен списък (под печат, представена служебна бележка)

Киберразузнавателната информация (Cyber Threat Intelligence – CTI) се утвърди като ключов елемент на проактивната защита срещу противници в киберпространството. Въпреки това по-голямата част от ценната информация се съдържа в огромни обеми неструктурирани данни и потоци, което прави тяхната обработка изключително продължителен и податлив на грешки процес. Настоящото изследване има за цел да представи автоматизирана рамка в реално време, която използва обработка на естествен език (Natural Language Processing – NLP) и стандартизирани онтологии като Structured Threat Information Expression (STIX) v2.1 и MITRE ATT&CK, за да идентифицира индикатори за компрометиране (IoCs), тактики, техники и процедури (TTPs) от множество източници на CTI и да ги съпоставя с профил на заплахов актьор. Описаният подход обработва данни от публични доклади за заплахи, социални мрежи и други платформи за споделяне на информация. Използват се домейн-специфични езикови модели и анализатори, базирани на правила, за разпознаване на същности (напр. зловреден софтуер, инструменти, цели), които се картографират към обекти по STIX и се свързват с техники от рамката ATT&CK. Рамката е тествана чрез хипотетичен казус с рансъмуер, който демонстрира как извлечените индикатори, етапи от kill chain и поведенчески модели могат да бъдат асоциирани с профил на заплахов актьор. Резултатите показват, че предложената ИИ-базирана обработваща линия значително намалява необходимите ръчни усилия при анализа на CTI, като същевременно поддържа висока точност на извличане. Изследването поставя основите за внедряване на автоматизирано профилиране на противници в рамките на киберразузнаването, което подпомага проактивната защита и усилията по атрибуция.

18. **Babanov, V.** (2026). „Delegating cyber defense to algorithms: the legal boundaries of autonomous response in Bulgaria“, сп. „Образование, научни изследвания и

иновации“, година 4 , книжка 2, юни 2026, ISSN 2815-4630, (под печат, представена служебна бележка)

Статията разглежда правните последици от използването на автономни механизми за реакция в българската система за киберотбрана. Анализира се националната правна рамка на България в по-широкия контекст на стратегическите документи на НАТО и Европейския съюз. Дефинира се понятието за автономен киберотговор и се изследва неговата правна приложимост, като се подчертава, че автоматизираните отбранителни действия поставят предизвикателства пред съществуващите правни стандарти. Проследява се еволюцията на българската киберотбранителна политика – от ранните стратегии в областта на киберсигурността до най-новото съобразяване с директивите на ЕС и изискванията на НАТО. Анализът показва, че българското законодателство не предвижда изрично правно основание за прилагане на автоматизирани контрамерки при кибератаки. Липсата на такава правна регламентация поражда както теоретични, така и практически проблеми, свързани със съответствието и прилагането на нормите. В заключение се посочва, че макар националното законодателство да предоставя цялостна основа за противодействие на киберпрестъпността и защита на критичната инфраструктура, съществуват предизвикателства при интегрирането на автономни киберотговори в действащата нормативна рамка. Подчертава се, че разработването на всяка стратегия следва да бъде съобразено с международните задължения на страната и с изискванията на съюзните формати, в които тя участва.

19. **Babanov, V.** (2026) Cybertime as a battlefield and the end of sequential military strategy; сп. *Национална сигурност* (9), 46-49. https://nacionalna-sigurnost.bg/broi-23/ ISSN 2682-941X & ISSN 2682-9983. https://nacionalna-sigurnost.bg/broi-23/

В съвременните конфликти времето все по-често се използва като бойно поле. Процесите на вземане на решения, ускорени от кибер-ИИ технологии, се компресират до степен, при която се размиват традиционните представи за това какво представлява войната. С нарастването на темпа на конфликта моделите, основани на подредени и последователни цикли на вземане на решения – като OODA-цикъла или фазите на

кампанията – все повече се разминават с реалностите на висикоскоростната, предиктивна война. В резултат на това последователната рамка в военната стратегия се поставя под сериозно предизвикателство. Обсъждат се последиците за теорията и практиката, като се подчертава необходимостта от нови концептуализации на времето в стратегическия анализ. Наред с това се отбелязват ограниченията на настоящото изследване и се очертават възможни направления за бъдещи научни разработки.

20. **Babanov, V.** (2026). Cybersecurity risks from AI–physical convergence, сп. "Knowledge International Journal", Vol. 74 No. 1 (2026): Knowledge in Practice, ISSN: 1857-923X (Printed), ISSN: 2545-4439 (Online), https://ojs.ikm.mk/index.php/kij/article/view/8104

Основната цел на настоящото изследване е да установи в каква степен текущата интеграция на изкуствен интелект във физически системи създава нови типове киберзаплахи. Освен това се цели да се покаже как съчетаването на ИИ и физически системи поражда уникални и трудно предвидими рискове за сигурността с потенциал за причиняване на реални физически щети. За постигането на тези цели е приложена концептуална рамка, основана на преглед на литературата, отбранителен анализ и моделиране на заплахи, чрез която са идентифицирани и категоризирани основните уязвимости при ИИ-физическите системи. Те включват системни уязвимости, уязвимости, свързани със злонамерен вход (adverse input), уязвимости при мрежови прониквания и уязвимости по веригата на доставки. Данните, събрани чрез казуси и документирани събития, като Stuxnet и пробиви в системи за автономни превозни средства, показват, че конвергенцията между ИИ и физически системи значително увеличава степента на неопределеност и създава условия за подвеждане на сензори (sensor spoofing), компрометиране на модели и прикрити противникови атаки. Допълнително се установява, че тази конвергенция притежава потенциал да доведе до физически повреди и оперативни сривове. Съществуващите парадигми на киберсигурност, ориентирани основно към информационните технологии, се оказват недостатъчни за защита на ИИ-физическите системи, особено когато те се използват в критична инфраструктура или в отбранителни приложения. Това се дължи на бързата ескалация на атаките и трудността при тяхната атрибуция. Сливането на

дигиталното и физическото измерение размива традиционните граници и налага преоценка на установените подходи за противодействие на киберзаплахи. В тази връзка се препоръчва разработването на защитни архитектури с многослойна структура, системи за откриване на аномалии в реално време, междудисциплинарни оценки на риска и проектиране на сигурни ИИ модели, с цел ограничаване на заплахите, произтичащи от конвергенцията между ИИ и физически системи. Освен това се подчертава, че киберсигурността не може да бъде разглеждана отделно от физическата безопасност при работа с подобни системи. Сред допълнителните препоръки са разработването на актуализирани модели на управление и включването на киберфизическата устойчивост в граждански и военни планове, за да се предотврати катастрофално използване на ИИ-базирани системи.

ABSTRACTS OF SCIENTIFIC PAPERS

Of chief-assistant professor Vladimir Babanov, Ph.D.

Presented for participation in a competition for the academic position of **"Associate Professor"** in Professional Field 9.1. **"National Security"**, at **South-West University "Neofit Rilski" – Blagoevgrad**, announced in the State Gazette (SG), issue no. 107 of 12.12.2025.

1.Monograph:

V. Babanov (2026), **"The Impact of Generative Artificial Intelligence on the Concept of Cybersecurity,"** University Publishing House "Neofit Rilski," Blagoevgrad. ISBN: 978-954-00-0446-4

The monograph "The Impact of Generative Artificial Intelligence on the Concept of Cybersecurity" presents an interdisciplinary study devoted to the transformative influence of generative artificial intelligence (AI) on the theoretical foundations, strategic dimensions, and practical mechanisms of cybersecurity. The research is situated within the context of accelerated digital transformation following 2022, when the public availability of large language models demonstrated that AI has evolved from an experimental technology into a structural factor shaping economic systems, governance, and security. The central thesis maintains that generative AI does not merely introduce new tools into the cyber domain but fundamentally reshapes the philosophy of security, requiring a reassessment of established principles and approaches.

The primary objective of the study is to examine the impact of generative AI on the core principles of cybersecurity and on the dynamics of next-generation cybercrime, while outlining opportunities for integrating this technology into modern cyber defense architectures. The object of analysis is cyberspace as an environment in which intelligent systems, institutions, and malicious actors interact. The subject of the study concerns the effects of generative models on cybersecurity principles, practices, and the balance between offensive and defensive capabilities. Methodologically, the research applies comparative analysis of regulatory frameworks and strategic documents, critical review of academic and expert literature, case study methods, and conceptual modeling.

The first chapter examines classical cybersecurity concepts and their evolution under the influence of generative AI. Particular attention is devoted to the confidentiality, integrity, and availability (CIA) triad as the cornerstone of information security. It is argued that generative models introduce new risks to confidentiality through the potential reproduction of sensitive data, to integrity through the creation of highly convincing synthetic content, and to availability through automated exploitation of vulnerabilities. At the same time, it is emphasized that the same technology may support dynamic risk management, simulation modeling, and early anomaly detection.

The principles of defense in depth and zero trust are analyzed within the context of highly interconnected and automated digital environments. The growing integration of AI into cloud and hybrid infrastructures is shown to expand the attack surface while simultaneously enabling continuous monitoring and adaptive responses. The principles of least privilege and separation of duties are also reconsidered in light of autonomous AI agents. The concept of "machine-based separation of duties" is introduced as a means of preventing excessive concentration of access rights and functional authority within automated systems.

Significant attention is devoted to security by design and the Keep It Simple and Secure (KISS) principle, both of which gain renewed relevance in increasingly complex digital ecosystems. The integration of generative AI requires the embedding of security mechanisms from the earliest stages of system design and clear regulation of algorithmic roles within organizational processes. The study further explores incident response, business continuity, and disaster recovery, outlining the potential of AI to enhance scenario simulations, impact assessments, and recovery planning.

The second chapter addresses generative AI as a catalyst for next-generation cybercrime. The technology is examined as a strategic advantage for malicious actors due to its adaptability, scalability, and low barrier to entry. Specific forms of misuse are analyzed, including highly personalized phishing and social engineering campaigns, automated malware generation and optimization, deepfake creation, and AI-driven reconnaissance and vulnerability scanning. The existence of structured illicit markets offering AI-based tools and services further lowers the threshold for cybercriminal activity and increases operational sophistication.

Advanced persistent threats (APTs) are examined, including collaboration between state-sponsored groups and criminal networks. Generative AI is identified as a factor

amplifying asymmetry in cyberspace and blurring the distinction between state and non-state actors. The geopolitical dimension of technological competition is emphasized, highlighting the strategic implications of AI dominance for national security and global power structures.

The third chapter explores the defensive potential of generative AI in cybersecurity practices. Applications are discussed in areas such as automation of analytical processes, threat hunting, anomaly detection, and integration with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems. It is argued that the optimal model of application is based on human–machine collaboration, where AI enhances analytical capacity and efficiency without replacing expert judgment or strategic oversight.

A central scientific and practical contribution of the study is the development of a conceptual framework for automated attribution of malicious activities to known hacker groups through the use of generative AI and cyber intelligence data. This framework aims to significantly reduce the time required for attribution and improve analytical effectiveness by combining large-scale algorithmic data processing with expert validation.

In conclusion, the monograph advances the necessity of a new cybersecurity paradigm grounded in adaptability, transparency, and strategic integration of AI technologies. Generative artificial intelligence is conceptualized as a dual-use phenomenon—simultaneously a source of emerging risks and a powerful instrument for their mitigation. The study outlines directions for future research and policy development in an era defined by rapid algorithmic transformation, growing technological interdependence, and the increasing reliance of national security systems on intelligent digital infrastructures.

2. Articles and papers published in scientific journals referenced and indexed in internationally recognized scientific databases.

1. G. Belova, G. Georgieva, Y. Kochev, A. Yankov, and **V. Babanov**, “COVID-19, INFODEMIC AND CYBER SECURITY”, ETR, vol. 5, pp. 57–61, Jun. 2025, doi: 10.17770/etr2025vol5.8479. https://archive-journals.rtu.lv/etr/article/view/5290

The article tries to trace the impact of some processes related to the COVID-19 pandemic on some areas of public life and on national security. The analysis focuses on two main points, namely the infodemic and cybersecurity, as during COVID-19 they stood out as

problems that will continue over time. The COVID-19 pandemic has been a challenge that requires the international community, governments, and political elites to address multiple dimensions that go beyond just the effects on population health and have an impact on security aspects. The starting point of the analysis is, of course, the social determinants of the right to health, which promote public health as an element of security and at the same time as one of the goals of sustainable development. In fact, it is precisely some of the determinants of the right to health that are subject to the infodemic, false or misleading information deliberately created to harm a person, social group, organization or country. Furthermore, the weaknesses of the pandemic have so far highlighted an urgent need for a stronger international framework that would counteract the spread of misinformation and increasing complexity of cyberattacks. That calls for an all-rounded strategy that includes increased international cooperation, public awareness, and the application of cutting-edge technical solutions. An appropriate methodology has been used in view of the delicate matter of health, which becomes even more vulnerable when subjected to infodemic or cybercrime. The main conclusion of the authors is that, in addition to improving international legislation with a view to preparing for and preventing future pandemics, more attention should also be paid to the phenomena that accompany them, such as the infodemic and cybercrime. This is of utmost importance, as they could be expected to develop on a much larger scale in possible future pandemics. The international community and national elites should discuss and take measures to deal with these phenomena.

3. Articles and papers published in non-indexed peer-reviewed journals or in edited collective volumes:

1. Babanov, V. (2024). "Internals of Defense-In-Depth Strategy in Cybersecurity," Security and Defense, vol. 2, pp. 37-42, Dec. 2024. https://doi.org/10.70265/PNEZ3158 DOI: https://doi.org/10.70265/PNEZ3158

The current paper explores the fundamentals of the defense-in-depth strategy in cybersecurity, emphasizing its importance for threat response in the dynamic security landscape. By implementing multiple layers of independent security controls across physical, technical, managerial, and operational domains, organizations can effectively mitigate risks and prevent cyberattacks. The strategy's adaptability makes it a robust framework for

addressing evolving cybersecurity challenges, offering a comprehensive method of protection against a wide range of threats.

2. **Babanov, V.** (2023). "The Military Conflict in Ukraine – Towards a New World Order or a Struggle for Russia's Survival." *Security and Defence*, (1), 212–222. ISSN 2815-4584 (Online), ISSN 2815-388X (Print). https://doi.org/10.70265/RXAG6807

The present article examines the impact of the war in Ukraine on the global order and on the future of Russia. Could the conflict trigger a chain reaction in other parts of the world and lead to the collapse of the "American world" and the decline of the West, or will the dilemmas facing the Russian Federation deepen, rendering its future increasingly uncertain? There are indications supporting the development of both scenarios, yet only one can ultimately prevail. Russia's actions in Ukraine undermine fundamental principles of contemporary international relations, which will either be upheld or give way to a dangerous precedent capable of destabilizing global security. For Bulgaria, these issues are of exceptional importance.

3. **Babanov, V.** (2025). "Digital Sovereignty and the United Nations – Between the Protection of National Security and International Cooperation in Cyberspace." In: *Contemporary International Communications and the Protection of Human Rights. The Role of the United Nations.* University Publishing House "Za bukvite – O pismeneh," Sofia, 2025, p. 61. ISBN 978-619-185-735-7. https://drive.google.com/file/d/1iLzqeAI4_jHwLd5CNn0YO6cMt3RflVUS/view

The present article examines the concept of digital sovereignty within the context of the international system and the role of the United Nations (UN) in managing cyberspace. In an era of global digitalization, national sovereignty takes on new significance, particularly in relation to internet governance and cybersecurity protection. The paper explores the conflicting approaches of leading geopolitical powers – such as Russia, China, and North Korea on one side, and democratic states on the other – and how their approach impact international cooperation.

4. **Babanov, V.** (2021). "The Global Security Environment and Contemporary Characteristics of the System of International Relations." *National Security Journal*, (9), 37–41. ISSN 2682-941X & ISSN 2682-9983. https://nacionalna-sigurnost.bg/broi-9/

The topic of the effects of COVID-19 on the world has unquestionably become a central focus for states and societies. The virus complicates the global security environment, yet the major processes inherent in the system of international relations have not ceased to develop. The article examines relations among the great powers of the 21st century, the hierarchy within the system, and its overall character—while the early signs of a multipolar world are visible, they do not in themselves guarantee such an outcome. Alongside the interaction among major centers of power, a significant number of global processes continue to influence international security.

5. **Babanov, V.** & Naseva, Yo. (2022). "Effects of the COVID-19 Pandemic on National and International Security." *Law, Politics, Administration*, 9(2), 1–7. https://lpajournal.swu.bg/wp-content/uploads/2022/09/Vladimir-Babanov-summary-BG.pdf

The COVID-19 pandemic continues to wreak havoc on all nation-states' systems. Since its inception, societies around the world have chosen a proactive approach to disease prevention and containment, which has led to a number of expected and unexpected effects. It is difficult to calculate the true value of tangible and intangible damage on a global scale, thus the current article focuses on three areas of great importance to national security - economy, healthcare and digitalization. Each of these areas is experiencing disparate effects, including positive ones, but one thing could be claimed with certainty - the COVID-19 pandemic has caused a massive global transformation.

6. **Babanov, V.** (2021). "Building a Comprehensive Cybersecurity System – A Priority for Bulgaria in the Present Decade." *Electronic Journal "Law, Politics, Administration"*, Vol. 8, No. 2/2021, pp. 46–52. ISSN 2367-4601 (Online). https://lpajournal.swu.bg/wp-content/uploads/2021/12/Vladimir-Babanov-br8-2.pdf

Cybersecurity has become an integral part of the broader study of security. This publication focuses on the process of building a cybersecurity system in the Republic of Bulgaria. The objective is for the country to develop, by 2030, a comprehensive cyber defense framework that will function as an integral component of the European Union's cybersecurity system. This common cybersecurity network serves as the starting point for EU member states in their efforts to respond to emerging threats in the digital environment.

7. **Babanov, V.** (2025) "Artificial Intelligence and Cybersecurity in Space Warfare", сп. „Международна политика", бр. 2, стр. 105-110; Retrieved from http://ip.swu.bg/mod/data/view.php?d=1&rid=739&filter=1 ; ISSN 2367-5373;

Space operations have been profoundly affected by the swift expansion of artificial intelligence (AI) into the realm of cybersecurity. The current paper examines leading contemporary research on the topic and explores the inevitable dual role of AI for both defense and offence in space warfare. It reveals the ways AI is implemented for advanced threat detection and response in orbit for an attempt to safeguard critical space apparatuses from cyberattacks. It becomes evident that robust and flexible technology as AI poses an extreme threat to space infrastructure, built decades ago. Malicious actors and states themselves scramble to both take advantage of their adversaries and protect their own vulnerable space hardware. Drawing upon the extensive work in the field, the paper discusses the technological challenges, the strategic imperatives and the lack of international governance framework necessary to lift the fog from the topic of the complex implications of AI on space security and subsequently of what appears to be a warfare. The analysis underscores the urgency for technical and legal frameworks to regulate the dangerous balance between AI, cybersecurity, and the growing stakes in the last frontier of strategic competition.

8. **Babanov, V.** (2024). "Disinformation in Cyberspace – A Threat to Democratic Processes in Southeast Europe." In: *Proceedings of the Round Table "Contemporary Dimensions of Security in Southeast Europe,"* organized by South-West University "Neofit Rilski" and the University of Library Studies and Information Technologies (ULSIT). Blagoevgrad: South-West University "Neofit Rilski," pp. 51–58. ISBN 978-954-00-0356-6. http://press.swu.bg/images/conf/collection_security_unibit.pdf

Disinformation has been used as a primary weapon in the struggle for geopolitical dominance between the great powers. The development of Internet and hi-tech have eased tremendously its spread and the Artificial Intelligence contributed to almost fully automating the process of disinformation of societies. The possibility of Internet ending up dominated by bots, disinformation and malicious actors in completely real- circumstance which worries South-East Europe countries due to their vulnerability. The current paper focuses on these processes.

9. **Babanov, V.** (2025), Strategic Considerations for AI-Enhanced Cybercrime, сп. „Право, Политика, Администрация", том 13, бр. 2/2025 г., с. 46-52, ISSN 2367-4601 (Online); Retrieved from https://lpajournal.swu.bg/wp-content/uploads/2025/12/1-Vladimir-Babanov.pdf

The current paper aims to outline some of the ways cybercriminals utilize Artificial Intelligence (AI) for malicious actions of perpetration. The effects of AI on cybercrime are also a focus together with the reasons behind the rapid proliferation of AI models. The outcome of such a merger between technology, criminal interests and economic incentive is impossible to predict, but entertaining several considerations for AI-enhanced cybercrime might provide valuable starting points for subsequent discussions.

10. **Babanov, V**. (2026) "AI-Enabled predictive diplomacy: data-driven approach to foreign policy", сборник „Международната система в преход. Нови парадигми на сигурността и дипломацията в дигиталната епоха." Издателство „За буквите- О писменехь", 2026 г., ISBN 978-619-185-793-7, (in press, official certificate submitted)

The current paper explores the concept of AI-enabled predictive diplomacy as a new phenomenon in the realm of foreign policy. By leveraging new and powerful technologyes, nation states could infer latent interests and behaviour patterns of their counterparts from vast amounts of seemingly unrelated information. The proposed framework shifts the focus of negotiations from passive reliance on BATNA towards proactive AI-enhanced strategy.The study demonstrates the upside potential of AI in negotiations while not neglecting the ethical boundaries it is pushing.

11. **Babanov, V.** (2026) “OSINT with AI for geopolitical conflict forecasting”, сборник „Международната система в преход. Нови парадигми на сигурността и дипломацията в дигиталната епоха.“ Издателство „За буквите- О писменехь“, 2026 г., ISBN 978-619-185-793-7, (in press, official certificate submitted)

The present paper is a survey of the AI-based OSINT theory in relation to strategic early warning systems. The paper describes how an AI may improve all of the different stages of the intelligence cycle from ingesting data to making forecasts, as well as the potential to improve the ability to strategically warn of conflicts. The paper also examines some key challenges to AI-based OSINT, such as data bias, limitations on models, lack of transparency or explainability of AI methods, and the warning-response gap as it relates to geopolitical instability modeling. Therefore, while AI-augmented OSINT has the potential to revolutionize geopolitical instability modeling, there must be a rigorous integration of human judgment and consideration of the technical and institutional constraints before that potential is realized.

12. **Babanov, V.** (2026). „Synthetic reality as a strategic threat: from disinformation to predictive manipulation“. E-Journal VFU, 25, 84-93. Издателски център на ВСУ "Черноризец Храбър", ISSN 1313-7514, https://ejournal.vfu.bg/index.php/vfu/article/view/261

The article examines the potential of artificial intelligence to transform disinformation into a sophisticated type of synthetic reality operating on hyper-personalized manipulation and cognitive exploitation. Synthetic reality is fundamentally different from traditional forms of propaganda as it is deeply immersive, far more persistent, and has the capacity to influence the decisions and behaviours of individuals and societies. The discussion explores how synthetic media undermine strategic trust, while creating a lasting threat bypassing conventional detection and defense mechanisms. The paper identifies significant gaps in preparedness in terms of law, technology and doctrine and concludes by identifying policy and resilience based solutions for dealing with these evolving challenges.

13. **Babanov, V**., (2026). „Ai-enhanced counter-offensive decision-making in hybrid warfare.“ E-Journal VFU, 25, 94-102. Издателски център на ВСУ "Черноризец Храбър",ISSN1313-7514, https://ejournal.vfu.bg/index.php/vfu/article/view/262

In this article the use of artificial intelligence (AI) is being explored as a method for enhancing counter-offensive decision making within a hybrid warfare environment. It is defined as an area where the intersection of conventional military tactics and other forms of warfare, such as cyber warfare, information warfare and psychological warfare, occur. Hybrid warfare creates conditions of uncertainty, urgency and high levels of asymmetry which necessitates effective and timely decision-making. The research demonstrates that the use of AI may provide enhanced support for counter-offensive planning by reducing decision cycle time, providing support for the integration of multiple domain data and by enhancing situational awareness using analytical tools and decision-support systems. The research identifies the benefits of AI enabled decision-making but also points out the existing limitations. It concludes that AI could be most effective when used as part of a balanced human-machine system whereby AI provides support for data driven decision-making processes and humans maintain strategic judgment and accountability.

14. **Babanov, V.** (2026). „Artificial intelligence in anti-money laundering and the questions of explainability, privacy and trust.“ сп. „Право, Политика, Администрация”, том 13, бр. 1/2026 г., ISSN 2367-4601 (Online); (in press, official certificate submitted)

The current paper aims to explore the transformative capabilities of artificial intelligence to enhance money laundering detection and prevention. It synthesizes the research on AI-driven financial fraud detection and focuses on the roles of explainable artificial intelligence for transparency and regulatory compliance. The paper also turns attention on Federated Learning for privacy-preserving data analysis. Further, it is discussed what factors can balance the relationship between illicit finance detection, data privacy, and user trust. A conclusion is drawn with a summary of key benefits and challenges to integrating artificial intelligence into anti-money laundering frameworks.

15. **Babanov, V**. (2026). The ascending techno-nationalism in the U.S.– China rivalry and the EU's technological independence., сп. „Международна политика“, бр. 1, 2026 г.; ISSN 2367-5373; (in press, official certificate submitted)

The rise of techno-nationalism is a key factor in defining the U.S.-China technological rivalry and it shapes the way the European Union pursues technological independence. Techno-nationalism has defined the way the U.S. and China are chasing strategic dominance through emerging technologies like AI, semiconductors, and cloud computing. This study argues that although the EU seeks to achieve digital sovereignty, it faces challenges from its fragmented industrial base, slow innovation cycle and reliance on foreign developed technologies in critical areas. The findings of this study emphasize the importance of developing the EU's industrial policy and increasing innovation capacity in addition to achieving regulatory objectives in order to maintain strategic autonomy in a rapidly changing world technology order.

16. **Babanov, V.** (2026). „Fractured cyberspace and digital disorder as a strategic threat to international security“, сп. сп. „Международна политика“, бр. 2, 2026 г.; ISSN 2367-5373; CEEOL; Национален референтен списък; (in press, official certificate submitted)

The article envisions a further development of "Splinternet," where digital chaos increases exponentially. The article focuses on uncontrolled rise of cybercrime, unmitigated distortions of reality through disinformation and synthetic personas. The research looks into the efforts of nations to pursue digital sovereignty to the detriment of global connectivity. The fracturing of the Internet is boosting the ability of the malevolent actors to undermine its stability. The article illustrates how the lack of international cooperation deteriorates the current tendencies.

17. **Babanov, V.** (2026). „Automated threat actor profiling with AI in cyber threat intelligence: a framework for real-time extraction and attribution“, сп. „Образование, научни изследвания и иновации“, година 4, книжка 1, март 2026, ISSN 2815-4630, CEEOL, CrossRef, Национален референтен списък (in press, official certificate submitted)

Cyber threat intelligence (CTI) has become essential for a proactive defense against adversaries in cyberspace. However, the majority of valuable information resides in vast volumes of unstructured data and feeds, which renders their analysis an extremely lengthy and error-prone process. This paper aims to present a real-time automated framework that utilizes Natural Language Processing (NLP) and standardized ontologies such as Structured Threat Information Expression (STIX) v2.1 and MITRE ATT&CK to identify indicators of compromise (IoCs), tactics, techniques and procedures (TTPs) from multiple CTI sources and correlate them with a threat actor profile. The approach described in it digests data from open-source threat reports, social media and other sharing platforms. It also uses domain-specific language models and rule-based analyzers to identify entities (e.g. malware, tools, targets), mapping them to STIX objects and linking extracted TTPs to ATT&CK techniques. The framework is tested with a hypothetical ransomware case study, which displays how extracted indicators, killchain stages and behavioural patterns could be associated with a threat-actor profile. The results demonstrate that the suggested AI-driven pipeline could enormously reduce the manual effort in CTI processing, maintaining high extraction accuracy. The work lays the foundation for implementing automatic CTI profiling of adversaries aiding with proactive defense and attribution efforts.

18. **Babanov, V.** (2026). „Delegating cyber defense to algorithms: the legal boundaries of autonomous response in Bulgaria“, сп. „Образование, научни изследвания и иновации“, година 4 , книжка 2, юни 2026, ISSN 2815-4630, (in press, official certificate submitted)

The article examines the legal implications of autonomous response mechanisms in the Bulgarian cyber defense system. It analyzes Bulgaria's legal framework and observes it into the broader context of NATO and EU’s strategic documents. The article defines and studies the legal viability of autonomous cyber response, highlighting how automated defensive actions challenge existing legal standards. The evolution of Bulgaria's cyber defense posture is documented, beginning with early cyber defense strategies and through to the most recent alignment of the EU directives and NATO requirements. The discussion reveals that the Bulgarian law does not provide specific legal authorization for automated counter-measures in the case of cyber-attacks. The lack of legal authorization creates theoretical and compliance issues. The article concluded that while the national law of Bulgaria provides a comprehensive

base to address cybercrime and protect critical infrastructure, there are challenges to incorporate autonomous cyber responses into existing legislation. It is based on the clear presumption that development of any strategy requires compatibility with the international obligations of the country

19. **Babanov, V.** (2026) Cybertime as a battlefield and the end of sequential military strategy; сп. Национална сигурност (9), 46-49. https://nacionalna-sigurnost.bg/broi-23/ ISSN 2682-941X & ISSN 2682-9983. https://nacionalna-sigurnost.bg/broi-23/

Time is being used as a battlefield within modern conflicts. Decision making processes, accelerated by cyber-AI technologies, have been compressed to disrupt the traditional definitions of what constitutes warfare. As the tempo of conflict increases, models based upon orderly sequential decision cycles such as the OODA loop or campaign phases, will continue to grow out of sync with the realities of high-speed anticipatory warfare. Therefore, the sequential framework in military strategy is being challenged. The implications for theory and practice are discussed and the necessity for new conceptions of time in strategy is emphasized. In addition, the current study's limitations are noted and areas of potential future research are suggested.

20. **Babanov, V.** (2026). Cybersecurity risks from AI–physical convergence, сп. "Knowledge International Journal", Vol. 74 No. 1 (2026): Knowledge in Practice, ISSN: 1857-923X (Printed), ISSN: 2545-4439 (Online), https://ojs.ikm.mk/index.php/kij/article/view/8104

The primary goal of this research is to identify the extent to which ongoing artificial intelligence integration into physical systems creates new types of multidomain cyber threats. It also aims to illustrate how the combination of AI and physical systems creates unique and unpredictable security risks with the potential to cause physical harm. In order to accomplish these objectives, a conceptual framework based on literature, defense analysis and threat modeling was applied to identify and categorize the major vulnerability areas in AI-physical systems such as systemic vulnerabilities, adverse input vulnerabilities, network intrusion vulnerabilities, and supply chain vulnerabilities. Data collected through case studies and documented events such as Stuxnet and hacking of autonomous vehicle systems, indicated that

AI-physical system convergence significantly increases uncertainty and therefore allows for sensor spoofing, model corruption and stealthy adversarial attacks. Additionally, these data indicate that AI-physical system convergence has the potential for causing physical damage and operational failure. Current Information Technology-centric cybersecurity paradigms are inadequate for protecting AI-physical systems, particularly when those systems are used within critical infrastructure or defense applications due to the rapid escalation of attacks and the difficulty of attributing them to a specific party. The convergence of AI and physical systems blurs the distinctions between digital and physical and forces a reevaluation of traditional responses to cyber threats. Therefore, it is recommended that the development of defensive architectures that include multiple layers, real-time anomaly detection, cross-discipline risk assessments, and the design of secure AI models be employed to mitigate the threats associated with AI-physical system convergence. Further, policymakers and industry stakeholders should recognize that cybersecurity cannot be separated from physical safety when dealing with AI-physical systems. Additional recommendations in the study include the development of updated governance models and the inclusion of cyber-physical resilience in military and civilian plans to prevent catastrophic exploitation of AI-based systems.