Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Project „Misijomis grįstų mokslo ir inovacijų programų įgyvendinimas“ (Project Nr. 02-002-P-0001) report

Project name: ***HIPSTER***

Responsible/Implementation partner (-s): ***MRU***

Action result: ***HIPSTER Regulatory Mapping Report***

Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Editor
<main editor>

Contributors
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)

Reviewers
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view. The users use the information at their sole risk and liability.

AI-assisted tools were used to support the drafting, structuring and linguistic refinement of this document. The final content was reviewed and approved by the authors, who remain responsible for its accuracy, integrity and suitability for use. The use of AI-assisted tools was limited to preparatory and editorial support and was not intended to infringe, misappropriate or otherwise affect any third-party proprietary, confidential, copyrighted or otherwise protected rights or materials.

Executive Summary

This report provides a regulatory mapping for HIPSTER, an AI-supported system designed to detect and analyse hybrid threats, including cyberattacks, disinformation, societal manipulation and hostile influence activities. It shows that HIPSTER operates across several legal and operational domains, meaning that compliance cannot be assessed under one framework alone.

The analysis identifies the main EU and national regulatory regimes relevant to HIPSTER, including data protection, AI governance, cybersecurity, platform regulation, criminal law, intelligence law, public information rules and fundamental rights protection. A central finding is that the applicable obligations depend on the deployment context: civilian and research use, law-enforcement usee and national-security and defense use.

The report also highlights that HIPSTER must be designed as a decision-support tool rather than an autonomous decision-making system. Human oversight, explainability, auditability, data minimisation, purpose limitation, secure data handling and clear separation between factual observations and analytical assessments are part of the distinguished essential safeguards.

The ethical and societal assessment further confirms that responsible deployment requires more than legal compliance. Ethical governance, bias testing, societal impact assessment, stakeholder engagement, cybersecurity-by-design and transparency are necessary to ensure public trust and protect fundamental rights.

Overall, this report concludes that HIPSTER can offer important scientific and practical value for hybrid-threat resilience, provided that regulatory compliance and ethical safeguards are embedded into the system's architecture, governance and operational use from the outset.

Table of Contents

List of Figures

No table of figures entries found.

List of Tables

No table of figures entries found.

1. Introduction

The HIPSTER project, titled "Hybrid Information Psychological Societal Threats Handling System for Public Security Domain Practitioners, Businesses and Education," aims to develop an advanced technological solution to address the complex nature of hybrid threats. Hybrid threats, characterized by a combination of cyber-attacks, disinformation campaigns and societal manipulation, pose significant challenges to public security and national resilience. These threats exploit vulnerabilities in digital infrastructure, public perception, and information systems, necessitating a comprehensive, cross-disciplinary approach to detection and response.

The project is a collaborative effort involving NOVIAN Technologies (**NOVIAN**), L3CE, Kaunas University of Technology (**KTU**), Vilnius Tech and Mykolas Romeris University (**MRU**). Each partner brings specialized expertise in cybersecurity, artificial intelligence (**AI**), machine learning, legal regulation, and social sciences. This interdisciplinary team aims to develop the HIPSTER system, an innovative platform that integrates advanced AI, Open-Source Intelligence (**OSINT**), Social Media Intelligence (**SocMINT**), and Natural Language Processing (**NLP**) to automatically detect, attribute and counter hybrid threats in real time.

The HIPSTER system is aimed to be designed to operate continuously, providing 24/7 monitoring and analysis capabilities for public security practitioners, businesses, and educational institutions. It will address key areas of concern, including the detection of hate speech, radical content, extremist communication patterns, and the identification of new online spaces used for propaganda and disinformation. By advancing the state-of-the-art (**SOTA**) in threat detection and attribution, HIPSTER aims to set new standards in the management of hybrid threats, contributing to the security and resilience of societies at both national and European levels.

This document provides a comprehensive regulatory analysis, comparison and ethical and social aspects requirements definition for similar systems as developed under the HIPSTER project. It examines the relevant regulatory frameworks from Lithuania, the European Union, and NATO, with a focus on compliance with data protection laws AI ethics, and cybersecurity standards as well as other regulatory frameworks applicable to hybrid information psychological societal threats handling systems (**Systems**). Key regulations examined include the EU's General Data Protection Regulation (**GDPR**), the Artificial Intelligence Act (**AI Act**), the Digital Services Act (**DSA**), EU and national cybersecurity regulation framework as well as other EU-level legislation and NATO's Strategic Concept.

This report maps the main hard-law requirements relevant to HIPSTER and Systems for hybrid threat detection and analysis. Non-binding guidance, soft law, policy documents and case-law analysis are addressed separately, where they may support interpretation and implementation but should not be presented as binding legal requirements in this section. The mapping is non-exhaustive and should be treated as a living document. The regulatory environment for AI, cybersecurity, data protection and hybrid-threat response is evolving rapidly. In addition, the applicable legal framework depends on the system's deployment context, the operator, the purpose of use, the type of data processed and the potential impact of system outputs. The report should therefore be reviewed and updated following operational settings and legal developments.

2. DOA, SOTA and Context

A. Introduction to Hybrid Threats

Hybrid threats are a complex and evolving challenge characterized by the use of a wide range of hostile actions, including cyber-attacks, disinformation, and psychological operations, often conducted in concert by state or non-state actors. These threats aim to exploit the vulnerabilities of target societies by blending conventional and unconventional tactics, thus blurring the lines between peace and conflict. The multidimensional nature of hybrid threats necessitates a comprehensive approach to detection, attribution, and response, involving cross-sectoral and interdisciplinary collaboration.

The literature on hybrid threats has expanded significantly in recent years, reflecting the growing recognition of their impact on national and international security. Key studies emphasize the need for integrated strategies that encompass technological, legal, and social dimensions, addressing not only the technical aspects of threat detection but also the broader ethical and regulatory implications.

B. State-of-the-Art in Threat Detection: OSINT and SocMINT

Open-Source Intelligence (OSINT) and Social Media Intelligence (SocMINT) have emerged as critical tools in the detection and analysis of hybrid threats. OSINT involves the collection and analysis of publicly available information from diverse sources, including social media, news outlets, and public records, to identify potential threats and malicious activities. SocMINT, a subset of OSINT, specifically focuses on social media platforms, leveraging real-time data to track the spread of disinformation, radical content, and other forms of online manipulation.

Recent advancements in OSINT and SocMINT have been driven by developments in machine learning and natural language processing (NLP), which enable automated analysis of large volumes of data. Studies such as those by Li et al. (2021) highlight the potential of AI-driven OSINT tools to enhance situational awareness and provide actionable intelligence for security practitioners. However, challenges remain in terms of data quality, ethical considerations, and the need for advanced algorithms that can accurately distinguish between legitimate and malicious content.

The HIPSTER project aims to advance the state-of-the-art in OSINT and SocMINT by developing new models and methodologies for real-time threat detection and attribution. By integrating AI-driven tools with robust data processing capabilities, HIPSTER seeks to address existing gaps in the accuracy, efficiency, and scalability of current systems, providing a comprehensive solution that can operate continuously to detect and counter hybrid threats.

C. Natural Language Processing (NLP) and AI in Hybrid Threat Detection

NLP and artificial intelligence (AI) are at the forefront of efforts to enhance the detection and attribution of hybrid threats. NLP enables the automated analysis of textual data, including the identification of hate speech, extremist content, and coordinated disinformation campaigns. AI algorithms, particularly those based on machine learning, can be trained to recognize patterns of malicious activity, making it possible to detect and respond to threats in real time.

A significant body of research, including the work of Zhang and Luo (2022), has explored the use of NLP and AI in security applications, demonstrating the potential of these technologies to improve the speed and accuracy of threat detection. However, there are ongoing challenges related to the interpretability of AI models, the risk of bias in algorithmic decision-making, and the ethical implications of automated surveillance.

The HIPSTER project addresses these challenges by incorporating the latest advancements in NLP and context-driven AI applications. The system will use AI to automate the detection of various types of harmful content, including hate speech, radical content, and extremist communication schemas. By staying at the forefront of these technological developments, HIPSTER aims to provide a solution that not only detects threats effectively but also adheres to ethical standards and regulatory requirements.

D. Case Studies and Real-World Applications

To provide context for the HIPSTER project and broader deployment of Systems, several case studies of hybrid threat detection and response in real-world scenarios are examined. These include the use of OSINT and AI-driven tools by law enforcement agencies, government bodies, and private sector organizations to counter disinformation and protect critical infrastructure. For example, the European External Action Service (EEAS) has implemented strategies that leverage advanced data analytics to monitor and counteract foreign information manipulation (EEAS, 2020).

These case studies highlight both the potential and the limitations of current approaches, underscoring the need for more integrated and adaptable systems like HIPSTER.

E. Identifying Gaps and Advancing the State-of-the-Art (continued)

While advancements in OSINT, SocMINT, NLP, and AI have enhanced capabilities in hybrid threat detection, there are several key gaps that need addressing to develop a truly comprehensive system. One of the primary challenges is the lack of standardized frameworks for threat attribution, particularly in distinguishing between state-sponsored actions and non-state actors. This gap complicates the response strategies for public security practitioners and hinders coordinated international efforts against hybrid threats.

Additionally, current systems often struggle with the integration of diverse data sources, which include structured and unstructured data from social media, public records, and private communications. The sheer volume and complexity of data require advanced algorithms capable of real-time processing and analysis. However, many existing solutions are limited by their reliance on rule-based approaches, which lack the flexibility and adaptability required to keep pace with rapidly evolving threat landscapes.

Another critical gap lies in the scalability of current detection systems. As hybrid threats increase in frequency and sophistication, there is a growing need for platforms that can scale their operations to handle larger datasets without compromising performance. This is particularly relevant for public security domains, where timely responses can significantly impact the effectiveness of countermeasures.

The HIPSTER project aims to fill these gaps by developing new threat detection and attribution models that leverage recent advancements in AI, machine learning, and big data analytics. By incorporating a modular architecture, Systems have to be designed to scale dynamically, adapting to varying data loads and operational demands. This scalability is essential for ensuring that the system remains effective in diverse scenarios, from localized threats to large-scale information operations.

Furthermore, the project will place a strong emphasis on enhancing the interpretability and transparency of AI models used in threat detection. Given the ethical concerns surrounding AI-driven surveillance, it is crucial that the algorithms employed are not only accurate but also explainable. This approach will help mitigate the risk of false positives and ensure that decisions made by the system are justifiable and align with established legal standards.

Systems also need to address the need for improved data integration by employing advanced data fusion techniques. These techniques will allow the system to combine information from various sources, providing a more comprehensive view of potential threats. The project explores the use of graph-based models and other innovative approaches to represent complex relationships within the data, enabling more accurate and actionable insights.

By advancing the state-of-the-art in hybrid threat detection and attribution, HIPSTER aims to provide a powerful tool that enhances the ability of public security practitioners to manage the complex and evolving nature of modern threats. The project's interdisciplinary approach, combining insights from cybersecurity, artificial intelligence, social sciences, and legal studies, ensures that the resulting solution is not only technically robust but also ethically sound and legally compliant.

3. Regulatory Mapping Approach

HIPSTER is designed for a threat environment in which hostile activities do not fall neatly into a single legal, technical or institutional category. As described above, hybrid threats combine cyber operations, disinformation, foreign information manipulation, societal polarisation, covert influence, hostile intelligence activity and, in some scenarios, preparatory or accompanying military action. A system capable of detecting and analysing such activity therefore cannot be assessed under a single regulatory instrument. Its legality depends on who deploys it, for what purpose, what data it processes, whether it supports civilian, law-enforcement, intelligence or defence functions and whether its outputs produce legal or similarly significant consequences for individuals.

The scientific significance of this regulatory mapping lies in treating compliance not as an external checklist but as part of the system architecture. HIPSTER-like systems operate at the intersection of AI governance, data protection, cybersecurity, public security, criminal law, media regulation, intelligence law and fundamental rights. The novelty of the mapping is therefore twofold. First, it identifies the regime-sensitive nature of hybrid-threat technologies: the same technical capability may fall under different legal regimes depending on deployment context. Secondly, it translates this regulatory complexity into design implications.

This section provides a non-exhaustive but operationally applicable overview of the regulatory landscape relevant to HIPSTER-like systems in the European Union, Lithuania and NATO-related security contexts. Lithuanian law is used as an illustrative national case study because HIPSTER's anticipated use cases are closely connected to public security, national resilience and hybrid-threat response in this EU Member State particularly exposed to hybrid activity.

4. Fundamental Rights Protection

Any HIPSTER-like system must be developed against the baseline of fundamental rights protection. At European level, the relevant sources include the European Convention on Human Rights[1] and the Charter of Fundamental Rights of the European Union.[2] At national level, constitutional protections, including those in the Constitution of the Republic of Lithuania, remain primarily important. These instruments protect, among other rights, private life, personal data, freedom of expression, non-discrimination, effective remedy and due process.

This baseline is particularly important because hybrid-threat detection systems may process large volumes of publicly available but personally identifiable information. OSINT and SOCINT data may contain names, handles, images, location information, political opinions, religious beliefs, social relationships and behavioural patterns. The fact that data is publicly accessible does not remove it from the scope of rights protection. In addition, automated or AI-supported classification of content, narratives, accounts or behavioural patterns may affect freedom of expression where false positives lead to escalation, content restriction, surveillance, investigation or reputational harm. Profiling and behavioural inference may also create discrimination risks if protected characteristics are directly or indirectly used as indicators of threat.

The main design consequence is that HIPSTER must function as a decision-support system, not as a system for autonomous legal determination. It should support human analysts, competent authorities and decision-makers by structuring evidence, identifying patterns and indicating uncertainty. It should not replace contextual legal assessment, especially in areas involving political speech, journalistic activity, satire, activism, minority expression or borderline conduct.

[1] European Convention on Human Rights, available at: https://www.echr.coe.int/documents/d/echr/convention_eng.

[2] Charter of Fundamental Rights of the European Union, available at: https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng.

5. European Union Law Framework

A. General Data Protection Regulation

Where HIPSTER is developed or deployed by research institutions, private entities, public bodies acting outside criminal-law enforcement, or other civilian actors, the General Data Protection Regulation (**GDPR**)[3] is the foundational legal framework for personal data processing. The GDPR applies to all data processing operations – e.g., personal data processed in OSINT collection, social-media monitoring, account and behavioural analysis, validation and testing datasets and others.

While the GDPR would apply in full scope, several GDPR concepts could be mentioned here as primarily relevant. E.g., Article 5 requires lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability. Article 6 requires a lawful basis for processing. Depending on the actor and use case, the relevant basis may be performance of a task carried out in the public interest, compliance with a legal obligation, or legitimate interests, although public authorities cannot rely on legitimate interests for processing carried out in the performance of their public tasks. Where special categories of data arise, Article 9 requires an additional condition, such as manifest public disclosure by the data subject or processing necessary for reasons of substantial public interest based on the EU or national law.

Under the GDPR, data subjects have several rights including the rights to information, access, rectification, erasure, restriction of processing, data portability, objection and protection against certain solely automated decisions. For HIPSTER, these rights are particularly important because the system may process OSINT/SOCINT data, infer behavioural patterns or generate threat-related assessments involving identifiable individuals. System design should therefore enable controllers to respond to data-subject requests, correct inaccurate data, restrict or delete data where required and explain relevant processing in a meaningful way. At the same time, some rights may be restricted where permitted by law, for example to protect public security, criminal investigations or national security. Any such restriction must be lawful, necessary, proportionate and properly documented.

HIPSTER-like systems will almost undoubtedly trigger the need for a Data Protection Impact Assessment (**DPIA**) under Article 35. This is because such systems may involve systematic monitoring, profiling, large-scale processing of publicly accessible data, special-category data, innovative technology and potentially significant effects on individuals. A DPIA should assess all the possible risks, including but not limited to misclassification, unjustified inference, chilling effects, bias, excessive retention, function creep and unauthorised disclosure. It should also specify state of the art safeguards, including but not limited to pseudonymisation, access controls, role-based permissions, human review, accuracy testing, explainability mechanisms, retention limits and incident-response procedures.

Article 25 GDPR is especially important for HIPSTER because it requires data protection by design and by default. This means that privacy and data-protection principles must be embedded at the point when processing means are determined, not added after deployment. For HIPSTER, this implies architectural controls including but not limited to purpose-based data segmentation, separation of training and operational datasets, minimisation of identifiers, documented legal bases, configurable retention periods and audit logs.

Where threat-intelligence outputs are shared with other parties, independent controller, joint-controller and processor roles must be determined in advance. Article 26 applies to joint controllership, while Article 28 applies to processor arrangements. International data transfers outside the European Economic Area must comply with Chapter V GDPR. Security obligations under Article 32 require appropriate technical and organisational measures, including encryption, pseudonymisation, confidentiality, resilience, restoration capability and regular testing.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Member States may also have relevant national laws that supplement or specify EU-level requirements. These national frameworks are important because HIPSTER's obligations may depend not only on EU law, but also on the country of deployment and the competent authority involved. In Lithuania, for example, the Law on Legal Protection of Personal Data supplements the GDPR by establishing national procedural and supervisory rules.

B. Law Enforcement Directive

The Law Enforcement Directive (**LED**)[4] applies when personal data is processed by competent authorities for the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, or safeguarding against threats to public security. This is a narrower and purpose-specific framework. It does not apply simply because a system concerns security; it applies when the actor and purpose fall within the LED.

For HIPSTER, this distinction is operationally significant. A civilian research deployment, a platform-support deployment and a police deployment may involve similar technical functions but different legal regimes. Where a competent authority uses HIPSTER for criminal-intelligence or investigative purposes, the system should operate in a clearly separated law-enforcement mode.

In that mode, the LED's principles of lawfulness, fairness, purpose limitation, data minimisation, accuracy and storage limitation must be reflected in the technical architecture. While the same principles are established in the GDPR, such principles under the LED mode should have the LED purposes in mind. Additionally, Article 7 of the LED requires a distinction, as far as possible, between personal data based on facts and personal data based on personal assessments. This is highly relevant for AI-supported threat analysis. HIPSTER should therefore, for example, label outputs as factual observations, inferred assessments, probability scores, analyst conclusions or intelligence leads, rather than presenting all outputs as established facts.

Article 10 LED governs special categories of data. Political opinions, religious beliefs, ethnic origin and similar attributes may arise frequently in information-environment monitoring. Under the LED, such processing is permitted only where strictly necessary, subject to appropriate safeguards and where authorised by the EU or national law or otherwise permitted under the LED. Article 11 restricts solely automated decisions producing adverse legal effects or significantly affecting individuals, unless authorised by law and accompanied by safeguards.

Articles 25 and 29 are also essential. Article 25 requires logging of processing operations, while Article 29 requires appropriate security measures. HIPSTER should therefore provide tamper-evident logs, traceability of queries, records of access and disclosure, role-based access, secure authentication, encryption, retention controls and supervisory review capabilities.

The LED does not apply directly in the same way as an EU regulation. As a directive, it must be transposed into national law by each Member State. Therefore, where HIPSTER-like systems are used by competent authorities for the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, or safeguarding against threats to public security, the applicable rules will be found in the relevant national law implementing the LED. In Lithuania, the LED is implemented through the Law of the Republic of Lithuania on the Legal Protection of Personal Data Processed for the Prevention, Investigation, Detection or Prosecution of Criminal Offences, the Enforcement of Penalties or National Security or Defence Purposes.

C. National security, defence and intelligence boundary

[4] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, available at: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng.

National security remains a particularly sensitive boundary in EU law. Article 4(2) of the Treaty on European Union[5] states that national security remains the sole responsibility of each Member State. The GDPR excludes processing in the course of activities falling outside the scope of the EU law, and the AI Act contains an express exclusion for AI systems placed on the market, put into service or used exclusively for military, defence or national-security purposes.

This does not mean that HIPSTER-like systems used for national security are unregulated. Rather, their regulation shifts primarily to constitutional law, national intelligence law, sector-specific security law, classified-information rules, parliamentary or specialised oversight and human-rights obligations. The practical implication is that HIPSTER should be designed to support different legal operating environments, rather than assuming that one compliance model applies universally.

D. Artificial Intelligence Act

The EU Artificial Intelligence Act[6] is a central regulatory layer for HIPSTER where the system is not used exclusively for military, defence or national-security purposes. The Act entered into force in August 2024 and establishes a risk-based framework for AI systems in the EU.

HIPSTER-like systems may fall within the high-risk category where deployed in law-enforcement, public-security, border-management, critical-infrastructure, migration or other Annex III contexts. The precise classification depends on the specific use case. A research prototype, a platform-monitoring tool, a law-enforcement analytical system and a national-security deployment should therefore be assessed separately.

If classified as high-risk, HIPSTER would need to comply with requirements including a risk-management system, data governance, technical documentation, record-keeping, transparency and instructions for use, human oversight, accuracy, robustness and cybersecurity. These requirements are not merely documentary. They require measurable design and governance controls: validated datasets, bias testing, performance monitoring, known limitation statements, adversarial robustness measures, operator training and post-market monitoring.

The AI Act also requires attention to prohibited practices. HIPSTER should not be designed or deployed in a manner that enables unlawful social scoring, manipulative techniques, impermissible biometric categorisation, prohibited predictive policing practices or indiscriminate surveillance incompatible with the Act. Where outputs may affect individuals, the system must preserve meaningful human assessment and avoid converting probabilistic indicators into automatic enforcement outcomes.

For public-sector deployment, the Fundamental Rights Impact Assessment (**FRIA**) requirement is particularly relevant. A FRIA should consider effects on privacy, data protection, freedom of expression, non-discrimination, effective remedy and democratic participation. For HIPSTER, the FRIA should be coordinated with the DPIA where personal data processing is involved, while remaining analytically distinct: the DPIA focuses on data-protection risks, whereas the FRIA captures broader fundamental-rights impacts.

E. Digital Services Act

The Digital Services Act (**DSA**)[7] does not primarily regulate HIPSTER as a public-security or law-enforcement tool. Its primary addressees are intermediary services, hosting services, online platforms,

[5] The Treaty on European Union, available at: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

[7] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng.

very large online platforms and very large online search engines. However, it becomes relevant if HIPSTER-like system's outputs would be used to support platform governance, content moderation, trusted-flagger activity, risk assessment or mitigation of disinformation-related systemic risks.

If HIPSTER-generated alerts are submitted to platforms as notices, the DSA requirements must be carefully reviewed. For example, Article 16 DSA requires notices to be sufficiently precise and adequately substantiated. The system should therefore preserve source evidence, timestamps, reasons for classification, confidence levels and any human validation. Where platform action is taken, Article 17 statements of reasons and Article 20 internal complaint-handling obligations may require explanations that are understandable to affected users. HIPSTER should therefore support auditability and explanation rather than opaque flagging.

For very large online platforms and search engines, Articles 34 and 35 require assessment and mitigation of systemic risks, including risks linked to civic discourse, electoral processes, public security and disinformation. HIPSTER may support such risk analysis, but it should not bypass the DSA's procedural safeguards. In platform contexts, the system's value lies in structured evidence and risk intelligence, not in automatic content restriction.

F. NIS2 Directive and cybersecurity obligations

The NIS2 Directive[8] strengthens EU-wide cybersecurity obligations for essential and important entities. It is relevant where HIPSTER is developed, operated or deployed by an entity within the scope of NIS2 or where HIPSTER forms part of the supply chain or security architecture of such an entity.

For HIPSTER, NIS2 translates into secure-by-design and secure-by-default requirements. The system should, among others, support incident detection, logging, evidence preservation, business continuity, vulnerability handling, supply-chain risk management, secure development practices and timely incident reporting. NIS2's incident-reporting logic also has architectural consequences: HIPSTER should be able to preserve event timelines, technical indicators, access logs and system-integrity information needed for early warning, notification and final reporting.

The NIS2 Directive does not apply directly in the same manner as an EU regulation. As a directive, it requires transposition into national law by each Member State. Therefore, where HIPSTER-like systems are developed, operated or deployed by entities falling within the scope of NIS2, the applicable obligations must be assessed under the relevant national transposing legislation, together with any implementing acts adopted at Member State level. In Lithuania, NIS2 has been transposed primarily through the Law on Cyber Security of the Republic of Lithuania[9] while technical requirements have been set in the Resolution of the Government of the Republic of Lithuania "On the Implementation of the Law on Cyber Security of the Republic of Lithuania".[10]

G. Copyright, text and data mining and web scraping

HIPSTER-like systems may rely on web scraping and automated collection of publicly accessible information. This raises several legal issues. Where scraped material contains personal data, the GDPR or LED analysis above applies. Separately, copyright, database rights and text-and-data-mining rules may be relevant.

[8] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[9] Lietuvos Respublikos kibernetinio saugumo įstatymas, available at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr.

[10] Lietuvos Respublikos Vyriausybės nutarimas " Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo", available at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr.

The Directive on Copyright and Related Rights in the Digital Single Market[11] establishes text-and-data-mining exceptions. Article 3 concerns text and data mining for scientific research by research organisations and cultural heritage institutions. Article 4 provides a broader text-and-data-mining exception for lawfully accessible works, subject to rights holders reserving their rights in an appropriate manner.

For HIPSTER, this means that scraping and data mining should be limited to lawfully accessible sources, respect applicable rights reservations, preserve source and licence metadata and distinguish between operational analysis and reuse of material for model training. If the system uses or incorporates general-purpose AI models, the AI Act's copyright-related obligations for such models may also become relevant.

6. Lithuanian National Law

A. Intelligence legislation

Intelligence rules differ across Member States and must therefore be assessed under the relevant national legal framework in each deployment context. Lithuania's intelligence framework is one example and is relevant where HIPSTER-like systems are used by intelligence authorities or support national-security functions.[12]

For HIPSTER, this means that intelligence deployment must be tied to statutory mandates, oversight mechanisms, classification rules and necessity and proportionality requirements. Intelligence use also requires stricter separation between classified and non-classified environments, controlled disclosure, auditability, access restrictions and procedures for sharing information with non-intelligence actors.

If HIPSTER is used outside intelligence authorities, it should not simulate intelligence powers through private or research activity. Rather, it should provide lawful analytical support within the mandate of the deploying actor.

B. Criminal-law

Criminal law is not merely a downstream enforcement matter. It shapes the categories that HIPSTER may be asked to detect, including election interference, threats to public officials, false reporting of public danger, incitement, cyber-related offences and conduct linked to public disorder or national security. In Lithuania, Criminal Code is the legislation where relevant crimes are extensively described.[13]

The design implication is that HIPSTER should not rely on keyword-based criminal classification. Many relevant offences require context, intent, likelihood of harm, target identification and assessment of whether expression crosses the threshold from protected speech into unlawful conduct. Therefore, HIPSTER outputs should be framed as indicators, alerts or analytical leads. Borderline cases should be escalated for human legal and operational review.

C. Public information and media regulation

Lithuania's public information framework is relevant to disinformation, propaganda and foreign information manipulation. In Lithuania, the Law on the Provision of Information to the Public[14] is the

[11] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, available at: https://eur-lex.europa.eu/eli/dir/2019/790/oj/eng.

- [12] Intelligence Ombudspersons' Office of Lithuania, Legislation. Available at: https://www.zki.lt/en/legislation/
- [13] Republic of Lithuania, Criminal Code. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111555/asr

[14] https://www.e-tar.lt/portal/lt/legalAct/TAR.065AB8483E1E/asr

principal law governing the collection, production, publication and dissemination of public information, as well as rights, duties and liability of public-information producers and disseminators.

This framework is important for HIPSTER because hybrid threats often operate through media channels, online outlets, coordinated narratives and foreign-state information ecosystems. HIPSTER may assist lawful implementation by identifying content linked to restricted or hostile sources, detecting coordinated narratives of propaganda, preserving evidence and supporting regulator or court review. However, because media regulation directly intersects with freedom of expression and media pluralism, HIPSTER should not be used as an automatic censorship tool. It should support proportional, reviewable and evidence-based decision-making.

D. Strategic communication coordination

Lithuania's Strategic Communication Coordination Framework, approved by Government Resolution No. 955,[15] establishes procedures for strategic communication in the field of national security. The Resolution sets out the institutional framework for identifying, assessing and responding to information threats, information incidents and hostile information influence activities. It provides for coordination between responsible public authorities, defines the main stages of strategic communication activity, and links monitoring and assessment of the information environment with planning, implementation and evaluation of response measures.

The framework also emphasises the need for timely exchange of information, inter-institutional cooperation, and proportionate responses to information threats. It distinguishes between different levels and forms of information-related risks and provides a basis for coordinated public communication, awareness-raising and resilience-building activities. In this context, HIPSTER-like systems may be relevant only as analytical support tools, while classification of incidents, public communication, response measures and institutional coordination remain the responsibility of competent public authorities.

E. Personal data processing for defence purposes in Lithuania

Lithuania's national framework is sufficiently broader than the LED alone. Although the LED concerns processing by competent authorities for criminal-law and public-security purposes, Lithuania's implementing legislation also establishes rules for personal data processed for national security and defence purposes. The relevant law is the Law of the Republic of Lithuania on Legal Protection of Personal Data, Processed for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences, or the Execution of Criminal Penalties, or National Security, or Defence.[16] Other Member States may likewise have specific national regimes governing personal data processing for defence, national security or intelligence purposes, so the applicable framework must always be assessed on a country-by-country and deployment-specific basis.

For HIPSTER-like systems used in a defence context, this means that processing of personal data must be assessed not only under general GDPR rules, but also under the specific data protection framework applicable to national security and defences.

F. National Security Strategy and Military Strategy

Lithuania's National Security Strategy[17] places hybrid threats within a broader whole-of-state and whole-of-society security approach. Official Lithuanian sources describe the updated strategy as

- [15] Register of Legal Acts of Lithuania, Government Resolution No. 955 on Strategic Communication Coordination in the field of national security. Available at: https://www.teisesakturegistras.lt/portal/lt/legalAct/4d789fb0eb8511eaa12ad7c04a383ca0

[16] https://www.e-tar.lt/portal/lt/legalAct/TAR.299D835159BE/asr

- [17] Ministry of National Defence of Lithuania, National Security Strategy update. Available at: https://kam.lt/en/the-seimas-approved-the-reviewed-national-security-strategy/

addressing threats from Russia, Belarus and China, strengthening resilience of the state and society, preparing for military, hybrid and other threats, improving crisis management and protecting critical infrastructure.

The Military Strategy of the Republic of Lithuania[18] similarly recognises that conventional military instruments may be combined with non-military tools designed to exploit vulnerabilities. It emphasises preparedness, resilience and the ability of the Lithuanian Armed Forces to operate in a complex security environment.

These strategic documents do not themselves impose technical compliance requirements on HIPSTER. They provide the national security rationale for systems that improve situational awareness, civil-military cooperation, information-domain defence, cyber resilience and coordinated response to hybrid activity.

7. EU and NATO policy frameworks

This section deliberately separates policy and soft-law frameworks from the binding EU legal analysis above. These frameworks do not replace legal obligations under the GDPR, LED, AI Act, DSA, NIS2 or national law. They do, however, explain the strategic need for HIPSTER-like systems and provide relevant design expectations.

The EU Joint Framework on Countering Hybrid Threats[19] establishes a coordinated approach to improving awareness, building resilience, preventing and responding to crises, recovering from hybrid activity and strengthening EU-NATO cooperation. It treats hybrid threats as activities combining coercive and subversive methods, conventional and unconventional tools, and state or non-state actors.

NATO's Strategic Concept[20] identifies hybrid threats as a persistent challenge to Allied security and recognises that hybrid operations against Allies may reach the level of armed attack. NATO also describes hybrid threats as combining military and non-military, covert and overt means, including disinformation, cyberattacks and economic pressure, often designed to blur the line between war and peace.

NATO's revised Artificial Intelligence Strategy[21] provides a relevant normative framework for AI in defence and security contexts. It emphasises responsible AI principles including lawfulness, responsibility and accountability, explainability and traceability, reliability, governability and bias mitigation.

For HIPSTER, these policy frameworks support the legitimacy and strategic relevance of hybrid-threat analytics. They also reinforce design choices already required by binding law: human responsibility, explainability, auditability, resilience, interoperability, proportionality and safeguards against bias or misuse.

8. Ethical and Social Aspects Requirements

HIPSTER's regulatory compliance should be complemented by a dedicated ethical and social aspects framework. This section does not repeat the hard-law requirements addressed in the regulatory mapping. Instead, it focuses on the ethical and societal conditions needed for responsible design, deployment and

- [18] Ministry of National Defence of Lithuania, Military Strategy of the Republic of Lithuania. Available at: https://kam.lt/wp-content/uploads/2022/03/karine-strategija-EN-2016.pdf
- [19] European Commission and High Representative, Joint Framework on Countering Hybrid Threats: a European Union response, JOIN(2016) 18 final. Available at: https://data.consilium.europa.eu/doc/document/ST-7688-2016-INIT/en/pdf
- [20] NATO, Strategic Concept 2022, PDF. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
- [21] NATO, Summary of NATO's revised Artificial Intelligence Strategy. Available at: https://www.nato.int/cps/en/natohq/official_texts_227237.htm

use of HIPSTER-like systems. Its purpose is to ensure that the system supports resilience against hybrid threats while preserving trust, human agency, democratic values and fundamental rights.

From an ethical perspective, HIPSTER's AI-supported analysis should be based on transparency, accountability, explainability, fairness, human oversight and robustness. These principles are consistent with the European Commission's Ethics Guidelines for Trustworthy AI,[22] which identify human agency and oversight, technical robustness, privacy and data governance, transparency, diversity and non-discrimination, societal well-being and accountability as core requirements for trustworthy AI.

Because HIPSTER may flag content, accounts, narratives, networks or behavioural patterns, its outputs should be understandable to the relevant user. Operational users should receive clear explanations of the main indicators, confidence levels and reasons for flagging. Auditors and oversight bodies should have access to more detailed information on model design, data sources, performance, limitations and bias testing. The level of explainability should be appropriate to the context, as also reflected in UNESCO's Recommendation on the Ethics of Artificial Intelligence,[23] which emphasises transparency, explainability, auditability and oversight.

Human oversight should remain central. HIPSTER should support expert assessment rather than replace it. High-impact actions, such as escalation to competent authorities, security intervention, long-term blocking recommendations or regulatory referral, should not be based solely on automated outputs. Regular ethical reviews, bias audits, performance testing and error-rate monitoring should be integrated into the system lifecycle.

Fairness and non-discrimination are also essential. Hybrid-threat analysis may involve sensitive social, political or behavioural signals, which can create risks of biased or disproportionate outcomes. HIPSTER should therefore be tested for discriminatory patterns, especially where outputs may affect vulnerable groups, minority communities, journalists, activists or politically exposed individuals. The EU Agency for Fundamental Rights has highlighted that algorithmic systems can create discrimination risks, making bias assessment and rights-sensitive design particularly important.

Freedom of expression requires specific ethical safeguards. Hybrid-threat detection may involve disinformation, propaganda, hostile influence and coordinated manipulation, but the system must avoid chilling lawful speech, journalism, academic debate, activism, satire or political criticism. The Council of Europe's guidance on digital technologies and freedom of expression stresses that digital technologies should serve rather than restrict freedom of expression and that their impacts should be reviewed regularly. Accordingly, borderline cases should be subject to human review, and public-interest content should be treated with caution.

The social dimension is equally important. Public trust is necessary for the legitimate use of hybrid-threat technologies. HIPSTER should therefore be accompanied by clear public-facing explanations of its purpose, capabilities and limits. Communication should avoid overstating system accuracy or certainty. Stakeholder engagement should involve, where appropriate, public institutions, civil society, academic experts, affected communities and users. The European Commission's Better Regulation Toolbox[24] recognises stakeholder consultation as an important part of evidence-based and transparent decision-making.

Finally, HIPSTER should be subject to periodic societal impact assessments. These assessments should examine the system's effects on privacy expectations, freedom of expression, non-discrimination, public

[22] European Commission, Ethics Guidelines for Trustworthy AI. Available at: https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf

- [23] UNESCO, Recommendation on the Ethics of Artificial Intelligence. Available at: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

- [24] European Commission, Better Regulation Toolbox – stakeholder consultation and impact assessment tools. Available at: https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en

trust, institutional accountability and societal resilience. Their findings should inform system design, user training, deployment rules and continuous improvement. In this way, the ethical and social aspects framework ensures that HIPSTER contributes to hybrid-threat resilience without undermining the democratic values it is intended to protect.

9. Comparative compliance model for HIPSTER

The regulatory mapping suggests that HIPSTER should not be governed through a single undifferentiated compliance layer. Instead, it should be designed around at least three legally distinct operating modes.

- **Civilian, research or private-sector mode**. This mode applies where HIPSTER is developed or used by research organisations, private entities or public bodies outside law-enforcement and national-security functions. The main legal framework is the GDPR, supplemented by the AI Act where applicable, NIS2 where the entity or deployment environment falls within scope, and the DSA where outputs are used for platform governance.
- **Law-enforcement mode**. This mode applies where competent authorities use HIPSTER for prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties or safeguarding against threats to public security. The LED and national implementing laws become essential. The system must distinguish facts from assessments, maintain detailed logs, support purpose-specific retention, restrict access, preserve human oversight and prevent spillover into civilian datasets.
- **National-security and defence mode**. This mode applies where HIPSTER is used exclusively for national security, defence or intelligence purposes under national law. EU data-protection and AI-law exclusions may become relevant, but constitutional, human-rights, intelligence, secrecy, oversight and proportionality requirements remain. This mode requires the strongest access controls, classification handling, audit trails and disclosure restrictions.

Across all modes, the following design controls should be treated as core compliance requirements:

- legal-basis and purpose tagging for datasets and outputs;
- separation of civilian, law-enforcement and national-security environments;
- documented provenance for OSINT and SOCINT sources;
- configurable retention and deletion rules;
- human review for consequential or borderline decisions;
- explainable outputs with confidence levels and limitations;
- distinction between factual observations, inferred assessments and legal conclusions;
- bias, accuracy and robustness testing;
- tamper-evident logging and audit trails;
- cybersecurity-by-design, including secure development and incident-response capability;
- DPIA and, where applicable, FRIA processes;
- governance arrangements for joint controllership, processing roles, data sharing and international transfers.

This compliance model demonstrates that regulatory mapping is not ancillary to HIPSTER's technical development. It is an enabling condition for trustworthy deployment. A system intended to detect hybrid threats must itself be resilient against legal uncertainty, overreach, misuse and loss of public trust.

10. Summary and Conclusion

This report maps the main regulatory, ethical and social requirements relevant to HIPSTER as an AI-supported system for hybrid threat detection and analysis. The document focuses primarily on hard-law requirements, including binding EU and national legal frameworks. Guidance, soft-law instruments, policy documents and case-law analysis are addressed separately, where they may support interpretation and implementation.

The analysis shows that HIPSTER operates in a complex legal environment because hybrid threats may, among others, involve cyberattacks, disinformation, societal manipulation, hostile intelligence activity, public-security risks and defence-related concerns. Therefore, the system cannot be assessed under one legal framework alone. Its obligations depend on the deployment context, the operator, the purpose of use, the type of data processed and whether system outputs may affect individuals or organisations.

A key conclusion is that HIPSTER must be designed as a context-sensitive and regime-sensitive system. Civilian, academic and private-sector uses are mainly governed by the GDPR, together with relevant AI Act, cybersecurity, intellectual property and platform-regulation requirements. Law-enforcement uses require assessment under national laws transposing the Law Enforcement Directive instead of the GDPR, while other requirements such as AI Act remain applicable to the extent they apply to law enforcement scenarios. National-security and defence use may fall partly outside EU regulatory instruments but remain subject to national constitutional, human-rights, intelligence, secrecy, oversight and proportionality requirements. Member States may also have specific national regimes in these areas, meaning that deployment must always be assessed on a country-by-country basis.

The deliverable further confirms that fundamental rights must be embedded into HIPSTER's design. The system may affect privacy, data protection, freedom of expression, non-discrimination and effective remedy, particularly when processing OSINT/SOCINT data, identifying coordinated behaviour or flagging harmful content. For this reason, HIPSTER should operate as a decision-support tool, not as an autonomous decision-maker. Human oversight, explainability, auditability, data minimisation, purpose limitation, retention control and a clear distinction between factual observations and analytical assessments are essential safeguards.

The Lithuanian mapping illustrates how national law complements EU-level requirements in practice. Lithuanian cybersecurity, personal data protection, public information, criminal-law, intelligence, defence and strategic communication frameworks provide important context for lawful hybrid-threat response.

Finally, the ethical and social assessment shows that legal compliance alone is not sufficient. HIPSTER's legitimacy also depends on ethical governance, bias testing, societal impact assessment, stakeholder engagement and public trust.

This report is therefore non-exhaustive and should be treated as a living document, to be updated regularly as EU and national frameworks evolve and as HIPSTER is considered for new operational contexts.

11. Bibliography

Fundamental rights and constitutional sources

- Council of Europe, European Convention on Human Rights. Available at: https://www.echr.coe.int/documents/d/echr/convention_ENG
- European Union, Charter of Fundamental Rights of the European Union. Available at: https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng
- European Union, Treaty on European Union, Article 4(2). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012M004
- Republic of Lithuania, Constitution of the Republic of Lithuania.Available at: https://www.lrs.lt/home/Konstitucija/Constitution.htm

European Union binding legal instruments

- Regulation (EU) 2016/679, General Data Protection Regulation. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
- Directive (EU) 2016/680, Law Enforcement Directive. Available at: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng
- Regulation (EU) 2024/1689, Artificial Intelligence Act. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
- Regulation (EU) 2022/2065, Digital Services Act. Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
- Directive (EU) 2022/2555, NIS2 Directive. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
- Regulation (EU) 2019/881, Cybersecurity Act. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng
- Directive (EU) 2019/790, Directive on Copyright and Related Rights in the Digital Single Market. Available at: https://eur-lex.europa.eu/eli/dir/2019/790/oj/eng
- Regulation (EU) 2023/2854, Data Act. Available at: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng
- European Commission, Regulatory framework on artificial intelligence. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
- European Commission, Digital Services Act: Very Large Online Platforms and Search Engines. Available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops
- European Commission, NIS2 Directive overview. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- European Commission, EU Cybersecurity Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- European Commission, European cybersecurity certification framework. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework
- ENISA, Cybersecurity certification framework. Available at: https://www.enisa.europa.eu/topics/product-security-and-certification/cybersecurity-certification-framework

Lithuanian official sources

- State Data Protection Inspectorate of Lithuania, Legislation. Available at: https://vdai.lrv.lt/en/legislation
- State Data Protection Inspectorate of Lithuania, Law on Legal Protection of Personal Data, English translation. Available at: https://vdai.lrv.lt/uploads/vdai/documents/files/Republic%20of%20Lithuania%20Law%20on%20legal%20protection%20of%20personal%20data%202018%20Non-Official%20Translation%2001_12_2021.pdf

- European Commission, NIS2 Directive: Lithuania country information. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-lithuania
- Ministry of National Defence of Lithuania, National Security Strategy update. Available at: https://kam.lt/en/the-seimas-approved-the-reviewed-national-security-strategy/
- Ministry of National Defence of Lithuania, Military Strategy of the Republic of Lithuania. Available at: https://kam.lt/wp-content/uploads/2022/03/karine-strategija-EN-2016.pdf
- Intelligence Ombudspersons' Office of Lithuania, Legislation. Available at: https://www.zki.lt/en/legislation/
- Republic of Lithuania, Criminal Code. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111555/asr
- Register of Legal Acts of Lithuania, Government Resolution No. 955 on Strategic Communication Coordination in the field of national security. Available at: https://www.teisesakturegistras.lt/portal/lt/legalAct/4d789fb0eb8511eaa12ad7c04a383ca0
- National Cyber Security Centre of Lithuania, 2024 key trends and statistics of cybersecurity. Available at: https://www.nksc.lt/doc/en/2024_key-trends-and-statistics-of-cyber-security.pdf

EU and NATO policy frameworks

- European Commission and High Representative, Joint Framework on Countering Hybrid Threats: a European Union response, JOIN(2016) 18 final. Available at: https://data.consilium.europa.eu/doc/document/ST-7688-2016-INIT/en/pdf
- NATO, Strategic Concept 2022. Available at: https://www.nato.int/cps/en/natohq/topics_210907.htm
- NATO, Strategic Concept 2022, PDF. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
- NATO, Countering hybrid threats. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm
- NATO, Summary of NATO's revised Artificial Intelligence Strategy. Available at: https://www.nato.int/cps/en/natohq/official_texts_227237.htm

Ethical and Social Requirements

- European Commission, High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
- European Commission, Ethics Guidelines for Trustworthy AI. Available at: https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf
- UNESCO, Recommendation on the Ethics of Artificial Intelligence. Available at: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics
- UNESCO, Recommendation on the Ethics of Artificial Intelligence, overview. Available at: https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence
- OECD, AI Principles. Available at: https://www.oecd.org/en/topics/ai-principles.html
- OECD, Recommendation of the Council on Artificial Intelligence. Available at: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449
- Council of Europe, The impacts of digital technologies on freedom of expression: Recommendation CM/Rec(2022)13. Available at: https://edoc.coe.int/en/international-law/11101-the-impacts-of-digital-technologies-on-freedom-of-expression-recommendation-cmrec202213.html

- Council of Europe, Recommendation CM/Rec(2022)13 of the Committee of Ministers to member States on the impacts of digital technologies on freedom of expression. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a61729
- European Union Agency for Fundamental Rights, Bias in algorithms – Artificial intelligence and discrimination. Available at: https://fra.europa.eu/en/publication/2022/bias-algorithm
- European Commission, Better Regulation Toolbox – stakeholder consultation and impact assessment tools. Available at: https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en