МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО
на засіданні кафедри
міжнародних відносин і політичної
філософії
Протокол № 17 від 28.08.2025 р.

ПОГОДЖЕНО
Проректор з навчально-методичної
роботи
Каріна НЕМАШКАЛО

КІБЕРДИПЛОМАТІЯ
робоча програма навчальної дисципліни (РПНД)

Галузь знань	**С «Соціальні науки, журналістика, інформація та міжнародні відносини»**
Спеціальність	**С3 «Міжнародні відносини»**
Освітній рівень	**Перший (бакалаврський)**
Освітня програма	**Міжнародні відносини**

Статус дисципліни **вибіркова**

Мова викладання, навчання та оцінювання **англійська**

Розробник:
викл. _____ Данило НЕПОЧАТОВ

Завідувач кафедри
міжнародних відносин і
політичної філософії _____ Олег КУЗЬ

Гарант програми _____ Ірина ЖЕРЕБЯТНІКОВА

Харків
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SIMON KUZNETS KHARKIV NATIONAL UNIVERSITY OF ECONOMICS

APPROVED
at the meeting of the Department of International Relations and Political Philosophy
Protocol №. 17 of 28.08.2025

AGREED
Vice-Rector for Educational and Methodical Work

_____ Karina NEMASHKALO

Cyberdiplomacy
Programme of the Course

Field of Knowledge	**C «Social Sciences, Journalism, Information and International Relations»**
Specialty	**C3 «International Relations»**
Study Cycle	**First (Bachelor's)**
Study Programme	**International Relations**

Course Status	**Elective**
Language	**English**

Developers:
Lecturer _____ Danylo NEPOCHATOV

Head of the Department of International Relations and Political Philosophy _____ Oleh KUZ

Head of Study Programme _____ Iryna ZHEREBIATNIKOVA

Kharkiv
2025

INTRODUCTION

The Course Programme Cyber Diplomacy is an elective component of the educational and professional training programme for Bachelor's students majoring in C3 International Relations. Its relevance is determined by the transformation of cyberspace into one of the key dimensions of international security, within which state competition takes place, new conflict dynamics emerge, and the need arises for diplomatic mechanisms to regulate digital threats.

In contemporary international relations, cyberattacks, influence operations, problems of attribution, and asymmetries of technological capabilities increasingly act as factors of strategic instability. Under these conditions, cyber diplomacy is taking shape as an instrument of foreign policy aimed at managing low-intensity conflicts in cyberspace, preventing escalation, developing international norms of behaviour, and ensuring predictability in the field of international cybersecurity.

The course considers cyber diplomacy not only as a set of diplomatic practices, but as an empirically observable and analytically measurable process of international interaction. Within the framework of the course, students acquire approaches to the analysis of cyber incidents, diplomatic statements, negotiation formats, and strategic documents, which makes it possible to interpret events in cyberspace as elements of a broader international security system.

The course is grounded in a combination of qualitative political and security analysis with elements of data-driven and computational approaches, which allows for the identification of structural trends, actor configurations, and patterns of behaviour of states and international organisations in the global cyberspace. This approach makes it possible to move beyond a purely descriptive level and to develop students' skills of systematic analytical thinking.

The course material is based on the analysis of representative case studies of cyber diplomatic practice that illustrate different models of ensuring cybersecurity, approaches to international norm-setting, as well as the specifics of interaction between state and non-state actors in the digital environment. Particular attention is paid to cases related to geopolitical competition, crises, and armed conflicts.

The object of the course is cyber diplomacy as a component of international cybersecurity and a form of interaction between actors in international relations in cyberspace.

The subject of the course comprises political, legal, institutional, and technological factors shaping international norms, diplomatic strategies, deterrence mechanisms, and cooperation in the field of cybersecurity.

The purpose of the course is to develop in students the ability to conceptually comprehend cyber diplomacy as an instrument of international cybersecurity, as well as to analyse the processes of norm formation, strategies, and practices of international interaction in cyberspace using comparative, case-based, and data-driven approaches.

The tasks of the course are as follows:

- to form a theoretical understanding of cyberspace as a specific domain of international security that combines political, military, legal, and technological dimensions;
- to analyse cyber diplomacy as an instrument of conflict management, de-escalation, and the formation of predictable patterns of state behaviour in an environment of limited transparency and complex attribution;
- to familiarise students with key approaches to international norm-setting in cyberspace within multilateral and regional formats;
- to develop the ability to critically analyse national and international cyber strategies in the context of foreign policy and international security;
- to teach students to interpret cyber incidents as political signals and instruments of strategic communication in international relations;
- to master basic skills in preparing analytical materials, policy briefs, and recommendations in the field of cyber diplomacy;
- to develop the ability to combine qualitative case analysis with elements of data-driven and OSINT analysis to identify actors and patterns of international interaction in cyberspace;
- to form an understanding of the limitations and risks of cyber diplomacy, including problems of escalation, capability asymmetries, and the instrumentalisation of international law.

The learning outcomes and competencies formed by the course are presented in Table 1.

Table 1

Learning Outcomes and Competencies Formed by the Course

Learning Outcomes	**Competencies**
LO2.	GC5, SC1, SC3, SC11.
LO3.	GC5, SC1, SC13.
LO7.	GC6, SC2, SC4.
LO8.	GC12, SC3, SC4, SC12.
LO9.	GC5, GC12, SC11, SC13.
LO10.	GC11, SC12.
LO11.	SC4, SC10, SC13.
LO14.	SC3, SC4, SC5, SC12.

where, LO02. To know and understand the nature and dynamics of international security, to understand the specifics of its provision at the global, regional, and national levels, and to know the nature of and approaches to resolving international and internationalised conflicts.

LO05. To know the nature and mechanisms of international communications.

LO07. To describe and analyse the international situation, and to collect from various sources the information necessary for this purpose on international and foreign policy events and processes.

LO08. To collect, process, and analyse large volumes of information on the state of international relations, the foreign policy of Ukraine and other states, regional systems, and international communications.

LO09. To study issues of international relations, regional development, foreign policy, and international communications using modern political, economic, and legal theories and concepts, scientific methods, and interdisciplinary approaches; to present research results and provide relevant recommendations.

LO10. To communicate fluently in the state language and foreign languages at a professional level necessary for conducting professional discussions and preparing analytical and research documents.

LO11. To carry out applied analysis of international relations, the foreign policy of Ukraine and other states, international processes, and the international situation in accordance with defined objectives; to prepare informational and analytical materials.

LO14. To use modern digital technologies, specialised software, databases, and information systems to solve complex specialised tasks in the field of international relations, social communications, and/or regional studies.

GC5. Ability to work in an international context.

GC6. Ability to generate new ideas (creativity).

GC11. Ability to communicate in a foreign language.

GC12. Ability to search for, process, and analyse information from various sources.

SC1. Ability to identify features and development trends, and to understand the nature, dynamics, and principles of organisation of international relations, social communications, and/or regional studies.

SC2. Ability to analyse international processes in various contexts (political, cultural, informational, etc.).

SC3. Ability to assess the state and directions of research in international relations and world politics.

SC4. Ability to solve complex specialised tasks and practical problems in the field of international relations and social communications.

SC5. Ability to analyse the impact of the global economy, international law, and domestic politics on international relations.

SC10. Ability to analyse the structure and dynamics of international public communications.

SC11. Ability to analyse the nature and evolution of international organisations.

SC12. Ability to carry out communication and information-analytical activities in the field of international relations.

SC13. Ability to analyse the activities of international non-state actors and transnational relations.

COURSE CONTENT

Topic 1. Introduction to Cyber Diplomacy: Cyberspace as a Dimension of International Security

The topic outlines the subject and logic of the course, explaining why cyberspace has become an independent dimension of international security alongside land, sea, air, and outer space. It analyses the transformation of digital threats from a technical issue into a political and security challenge. Cyber diplomacy is examined as an instrument for managing risks, conflicts, and international interaction in the digital environment.

Key questions:

- Why is cyberspace considered a domain of international security?
- What is the essence of cyber diplomacy as a diplomatic practice?
- What challenges does cyberspace pose to traditional diplomacy?

Topic 2. Actors of Cyber Diplomacy and the Structure of the Global Cyberspace

This topic is devoted to the analysis of key actors of cyber diplomacy and their roles in shaping the international order in cyberspace. It examines the interaction between states, international organisations, private technology companies, and expert communities. Particular attention is paid to the asymmetry of capabilities and influence among different groups of actors.

Key questions:

- Who are the main actors of cyber diplomacy?
- Why do non-state actors play a critical role in cybersecurity?
- How does resource asymmetry affect international cyber stability?

Topic 3. The Global Cyber Threat Landscape and the Logic of Conflict in Cyberspace

The topic explores the main types of cyber threats and their role in contemporary international conflicts. Cyber incidents are considered as forms of political signalling, coercion, or deterrence. Special attention is paid to the problem of attribution and the limited predictability of actions in cyberspace.

Key questions:

- Which types of cyber threats have strategic significance?
- How do cyber conflicts differ from traditional military conflicts?
- How does the attribution problem affect escalation?

Topic 4. Cyber Diplomacy of Leading States: Strategic Models of the United States and China

This topic focuses on a comparative analysis of the cyber diplomacy of the United States and China as two competing models of global influence. It examines differences in approaches to norm-setting, deterrence, and the role of the state in cyberspace. The integration of cyber diplomacy into broader geopolitical competition is analysed.

Key questions:

- What are the key differences between the cyber strategies of the United States and China?
- How does cyber diplomacy reflect global great power competition?
- What are the implications of this competition for international cybersecurity?

Topic 5. Cyber Diplomacy of Ukraine: A Security Perspective and International Interaction

The topic examines the specific features of Ukraine's cyber diplomacy in the context of armed conflict and hybrid warfare. It analyses the role of international support, partnerships, and legal mechanisms in ensuring cyber resilience. Particular attention is given to Ukraine's practical experience as a source of international lessons.

Key questions:

- What is Ukraine's place in the global cybersecurity system?
- How does war transform the instruments of cyber diplomacy?
- Which lessons from Ukraine's experience are relevant for other states?

Topic 6. International Law, Norms, and Digital Sovereignty in Cyberspace

This topic analyses the international legal foundations of cyberspace regulation and the challenges of developing universally accepted global norms. It examines concepts of digital sovereignty, state responsibility, and the legal limits of cyber activities. Special attention is paid to tensions between security, freedoms, and international law.

Key questions:

- Is effective international law in cyberspace possible?
- How do states interpret digital sovereignty?
- Where is the boundary between security and human rights in cyberspace?

Topic 7. Cyber Weapons, Deterrence, and Escalation in International Conflicts

The topic is devoted to the analysis of cyber weapons as instruments of international confrontation. It examines concepts of cyber deterrence, escalation risks, and challenges of controlling cyber arsenals. Emphasis is placed on strategic uncertainty and the opacity of cyber operations.

Key questions:

- Can cyber operations be considered a form of the use of force?
- How does deterrence function in cyberspace?
- What escalation risks are associated with cyber weapons?

Topic 8. The Technological Dimension of Cyber Diplomacy: AI, Semiconductors, Critical Infrastructure

This topic analyses advanced technologies as key factors of international cybersecurity and diplomacy. It examines the role of artificial intelligence, semiconductors, and the protection of critical infrastructure in shaping security dependencies. Technologies are presented as objects of strategic control and diplomatic agreements.

Key questions:

- Why have technologies become subjects of international diplomacy?
- How do technological supply chains affect state security?
- What risks and opportunities does AI pose for cyber diplomacy?

Topic 9. Cyber Diplomacy and Economic Security

The topic is devoted to the interconnection between cybersecurity, the global economy, and technology markets. It analyses sanctions, export controls, and technological restrictions as instruments of cyber diplomacy. Economic vulnerability is considered as a factor of international cyber stability.

Key questions:

- How does cybersecurity affect the economic security of states?
- Can economic cyber diplomacy be identified?
- What role do technological sanctions play in international relations?

Topic 10. Synthesis and Future Trends in Cyber Diplomacy

The concluding topic integrates the theoretical and applied approaches of the course and forms a holistic vision of cyber diplomacy. It analyses future trends in international cybersecurity and the requirements for analytical and diplomatic work. The topic is oriented toward preparing students for the practical application of knowledge.

Key questions:

- Which trends will shape the future of cyber diplomacy?
- What competencies are required for specialists in international cybersecurity?
- How can the analysis of cyber events be translated into political decisions?

The list of practical (seminar) classes / tasks for the course is given in Table 2.

Table 2

List of Practical (Seminar) Studies

Topic	Content
Task 1 Topic 1. Introduction to Cyber Diplomacy: Cyberspace as a Dimension of International Security	*Individual task:* Within 7 days, compile a basic dataset for 10–15 countries in a country–year format and construct two distribution charts of cybersecurity indicators. *Data:* GCI, NCSI, Polity2, or Freedom House. Tools: R, readr/readxl, dplyr, ggplot2. *Group task (Stage 1):* Development of a unified panel dataset format for the semester project.
Task 2 Topic 2. Actors of Cyber Diplomacy and the Structure of the Global	*Individual task:* Based on the prepared dataset, conduct a comparative analysis of two groups of states (e.g., democratic and authoritarian) using cybersecurity indicators. Apply descriptive statistics and visualisations to identify differences between the groups. Interpret the results taking into account the

Cyberspace	role of the state as an actor of cyber diplomacy. Formulate preliminary analytical conclusions. *Data:* GCI or NCSI, Polity2 or Freedom House. *Tools:* R, dplyr, ggplot2. *Group task (Stage 2):* Coordination of the list of countries and the time frame of the group study.
Task 3 Topic 3. The Global Cyber Threat Landscape and the Logic of Conflict in Cyberspace	*Individual task:* Construct time trends of cybersecurity indicators and analyse their dynamics. Briefly assess the stability or volatility of the cybersecurity environment. *Data:* GCI or NCSI for several years, Digital Development Index. *Tools:* R, lubridate, ggplot2. *Group task (Stage 3):* Formulate 2–3 analytical hypotheses to be tested within the group project. Agree on the indicators to be used for testing. Record the hypotheses in a shared document.
Task 4 Topic 3. The Global Cyber Threat Landscape and the Logic of Conflict in Cyberspace	*Individual task:* Calculate correlations between several cybersecurity indices and indicators of political regime type. Build a correlation matrix and visualise it as a heatmap. Analyse which indicators are most consistent with each other and which demonstrate divergence. Draw a conclusion regarding what different indices actually measure. *Data:* GCI, NCSI, EGDI, Digital Development Index, Cyber Risk Index, Internet penetration, Polity2, Freedom House. *Tools:* R, cor, ggcorrplot. *Group task (Stage 4):* Select key variables for further group analysis. Substantiate the choice of each variable from an analytical perspective. Record the final set of indicators.
Task 5 Topic 4. Cyber Diplomacy of Leading States: Strategic Models of the United States and China	*Individual task:* Apply principal component analysis or cluster analysis to a set of cybersecurity indicators. Identify the main analytical dimensions and interpret their meaning. Visualise the results and explain how they simplify the understanding of a complex dataset. Briefly assess the analytical value of the obtained components or clusters. *Data:* 6–8 quantitative cybersecurity indices. *Tools:* R, FactoMineR, factoextra. *Group task (Stage 5):* Agree on the set of analytical dimensions

	to be used in the group project. Relate them to the previously formulated hypotheses. Record the structure of the analytical model of the group study.
Task 6 Topic 4. Cyber Diplomacy of Leading States: Strategic Models of the United States and China	*Individual task:* Based on the prepared dataset, examine the relationship between political regime type and the level of cybersecurity, testing whether this relationship is non-linear. Construct a plot with local regression (LOESS) and compare it with a linear model. Optionally, apply GAM for a more formal test of non-linearity. Briefly interpret the ranges of regime indicators in which the relationship changes. *Data:* Polity2 or Freedom House, GCI or EGDI. *Tools:* R, ggplot2 (LOESS), mgcv. *Group task (Stage 6):* Discuss the identified non-linear patterns in groups and record whether they recur across different countries or regions. Determine which of these patterns should be included in the group analytical report. Formulate preliminary explanatory hypotheses.
Task 7 Topic 5. Cyber Diplomacy of Ukraine: A Security Perspective and International Interaction	*Individual task:* Based on the constructed model, identify countries whose cybersecurity indicators significantly deviate from predicted values. Analyse model residuals and identify positive and negative anomalies. For 1–2 countries, prepare a short explanation of possible reasons for deviation, taking into account the political or security context. *Data:* Cybersecurity indicators, residuals of regression models. *Tools:* R, broom, dplyr, ggplot2. *Group task (Stage 7):* Jointly select 2–3 countries that represent the greatest analytical interest as "deviations from expected outcomes". Agree on which cases will be examined in the final group project. Distribute countries among group members.
Task 8 Topic 6. International Law, Norms, and Digital Sovereignty in Cyberspace	*Individual task:* Download texts of strategic documents in the field of cybersecurity and prepare them for analysis as a data corpus. Conduct frequency analysis of key terms and basic text cleaning. Identify which concepts and categories are most frequently used in the cyber-diplomatic discourse of the selected actor. *Data:* National cybersecurity strategies, UN / EU / NATO

	documents. *Tools:* R, quanteda, tidytext. *Group task (Stage 8):* Compile a joint corpus of documents for group analysis by agreeing on selection criteria. Distribute documents among group members for further processing. Record corpus structure and metadata.
Task 9 Topic 7. Cyber Weapons, Deterrence, and Escalation in International Conflicts	*Individual task:* Compare cyber narratives of two states or international organisations through keyword and term analysis. Apply tf-idf measures to identify specific topics and emphases. Draw conclusions regarding differences in approaches to cyber diplomacy and international cybersecurity. *Data:* Corpora of strategic and policy documents. *Tools:* R, quanteda, tf-idf. *Group task (Stage 9):* Agree on a common interpretative framework for textual results in the group project. Identify which narrative differences are most significant for analytical conclusions. Formulate preliminary generalisations.
Task 10 Topic 8. The Technological Dimension of Cyber Diplomacy: AI, Semiconductors, Critical Infrastructure	*Individual task:* Based on an event dataset, construct a time-series analysis of cyber incidents and related diplomatic responses. Visualise changes in event intensity over time and identify key peaks. Briefly analyse how cyber incidents correlate with diplomatic actions. *Data:* Event dataset (date, country, event type). *Tools:* R, lubridate, ggplot2. *Group task (Stage 10):* Integrate event data with previously collected structural indicators. Agree on how event analysis complements the overall logic of the group study. Determine which events will be included in the final analysis.
Task 11 Topic 8. The Technological Dimension of Cyber Diplomacy: AI, Semiconductors,	*Individual task:* Based on the conducted analysis, prepare a short policy brief formulating key findings and recommendations. Particular attention should be paid to the logic of translating data into practical policy decisions. Clearly indicate analytical limitations and possible alternative interpretations. *Data:* Results of individual analytical tasks. *Tools:* RMarkdown or Quarto.

Critical Infrastructure	*Group task (Stage 11):* Formulate joint conclusions and recommendations of the group project. Agree on the structure of the final analytical report. Distribute responsibility for sections of the document.
Task 12 Topic 9. Cyber Diplomacy and Economic Security	*Individual task:* Prepare a short methodological reflection on the data and analytical methods used. Assess the strengths and weaknesses of the chosen approach. Propose possible directions for improving the study. *Data:* Final group dataset, analytical results. *Tools:* R, presentation tools. *Group task (Stage 12):* Finalisation of visual materials for the presentation.
Task 13 Topic 9. Cyber Diplomacy and Economic Security	*Individual task:* Based on all analytical tasks completed during the semester, prepare a synthesising analytical overview. Systematise the data, methods, and results applied, highlighting key analytical conclusions regarding international cybersecurity and cyber diplomacy. Critically assess the limitations of the indices, models, and data sources used, as well as their applicability to practical policy. Formulate a personal vision of how computational approaches can be applied in further research or professional activity in the field of international relations. *Data:* Results of all individual and group tasks of the course. *Tools:* RMarkdown or Quarto.
Task 14 Topic 10. Synthesis and Future Trends in Cyber Diplomacy	*Presentation of the group project on cyber diplomacy.* Defence of analytical conclusions and responses to questions. Summarisation of the experience of teamwork throughout the semester.

The list of self-studies in the course is given in Table 3.

Table 3

List of Self-Studies

Tasks	Content
Task 1	Independent familiarisation with the basic concepts of international cyber security and cyber diplomacy. Collection of basic quantitative data for 10–15 states in a country–year format (cyber security indicators, type of political regime, region). Initial data structuring and construction of distribution charts and regional comparison visualisations using the R programming language.
Task 2	Independent comparative analysis of two groups of states (e.g., democracies and authoritarian regimes) based on cyber security indicators. Application of descriptive statistics and visualisations to identify differences between groups. Formulation of preliminary analytical conclusions regarding the role of the state in cyber diplomacy.
Task 3	Independent construction of time series of cyber security indicators for selected countries over several years. Analysis of dynamics, identification of trends and possible turning points in the development of the cyber security environment. Comparison of dynamics across countries or regions using the R programming language.
Task 4	Independent calculation of correlations between several cyber security indices and political regime indicators. Construction of a correlation matrix and its visualisation in the form of a heatmap. Analytical assessment of the consistency of indices and their conceptual differences.
Task 5	Independent application of dimensionality reduction methods or cluster analysis to a set of cyber security indicators. Interpretation of the resulting components or clusters as analytical dimensions of cyber security. Assessment of their suitability for further comparative analysis.
Task 6	Independent study of non-linear relationships between the type of political regime and the level of cyber security. Construction of local and generalised models (LOESS or GAM) and comparison with linear approaches. Analytical interpretation of the identified

	relationships using the R programming language.
Task 7	Independent analysis of anomalies in cyber security indicators through the examination of residuals from regression models. Identification of countries that demonstrate significant deviations from expected values. Preparation of a short explanation of possible reasons for such deviations.
Task 8	Independent formation of a corpus of official documents in the field of cyber security and cyber diplomacy (national strategies, international declarations). Conducting frequency analysis of key terms and basic text preprocessing using the R programming language.
Task 9	Independent comparative analysis of cyber narratives of two states or international organisations. Application of keyword analysis and tf-idf metrics to identify differences in approaches to cyber diplomacy. Formulation of substantive conclusions based on textual data.
Task 10	Independent event-based analysis of cyber incidents and related diplomatic reactions. Construction of time-based visualisations and analysis of event intensity. Assessment of the relationship between cyber incidents and international diplomatic activity.
Task 11	Independent preparation of an individual analytical policy brief based on completed computational tasks. Formulation of conclusions and recommendations for the field of international cyber security with mandatory indication of methodological limitations of the analysis.
Task 12	Independent preparation of a short methodological reflection on the data and analytical methods used during the semester. Assessment of the strengths and weaknesses of the selected computational approach, as well as the limitations of the final group dataset and analytical models. Formulation of possible directions for improving the study and alternative methodological solutions.
Task 13	Independent preparation of a synthesising analytical review based on all individual and group tasks completed during the semester. Systematisation of the applied data, methods, and obtained results, highlighting key analytical conclusions regarding international cyber security and cyber diplomacy. Critical assessment of the suitability of the used indices, models, and data sources for informing practical

	policy decisions, as well as formulation of the student's own vision of the further application of computational approaches in research and professional activity in the field of international relations.
Task 14	The semester group project Cyber Diplomacy Intelligence Project is carried out by students in groups of 2–3 persons throughout the semester. The project involves the phased formation and analysis of a shared dataset on international cyber security and cyber diplomacy. At the end of the semester, project defence takes place in the format of a review. Each group project must include: - a structured panel dataset (country–year) with cyber security indicators, political regime variables, and additional variables; - analytical visualisations of dynamics and comparative indicators; - results of correlation, cluster, and non-linear analyses; - anomaly analysis and case studies of outlier countries; - a corpus of official documents and results of text-as-data analysis; - event-based analysis of cyber incidents and diplomatic reactions; - a reproducible analytical report (R scripts or Quarto/R Markdown); - a final analytical document — the Cyber Diplomacy Intelligence Brief, including a "Methods and Limitations" section; - a presentation of the group project results.

The number of lecture hours, practical (seminar) hours, and hours of self-study is given in the technological map of the course.

TEACHING METHODS

During the teaching of the course "Cyber Diplomacy", both traditional and innovative methods of organising the educational process are employed. These methods are aimed at developing students' systematic understanding of cyber diplomacy as an instrument of international cybersecurity, as well as skills of analytical work with

quantitative, event-based, and textual data in the field of international relations. Particular attention is paid to the application of computational approaches, the critical interpretation of cybersecurity indices and models, and the integration of empirical analysis with the political and diplomatic context.

The educational process combines lectures, practical classes, seminars, and research-project formats, with an emphasis on individual and group analytical work, the completion of computational tasks, and the preparation of a semester-long group analytical project in cyber diplomacy.

Verbal methods:

- lecture with elements of an analytical overview of the global international cybersecurity environment and the role of cyber diplomacy within it (Topics 1, 2, 10);
- problem-based lecture aimed at formulating research questions, developing analytical hypotheses, and critically reflecting on approaches to measuring cybersecurity (Topics 1, 3, 6);
- mini-lecture explaining theoretical and conceptual approaches to the analysis of cyber diplomacy, cyber sovereignty, international norms of behaviour in cyberspace, and models of cyber governance (Topics 3, 5, 7, 9).

Visual methods:

- demonstration and analysis of international cybersecurity indices, cyber threat maps, and visual models of digital inequality between states (Topics 1–4);
- use of statistical visualisations, time series, correlation matrices, cluster analyses, and event-based graphs created in the R environment (Topics 2–10);
- presentation of the results of individual and group computational analysis, including visual materials from the semester project (Topics 12–14).

Practical methods:

- completion of individual computational tasks related to the collection, structuring, and analysis of international cybersecurity data using the R programming language (Topics 1–11);
- analysis of the structure and dynamics of cybersecurity indicators, correlations, non-linear relationships, anomalies, and event patterns based on empirical data (Topics 3–10);

- work with official policy documents in the field of cybersecurity and cyber diplomacy, including their coding and analysis using a text-as-data approach (Topics 8, 9).

Interactive methods:

- group analytical work focused on the formation of a shared panel dataset and a document corpus for the semester project (Topics 1–5, 8);
- collective analysis of correlations, clusters, anomalies, and event-driven processes in international cybersecurity (Topics 4–10);
- group preparation of analytical visualisations and policy conclusions for the final group project (Topics 11–14);
- presentation and public defence of the results of the semester group project in cyber diplomacy in a review format (Topic 14).

Methods for enhancing learning and cognitive activity:

- research-based learning through the completion of individual computational tasks and the semester group project (Topics 1–14);
- problem-solving and inquiry-based tasks aimed at identifying structural and dynamic patterns in international cybersecurity (Topics 3–7);
- case method involving the analysis of specific international cyber incidents, diplomatic responses, and regulatory approaches (Topics 5, 7, 10);
- project method during the implementation of the semester group assignment Cyber Diplomacy Intelligence Project (Topics 1–14).

FORMS AND METHODS OF ASSESSMENT

The University uses a 100-point cumulative system for assessing the learning outcomes of students.

Current control is carried out during lectures and practical (seminar) classes and is aimed at checking the level of readiness of the student to perform a specific task. Assessment is based on the total number of points earned: for courses with a form of semester control as an exam, the maximum number of points for current control is 60 points.

Final control is carried out in the form of a semester exam. The maximum number of points for the exam is 40 points.

The final grade in the course is determined by summing all points obtained during the current control and the exam (maximum – 100 points).

To be admitted to the semester exam, a student must obtain at least 35 points for current control. The minimum passing score for the exam is 25 points.

Current control of academic achievement is carried out in the following forms:

- collection, structuring, and primary visualisation of international cybersecurity data — twice during the semester. Maximum score per submission — *2 points (2-point scale, total 4 points);*
- comparative analysis of states in the field of cybersecurity — twice during the semester. Maximum score per submission — *3 points (3-point scale, total 6 points);*
- analysis of dynamics, correlations, and structural dimensions of cybersecurity — three times during the semester. Maximum score per submission — *3 points (3-point scale, total 9 points);*
- analysis of non-linear relationships and anomalies in cybersecurity indicators — twice during the semester. Maximum score per submission — *4 points (4-point scale, total 8 points);*
- text-as-data analysis and comparison of cyber narratives — twice during the semester. Maximum score per submission — *4 points (4-point scale, total 8 points);*
- event-based analysis of cyber incidents and diplomatic responses — once during the semester. Maximum score — *3 points (3-point scale, total 3 points);*
- preparation of an individual policy brief or analytical review — once during the semester. Maximum score — *4 points (4-point scale, total 4 points);*

- semester group analytical project “Cyber Diplomacy Intelligence Project” — once during the semester. Maximum score — *18 points (18-point scale, total 18 points).*

AN EXAMPLE OF AN EXAMINATION CARD

Simon Kuznets Kharkiv National University of Economics
Field of Knowledge C “Social Sciences, Journalism, Information and International Relations”
Specialty C3 International Relations
First (Bachelor’s) cycle of higher education
Semester II
Study course Cyber Diplomacy
EXAMINATION CARD № 1

Task 1 (practical)

Based on the provided dataset of international cybersecurity indicators (indices, event-based or panel data), complete the following tasks:

a) Substantiate which type of analysis is appropriate for this dataset (comparative analysis of states / time-series analysis / correlation analysis / analysis of nonlinear relationships / event analysis) and explain your choice.

b) Propose pseudocode or R logic for:

constructing the time dynamics of cybersecurity indicators, or

calculating correlations between cybersecurity indices and indicators of political regime.

(The logic of the analytical approach is assessed; flawless syntax is not required.)

c) Explain which empirical pattern can be identified through such analysis (trend, asymmetry between groups of states, nonlinear dependence, presence of anomalies, etc.).

Maximum — 15 points for the question.

Task 2 (theoretical and methodological)

Based on the provided international cybersecurity dataset, propose R code or its structural logic for:

forming a panel dataset in the country–year format, or

conducting cluster or PCA analysis of cybersecurity indicators, or basic text-as-data analysis of official documents in the field of cyber diplomacy.

In your answer, briefly explain which variables are used and which analytical task the proposed code addresses.

Maximum — 15 points for the question.

Task 3 (heuristic)

a) Explain why cyber diplomacy is considered an instrument of international cybersecurity. Describe the logic of interaction between diplomacy, security, and digital technologies, and provide examples.

b) Explain the difference between national cyber policy, international cyber diplomacy, and global cyber governance.

In your answer, pay attention to actors, levels of decision-making, and instruments of influence.

Maximum — 10 points for the question.

Approved at the meeting of the Department of International Relations and Political Philosophy, protocol № 1, dated «22» August 2025.

Examiner Lecturer Danylo Nepochatov

Head of the Department Doctor of Philosophy Professor Oleh Kuz

THE ASSESSMENT CRITERIA

Criteria for Assessing Individual Analytical Tasks

2-point assessment scale

(basic tasks on data collection, structuring, and primary visualisation)

Level of Performance	Points
Data are collected correctly and in full; the dataset structure meets the requirements (country–year format, correct variables); visualisations correspond to the data; no critical errors are present.	2
Data are collected correctly and in full; the dataset structure meets the requirements (country–year format, correct variables); visualisations correspond to the data; no critical errors are present.	1

3-point assessment scale

(comparative analysis, time trends, correlations, event analysis)

Level of Performance	Points
The analysis is carried out correctly; data are used in accordance with the task; appropriate methods are applied; results are interpreted logically; a short analytical conclusion is formulated.	3
The analysis is generally correct, but some methodological, technical, or interpretative inaccuracies are present; conclusions are superficial but linked to the obtained data.	2
The analysis is generally correct, but some methodological, technical, or interpretative inaccuracies are present; conclusions are superficial but linked to the obtained data.	1

4-point assessment scale

(cluster / PCA analysis, nonlinear models, text-as-data, policy brief)

Level of Performance	Points
The analysis is carried out correctly; an appropriate method is applied (PCA, clustering, LOESS/GAM, text-as-data); the code is reproducible; visualisations are informative; results are interpreted analytically; a meaningful conclusion is provided.	4
The analysis is generally correct; the method is applied properly, but the interpretation is partially superficial or incomplete; minor technical inaccuracies may be present.	3
The analysis is completed partially; the method is applied formally or with errors; visualisations or interpretation are incorrect.	2

The analysis is incorrect or formal; the code is not reproducible; results are not related to the data or are absent.	1

Criteria for Assessing the Analytical Group Project

18-point assessment scale

Level of Performance	Points
Data are collected correctly and in full; the panel dataset is structured; the R analysis is fully reproducible; several types of analysis are applied (comparative, time-series, correlation, nonlinear, text-as-data, or event-based); analytical conclusions logically follow from empirical results; the final analytical document and presentation demonstrate a coherent synthesis of results.	18
The project is completed at a very high level; data are complete; the analysis is reproducible; at least three types of analysis are applied; interpretation is correct, but synthesis of results is less deep.	17
The project is of high quality and well structured; the main stages of analysis are performed correctly; visualisations are informative; analytical conclusions are formulated but partially descriptive.	16
The project generally meets the requirements; data are collected correctly; the analysis is conducted, but some technical or analytical shortcomings are present; reproducibility of the code is partial.	15
The project is completed at a sufficient level; the data corpus is limited in volume or diversity; the analysis is correct but without deep synthesis; the link between data and conclusions is traceable.	14
The project demonstrates a basic understanding of the task; the analysis is fragmentary; a limited number of methods is used; interpretation is predominantly descriptive.	13
The project is completed partially; data or analysis are incomplete; the computational approach is applied selectively; conclusions are weakly connected to the results.	12
The project is completed partially; data or analysis are incomplete; the computational approach is applied selectively; conclusions are weakly connected to the results.	11
The project is fragmentary; data or code are presented incorrectly; reproducibility of the analysis is absent; analytical conclusions are not formulated.	10
The project is completed formally; separate charts or tables are presented without a coherent analytical logic.	9
The project demonstrates minimal understanding of the task; data are collected partially; analysis is unsystematic; conclusions are declarative.	8
The project contains serious conceptual and methodological errors; data and analysis do not correspond to the task.	7
The project is fragmentary and unsystematic; most mandatory components are missing.	6
The project shows signs of purely formal completion; the analysis is unsuitable for interpretation.	5
The project almost does not meet the requirements; separate materials are submitted without an analytical connection.	4
The project does not reflect the content of the task; data and analysis are irrelevant.	3

The project is essentially not completed; structured data and analysis are absent.	2
Submitted materials lack substantive content and are unsuitable for assessment.	1

Criteria for Assessing the Practical Task in the Examination Card

15-point assessment scale

Level of Performance	Points
The task is completed fully and at a high level. The type of analysis (comparative, time-series, correlation, nonlinear, or event-based) is selected correctly and clearly justified with regard to the structure of the international cybersecurity dataset. The pseudocode is logical, consistent, and reflects the full analysis cycle (data preparation, aggregation, calculation, visualisation). The empirical pattern (trend, asymmetry, nonlinearity, anomaly) is described correctly and linked to the selected type of analysis.	15
The type of analysis is identified correctly; the justification is generally convincing. The pseudocode is logical but includes minor simplifications or omissions of individual analytical steps. The empirical pattern is described correctly, but the interpretation is less detailed.	14
The type of analysis is selected appropriately, but the justification is partially superficial. The pseudocode is understandable but presented in a shortened form. The empirical pattern is described in general terms without detail.	13
The type of analysis is selected appropriately; however, the logic of the choice is explained incompletely. The pseudocode is fragmentary but demonstrates an understanding of data processing and counting principles. The empirical pattern is formulated descriptively.	12
Partial understanding of types of international cybersecurity data analysis is demonstrated. The pseudocode contains logical inaccuracies or omits key stages. The pattern is defined unclearly or without a clear link to the data.	11
The type of analysis is identified formally, without in-depth justification. The pseudocode is schematic and describes the general idea of analysis without a clear structure. The pattern is described in very general terms.	10
An attempt to select the type of analysis is present, but with methodological inaccuracies. The pseudocode is inconsistent or incomplete. Interpretation of the empirical pattern is weak.	9
The task is completed partially. The type of analysis is identified incorrectly or without explanation. The pseudocode does not allow the logic of the analysis to be reproduced. The pattern is formulated superficially.	8
The analysis and pseudocode are presented fragmentarily. The link between data, method, and conclusions is weak or absent.	7
Formal completion of the task. The pseudocode is incorrect or does not correspond to the task. The empirical pattern is not explained.	6
Only separate elements of the answer are present (the name of the analysis or a general idea of calculation) without logic.	5
A superficial attempt at an answer with significant logical errors.	4
The task is completed incorrectly; there is no understanding of computational logic.	3
Minimal, random fragments of an answer without substantive content.	2
The task is essentially not completed.	1

Criteria for Assessing the Theoretical Task in the Examination Card

15-point assessment scale

Level of Performance	Points
correct and logically consistent R code is proposed, implementing the full analysis cycle (variable selection, grouping, counting, obtaining results). The code is aligned with the dataset structure and allows the analysis to be reproduced.	15
The R code is generally correct; the counting logic is preserved. Minor syntactic or structural inaccuracies are present but do not undermine the analytical idea.	14
The code is correct in essence but presented in a shortened form (some steps are omitted or implicitly defined). The principle of data aggregation is clear.	13
The code is correct in essence but presented in a shortened form (some steps are omitted or implicitly defined). The principle of data aggregation is clear.	12
Partial understanding of computational logic is demonstrated; the code is fragmentary or inconsistent.	11
The code is schematic, describing the idea of counting, but cannot be directly executed or reproduced.	10
Only a general approach to counting is provided without correct implementation in R.	9
The R code contains logical errors that prevent obtaining a correct result.	8
Formal completion of the task; the code does not correspond to the stated analytical task.	7
Separate R commands are provided without logical connections between them.	6
A minimal attempt at an answer; the code is unsuitable for interpretation.	5
Significant misunderstandings of data analysis principles are evident.	4
The code does not perform counting of mentions or frequencies.	3
Random or irrelevant code fragments are provided.	2
The task is essentially not completed.	1

Criteria for Assessing the Heuristic Task in the Examination Card

10-point assessment scale

Level of Performance	Points
The answer is complete, logically structured, and conceptually correct. The role of cyber diplomacy in international cybersecurity is explained; correct concepts are used; relevant examples from international practice are provided.	10
The answer is well-argued; examples are appropriate, but analytical depth is somewhat limited.	9
The answer is generally correct; concepts are used properly, but without extended examples.	8
Understanding of key ideas is demonstrated; argumentation is superficial.	7

Partial understanding of the topic; inaccuracies in definitions or examples are present.	6
Partial understanding of the topic; inaccuracies in definitions or examples are present.	5
Fragmentary knowledge; weak structure of the answer.	4
Significant conceptual errors; incorrect understanding of the role of media.	3
Minimal, superficial understanding of the topic.	2
The answer does not correspond to the content of the question.	1

RECOMMENDED LITERATURE

Main

1. International Relationships and World Policy / O. Kuz et al. Kharkiv : Simon Kuznets Kharkiv National University of Economics. Kharkiv, 2020. 200 p. URL: https://repository.hneu.edu.ua/handle/123456789/25295.
2. Topor L. Cyber sovereignty. Cham: Springer Nature Switzerland, 2024. URL: https://doi.org/10.1007/978-3-031-58199-1

Additional

3. Brovko O. Local government resilience in the face of Russian aggression: the case of Ukraine. Territory, Politics, Governance. 2024. P. 1–20. URL: https://repository.hneu.edu.ua/handle/123456789/32772.
4. Kuz O., Konnova N., Korotkov D. Corruption Models of Behaviour in the Structure of the Political System of Society. Dialogue and Universalism. 2024. Vol. 34, no. 1. P. 131–141. URL: https://repository.hneu.edu.ua/handle/123456789/32650
5. Kleiner J. How political regimes affect national cybersecurity: the polity flux effect. Democratization. 2025. P. 1–32. URL: https://doi.org/10.1080/13510347.2025.2451951
6. Steen S., Janet M B. Cognitive Warfare. Brussels, 2025. 24 p. URL: https://www.sto.nato.int/document/cognitive-warfare/.
7. Ünver H. A. Computational International Relations What Can Programming, Coding and Internet Research Do for the Discipline?. All Azimuth: A Journal of Foreign Policy and Peace. 2018. URL: https://doi.org/10.20991/allazimuth.476433

Information resources

8. The World Factbook - The World Factbook. We are the Nation's first line of defense - CIA. URL: https://www.cia.gov/the-world-factbook/
9. Britannica. Britannica. URL: https://www.britannica.com .
10. Atlantic Council. *Atlantic Council*. URL: http://www.atlanticcouncil.org
11. Brookings - Quality. Independence. Impact. Brookings. URL: https://www.brookings.edu