МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Кафедра міжнародних комунікацій та політичного аналізу

СИЛАБУС
вибіркової навчальної дисципліни
«ІНФОРМАЦІЙНА ПОЛІТИКА ТА НАЦІОНАЛЬНА БЕЗПЕКА ЄС»

Підготовки доктора філософії
галузі знань 29 «Міжнародні відносини»
Спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітньо-наукової програми «Міжнародна відносини та стратегічні комунікації України та ЄС»

Розробник: к. геогр. н., доц. Федонюк Сергій Валентинович

Силабус навчальної дисципліни затверджено на засіданні кафедри міжнародних комунікацій та політичного аналізу, протокол № № 13 від "22" червня 2022 року
Завідувач кафедри: Карпчук Н.П.

Гарант
освітньо-наукової програми
«Міжнародна відносини та стратегічні комунікації України та ЄС»

Шуляк А.М.

СИЛАБУС

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітня програма, освітній ступінь</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td rowspan="2">форма навчання очна</td><td rowspan="5">галузь знань 29 Міжнародні відносини, спеціальність 291 "Міжнародні відносини, суспільні комунікації та регіональні студії", освітньо-професійна програма «Міжнародні відносини та стратегічні комунікації», доктор філософії</td><td>Вибіркова</td></tr>
<tr><td>Рік навчання 1</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 120/4</td><td>Семестр 2</td></tr>
<tr><td>Лекції 10</td></tr>
<tr><td rowspan="2">ІНДЗ: Є</td><td>Практичні (семінарські) 14</td></tr>
<tr><td>Самостійна робота 88</td></tr>
<tr><td colspan="2">Мова викладання</td><td>Консультації 8</td></tr>
<tr><td colspan="2"></td><td>Форма контролю: залік</td></tr>
<tr><td colspan="2"></td><td>Українська</td></tr>
</table>

1. **ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА**	
ВИКЛАДАЧ	Федонюк Сергій Валентинович
КОНТАКТНІ ДАНІ	Sergii.fedoniuk@vnu.edu.ua
КОМПЕТЕНЦІЇ ТА ДАНІ ПРО ВИКЛАДАЧА	Кандидат географічних наук, доцент кафедри міжнародних комунікацій та політичного аналізу. Тематика наукових досліджень: інформаційна політика та безпека міжнародних акторів, стратегічні комунікації, масове співробітництво.
2.ОПИС КУРСУ	
ПЕРІОД РЕАЛІЗАЦІЇ КУРСУ	II семестр 2022 - 2023 навчальний рік
ОРГАНІЗАЦІЙНА СТРУКТУРА	Кафедра міжнародних комунікацій та політичного аналізу, факультет міжнародних відносин
АНОТАЦІЯ КУРСУ	Курс «Інформаційна політика та національна безпека ЄС» призначений для знайомства аспірантів з політологічними і нормативними підходами, сучасними тенденціями в оцінці значення інформаційної політики та проблеми інформаційної безпеки в міжнародному політичному процесі за участі Європейського Союзу і його членів. Дає змогу визначити місце, особливості та основні тенденції трансформації глобальної безпеки в зв'язку з загальною інформатизацією, революцією у військовій справі і формуванням інформаційного суспільства, а також впливом цих тенденцій на зовнішню політику України та інших держав.
ФОРМА	*(лекції, практичні заняття)*

РЕАЛІЗАЦІЇ	
МЕТОДИ ТА ФОРМИ ОЦІНКИ РОБОТИ СТУДЕНТІВ	Підсумкова оцінка складається з таких компонентів: присутність і активність на заняттях (на основі кількісних даних, отриманих за допомогою опції “Insights” команди Microsoft Teams, до 20 балів), обговорення теоретичних питань (до 20 балів), виконання практичних завдань (до 20 балів), виконання тестових завдань (до 20 балів) і виконання ІНДЗ (до 20 балів). **Затримки виконання:** допускається за умови наявності непереборних обставин, що перешкоджали вчасному представленню, що підтверджується документально (наприклад, довідка лікаря). **Повторне оцінювання:** допускається на підставі обґрунтованого письмового звернення студента (електронною поштою або в дописах команди MSTeams), але не пізніше як протягом одного тижня після основного оцінювання. **Політика відвідування та / або участі:** відвідування та активна участь є оцінюваною складовою курсу
ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦПЛІНИ	**Навчання відбувається із використанням цифрової платформи Microsoft 365.** Усі аудиторні заняття відбуваються із онлайн-включенням учасників у команді MSTeams. **Відвідування та / або участь:** відвідування та активна участь є класифікованою складовою курсу, що оцінюється. Дистанційна он-лайн участь здобувача допускається за умови наявності у нього відповідних технічних засобів. **Академічна доброчесність та співпраця:** не допускається порушення норм авторського права, у разі виявлення плагіату письмова робота студента не оцінюється. Заохочується групова робота із презентацією її результатів у розділі “Простір для співпраці” персональних електронних блокнотів здобувачів. **Здобувачі з обмеженими можливостями:** можуть брати дистанційну (онлайн) участь на підставі особистого звернення. Заява про стан здоров’я студентів: у випадку погіршення стану здоров’я здобувач, на підставі особистого письмового звернення (електронною поштою або в дописах команди MS Teams може брати дистанційну онлайн-участь у заняттях. **Мобільні пристрої:** заохочується використання мобільних пристроїв, - застосовується підхід BYOD (Bring Your Own Device).
МЕТА І ЗАВДАННЯ І КУРСУ	Метою курсу є формування компетентностей для дослідження й роботи у сферах, пов’язаних з інформаційною політикою ЄС у безпекових аспектах. Основними завданнями курсу є: вивчення нормативних та інституційних основ інформаційної політики ЄС, спільної політики безпеки й оборони ЄС, зокрема стратегічних комунікацій; вивчення основ міжнародної політики й стратегії ЄС у сфері інформаційної (кібер) безпеки; ознайомлення з особливостями національних політик членів ЄС у зазначених сферах.

ПРЕРЕКВІЗИТИ	Необхідне розуміння базових основ функціонування Європейського Союзу, міжнародної політики.
ПОСТРЕКВІЗИТИ	Цей курс є базовим для наступного формування компетентностей у сфері інформаційної безпеки, стратегічних комунікацій ЄС, вивчення сучасних проблем міжнародних відносин та глобального розвитку.

3 .СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин				
	Усього	у тому числі			
		Лек.	Сем, практ.	Сам. роб	Консул.
1	2	3	4	5	6
Змістовий модуль 1. Інформаційна політика та безпека в міжнародних відносинах					
Тема 1. Інформаційна політика та безпека: підходи і концепції		2		6	2
Тема 2. Ініціативи в галузі інформаційної політики й безпеки			2	10	
Тема 3. Переговорний процес і міжнародне співробітництво в галузі забезпечення інформаційної безпеки. Позиція ЄС.		2	2	8	
Разом за змістовим модулем 1		4	4	24	2
Змістовий модуль 2. Політики ЄС у сферах інформації, комунікацій та інформаційної (кібер) безпеки					
Тема 4. Секторальні й галузеві політики у сфері інформації та телекомунікацій		1	1	8	2
Тема 5. Інформаційно-комунікаційні аспекти безпекової стратегії ЄС		1	1	8	2
Тема 6. Безпековий вимір політики. Стратегічні комунікації, протидія дезінформації та гібридним загрозам			2	8	
Разом за змістовим модулем 2		2	4	24	4
Змістовий модуль 3. Міжнародна активність ЄС у сферах інформаційної (кібер) безпеки					
Тема 7. Міжнародна стратегія ЄС: основні напрями		1	1	8	
Тема 8. Відносини зі США і НАТО		1	1	8	
Тема 9. Відносини Україна-ЄС		2	2	14	2
Тема 10. Особливості національних стратегій членів ЄС			2	10	
Разом за змістовим модулем 3		4	6	40	2
Усього години		10	14	88	8

4. ТЕМАТИКА СЕМІНАРІВ / ПРАКТИЧНИХ / ЛАБОРАТОРНИХ РОБІТ

Назви змістових модулів і тем	год.
Змістовий модуль 1. Інформаційна політика та безпека в міжнародних	

відносинах Тема 2. Ініціативи в галузі інформаційної політики й безпеки *Семінар* 1. Концепції інформаційної (кібер) політики та безпеки 2. Об'єкти інформаційної безпеки 3.Загрози воєнно-політичного характеру, пов'язані з інформацією 4. Міжнародно-правова проблематика інформаційної (кібер) безпеки 5. Підходи ЄС у сфері інформаційної (кібер) безпеки *Практичне завдання* - Навести визначальні характеристики кожної з домінуючих концепцій інформаційної безпеки. Доповнити посиланнями на відповідні первинні документи.	2
Тема 3. Переговорний процес і міжнародне співробітництво в галузі забезпечення інформаційної безпеки. Позиція ЄС. *Семінар* 1. Діяльність РФ і США на рівні ООН 2. Переговорні треки в ООН 3. Активність головних міжнародних акторів на рівні регіональних організацій 4. Підхід і позиція ЄС у міжнародних процесах у сфері інформаційної (кібер) безпеки 5. Ініціативи ЄС на рівні ООН *Практичне завдання* - Скласти порівняльну характеристику підходів РФ, США та ЄС на основі, відповідно, документів ООН: *Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности (Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года); Advancing responsible State behaviour in cyberspace in the context of international security (Resolution adopted by the General Assembly on 22 December2018); The future of discussions on ICTs and cyberspace at the UN.*	2
Змістовий модуль 2. Політики ЄС у сферах інформації, комунікацій та інформаційної (кібер) безпеки Тема 4. Секторальні й горизонтальні політики у сфері інформації та телекомунікацій *Семінар* 1. Нормативна й інституційна основа політик ЄС 2. Секторальні політики, зокрема інформаційно-комунікаційні технології, цифрова економіка та суспільство, захист даних, підтримка аудіовізуального сектора, культура й ЗМІ	1
Тема 5. Інформаційно-комунікаційні аспекти безпекової стратегії ЄС *Семінар* 1. Розвиток стратегії ЄС у сфері кібербезпеки 2. Актуальна стратегія ЄС у сфері кібербезпеки 3. Стратегічні інвестиційні програми у сферах, пов'язаних з інформацією й телекомунікаціями 4. Безпекова стратегія "Стратегічний Компас" 5. Розвиток безпекової стратегії у відповідь на воєнну загрозу з боку РФ *Практичне завдання* - Виділити компоненти стратегії "Стратегічний компас", пов'язані з політикою ЄС у сферах, пов'язаних з інформацією та інформаційною (кібер) безпекою	1

Тема 6. Безпековий вимір політики. Стратегічні комунікації, протидія дезінформації та гібридним загрозам *Семінар* 1. Спільна політика безпеки і оборони ЄС (CSDP) 2. Реалізація стратегічних комунікацій ЄС в секторі CSDP 3. Протидія дезінформації і гібридним загрозам *Практичне завдання* - Скласти схему "Організація стратегічних комунікацій в системі CSDP"	2
Змістовий модуль 3. Міжнародна активність ЄС у сферах інформаційної (кібер) безпеки	
Тема 7. Міжнародна стратегія ЄС: основні напрями *Семінар* 1. Основні інтереси й напрями міжнародної політики ЄС у сферах інформації та кібербезпеки 2. Інформаційна політика в Глобальній стратегії ЄС 3. Інституційна й правова основа безпекової міжнародної співпраці ЄС у сферах, повязаних з ІКТ	1
Тема 8. Відносини зі США й НАТО *Семінар* 1. Взаємодія ЄС і США у сферах, пов'язаних з інформаційною (кібер) безпекою 2. Стратегічне партнерство ЄС і НАТО у сферах протидії гібридним загрозам, кібербезпеки й оборони 3. Політика ЄС щодо кібероборони і взаємодія у цій сфері з НАТО	1
Тема 9. Відносини Україна-ЄС *Семінар* 1. Підходи в національній політиці України в сфері інформації та інформаційної (кібер) безпеки 2. Розвиток взаємодії між Україною та ЄС у сфері інформаційної (кібер) безпеки 3. Співпраця у рамках "Кібердіалогу Україна - ЄС" 4. Виклики й перспективи взаємодії України та ЄС у зв'язку зі збройною агресією РФ проти України 5. Перспективні заходи у сферах, пов'язаних з інформацією та інформаційною (кібер) безпекою у зв'язку з набуттям Україною статусу члена ЄС *Практичне завдання* - Підготувати перелік необхідних заходи політики у сферах, пов'язаних з інформацією та інформаційною (кібер) безпекою у зв'язку з реалізацією курсу на набуття членства України в ЄС	2
Тема 10. Особливості національних стратегій членів ЄС *Семінар* 1. Стратегія у сфері інформаційної (кібер) безпеки одного із членів ЄС (на вибір здобувача) 2. Співпраця України з країною (членом ЄС) у сфері інформаційної (кібер) безпеки (на вибір здобувача)	2
Усього годин	14

5. РЕЗУЛЬТАТИ НАВЧАННЯ

	Інтегральна	Загальні	Фахові
	зазначення коду критерію+опис	*зазначення коду критерію+опис*	*зазначення коду критерію+опис*
Компетентності	Здатність розв’язувати складні задачі і проблеми у галузі міжнародних відносин, суспільних комунікацій та регіональних студій, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.	Знання та розуміння предметної області та розуміння професійної діяльності. Здатність працювати в міжнародному контексті. Здатність використовувати інформаційні та комунікаційні технології Здатність до пошуку, оброблення та аналізу інформації з різних джерел. Володіння основними методами, способами і засобами отримання, зберігання, переробки інформації, навичками роботи з комп'ютером як засобом управління інформацією; здатністю працювати з інформацією в глобальних комп'ютерних мережах. Уміння системно мислити, ставити цілі і вибирати шляхи їх досягнення, вміння знаходити міжнародно-політичні і дипломатичні смислові навантаження проблем і процесів. Здатність ясно, логічно правильно і аргументовано будувати усну і письмову мову у відповідній професійній області. Здатність розуміти суть і значення інформації в розвитку сучасного інформаційного суспільства, усвідомлювати небезпеку і загрози, що виникають в	Здатність аналізувати міжнародні процеси у різних контекстах, зокрема політичному, безпековому, правовому, економічному, суспільному, культурному та інформаційному. Здатність аналізувати вплив світової економіки, міжнародного права та внутрішньої політики на структуру й динаміку міжнародних відносин та зовнішньої політики держав. Здатність розуміти логіку глобальних та інтеграційних процесів і розвитку всесвітньої політичної системи міжнародних відносин в їх історичній, економічній та правовій обумовленості. Здатність володіти базовими навичками прикладного аналізу міжнародних ситуацій. Здатність розуміти зміст програмних документів з проблем зовнішньої політики України, уміння професійно грамотно аналізувати і пояснювати позиції України з основних міжнародних проблем.

		цьому процесі, дотримуватися основних вимог інформаційної безпеки, в тому числі захисту державної таємниці.	

Програмні результати	*зазначення коду критерію*	*опис*
		Знати та розуміти природу та динаміку міжнародної безпеки, розуміти особливості її забезпечення на глобальному, регіональному та національному рівні, знати природу та підходи до вирішення міжнародних та інтернаціоналізованих конфліктів.
		Знати природу та характер взаємодій окремих країн та регіонів на глобальному, регіональному та локальному рівнях, зокрема на рівні ЄС.
		Знати основні процеси, пов'язані з загальною інформатизацією; місце інформаційної політики та безпеки в світових політичних процесах; логіку зміни і розвитку проблеми інформаційної безпеки.
		Вміти співвідносити інтеграційні процеси в Європі й процеси інформатизації; визначати характер загроз, пов'язаних з процесом інформатизації.

6. ЗАПИТАННЯ ДЛЯ ПІДГОТОВКИ ІНДЗ

(ІНДЗ - коротке дослідження обсягом 1000-2000 слів по суті питання)

1. На яких принципах ґрунтується політика Європейського Союзу у сфері інформаційної безпеки?
2. Яку роль відіграє політика кібербезпеки в Глобальній стратегії ЄС?
3. Як розвивається політика кібербезпеки ЄС?
4. Які головні положення Стратегії кібербезпеки ЄС для цифрового десятиліття (2020 р.)?
5. Які пріоритети в політиці кібербезпеки ЄС актуалізуються із прийняттям стратегії “Цифровий компас: європейський шлях до Цифрового десятиліття”?
6. На яких концептуальних підходах засновано сучасну стратегію ЄС у сфері кібербезпеки?
7. У чому суть пропозиції Програми дій для просування відповідальної поведінки держав у кіберпросторі і яка роль ЄС у її просуванні?
8. Яка концептуальна позиція Європейського Союзу щодо політики у сфері безпеки кібер-простору?
9. Як узгоджуються зусилля ЄС і США у сфері міжнародної взаємодії щодо боротьби з кіберзлочинністю?
10. Які інституції функціонують у сфері співпраці ЄС і США щодо протидії кібер-загрозам?
11. Як здійснюється практична взаємодія ЄС і США і запозичення досвіду у сфері протидії кібер-загрозам?

12. Які розбіжності існують у підходах ЄС і США до політики безпеки кіберпростору?
13. Які проблеми безпеки кіберпростору покликана розв'язати кіберстратегія ЄС шляхом міжнародної взаємодії?
14. Які головні регіональні напрями міжнародної співпраці ЄС у сфері розвитку потенціалу протидії кібер-загрозам?
15. Які головні напрями співпраці держав ЄС у сфері кібербезпеки й оборони?

7. РОЗПОДІЛ БАЛІВ

<table>
<tr><th colspan="10">Модуль 1. Поточний контроль</th><th rowspan="2">Модуль 2 ІНДЗ</th><th rowspan="2">Модуль 3. Виконання тестових завдань</th><th rowspan="2">Модуль 4. Присутність і активність на заняттях</th><th rowspan="2">Сума балів</th></tr>
<tr><th colspan="3">Змістовий модуль 1</th><th colspan="3">Змістовий модуль 2</th><th colspan="4">Змістовий модуль 3</th></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="10">Обговорення теоретичних питань</td><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td></td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>4</td></tr>
<tr><td colspan="10">Виконання практичних завдань</td></tr>
<tr><td></td><td>4</td><td>4</td><td></td><td>4</td><td>4</td><td></td><td></td><td>4</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="10">40</td><td>20</td><td>20</td><td>20</td><td>100</td></tr>
</table>

8. ШКАЛА ОЦІНЮВАННЯ

Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою для екзамену
90 – 100	Зараховано
82 – 89	Зараховано
75 81	Зараховано
67 74	Зараховано
60 66	Зараховано
1 – 59	Незараховано

9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Методичне забезпечення	Методичне забезпечення знаходиться в команді учасників вивчення курсу (MSTeams) *Основний навчальний посібник* Федонюк Сергій. Міжнародна політика інформаційної (кібер) безпеки. 88 питань і відповідей : навч. посіб. / С. В. Федонюк. − Луцьк: Вежа-друк, 2022. – 1 електрон. опт. диск (CD-ROM).
Основна	1. Федонюк С. Передумови та етапи перебігу інтеграційних процесів у Європі, Цифрова економіка, Регіональна політика // Європейський Союз: навч. посіб / [А. О. Бояр (кер. авт. кол.), С. В. Федонюк, А. А. Моренчук та ін.] ; за ред. А. О. Бояра, С. В. Федонюка. Київ : ФОП Маслаков, 2020. 600 с. (9-31, 251-264, 336-350) 2. Федонюк Сергій. Міжнародні аспекти безпеки кіберпростору : монографія / С. В. Федонюк. – Луцьк : Вежа-Друк, 2022. – 1 електрон.

	опт. диск (CD-ROM). – Об'єм даних 4,72 Мб. ISBN 978-966-940-406-0 3. Федонюк Сергій (2021). Політика ЄС в аспекті основних глобальних концепцій інформаційної (кібер) безпеки, Міжнародні відносини, суспільні комунікації та регіональні студії, № 3 (11) 4. Федонюк Сергій, Карпук Юрій (2022). Концепції інформаційної безпеки в аспекті інтересів основних міжнародних акторів, Міжнародні відносини, суспільні комунікації та регіональні студії, № 2 (13). 5. Федонюк Сергій, Карпук Юрій (2022). Розвиток концепції стратегічних комунікацій ЄС, Міжнародні відносини, суспільні комунікації та регіональні студії, № 3 (14).
Додаткова	1. Фролова О. (2019). Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. *Вісник Львівського університету. Серія: Міжнародні відносини*. Вип. 46. С. 123–136. URL: http://nbuv.gov.ua/UJRN/VLNU_Mv_2019_46_13 2. Kushnir, V. (2020). Proposals for improving the legal mechanism on strategic communications in the armed forces of Ukraine, *Derzhavne upravlinnya: udoskonalennya ta rozvytok*. Vol. 10, URL: http://www.dy.nayka.com.ua/?op=1&z=1796 3. Géry Aude (2020). A New UN Path to Cyber Stability. Directions. Cyber Digital Europe, 6 October 2020. URL: https://directionsblog.eu/a-new-un-path-to-cyber-stability/ 4. Taylor Emily, Hoffmann Stacie (2019). EU–US Relations on Internet Governance. Chatham House. URL: https://www.chathamhouse.org/publication/eu-us-relations-internet-governance. [Google Scholar] 5. Даценко А. Ю. Європейський досвід протидії російській дезінформації періоду другої «холодної віний».Міжнародні відносини. Серія «Політичні науки».No 18–19 (2018). URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3381
Документи	1. 73/266. Advancing responsible State behaviour in cyberspace in the context of international security. Resolution adopted by the General Assembly on 22 December 2018. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266 2. EU Cyber Security strategy: An open, safe and secure Cyberspace. 7 February, 2013.URL:https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en210 3. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe /* COM/2015/0192 final */. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192211 4. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE ANDTHE COMMITTEE OF THE REGIONS The European Agenda on Security. Strasbourg, 28.4.2015 COM(2015) 185 final.URL:https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf212

5. Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy. June 2016.URL:https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf
6. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
7. Cybersecurity package 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'. Publication 19 September 2017.URL:https://digital-strategy.ec.europa.eu/en/library/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu216
8. The EU's Cybersecurity Strategy for the Digital Decade. European Commission. Publication 16 December 2020.URL:https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0217
9. Revised Directive on Security of Network and Information Systems (NIS2). European Commission. Publication 16 December 2020.URL:https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2218
10. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities. Brussels, 16.12.2020 COM(2020) 829 final.URL:https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf
11. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. European Commission. 16 December 2020.URL:https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391220
12. Bucharest-based Cybersecurity Competence Centre gets green light from Council. European Council. 20 April 2021.URL:https://www.consilium.europa.eu/en/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/
13. European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)).URL:https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html222
14. The Recovery and Resilience Facility. European Commission.URL:https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en
15. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 2030 Digital Compass: the European way for the Digital Decade. COM/2021/118 final.URL:https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

16. The future of discussions on ICTs and cyberspace at the UN. Updated version: 10/08/2020.URL:https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf
17. Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats. European Commission. MEMO/11/246 Brussels, 14th April 2011. URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_11_246
18. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Report on implementation of the EU's Cybersecurity Strategy for the Digital Decade. Brussels, 6.8.2021 JOIN(2021) 14 final/2. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=JOIN:2021:14:REV1&rid=1302
19. EU priorities at the United Nations during the 76th United Nations General Assembly, September 2021 -September 2022 -Council conclusions (12 July 2021). Brussels, 12 July 2021. URL: https://data.consilium.europa.eu/doc/document/ST-10393-2021-INIT/en/pdf
20. US support to the Budapest Convention. Council of Europe. Strasbourg, 25 September 2018. URL: https://www.coe.int/en/web/cybercrime/-/us support-to-the-budapest-convention307
21. Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats. European Commission. MEMO/11/246 Brussels, 14th April 2011. URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_11_246
22. EU-US WORKING GROUP ON CYBER-SECURITY AND CYBER-CRIME -CONCEPT PAPER. 13 April 2011.URL:https://www.statewatch.org/media/documents/news/2011/apr/eu-us-2011-04-13-concept-paper-cybersecurity.pdf
23. EU-U.S. Cyber Dialogue Bruxelles, 16/12/2016 -23:00 -UNIQUE ID: 161223_8. URL: https://www.statewatch.org/media/documents/news/2016/dec/eu-eeas-eu-us-cyber-dialogue-pr-16-12-16.pdf315
24. Directive(EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high commonlevel of security of network and information systems across the Union.URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG316
25. EU-U.S. Cyber Dialogue Bruxelles, 16/12/2016 -23:00 -UNIQUE ID: 161223_8. URL: https://www.statewatch.org/media/documents/news/2016/dec/eu-eeas-eu-us-cyber-dialogue-pr-16-12-16.pdf
26. Coordinated action cuts off access to vpn service used by ransomware groups.EUROPOL. Press Release. 30 June 2021.URL:https://www.europol.europa.eu/newsroom/news/coordinated-action-cuts-access-to-vpn-service-used-ransomware-groups
27. EU Data Protection Rules and U.S. Implications. Congressional Research Service. July 17, 2020. URL: https://sgp.fas.org/crs/row/IF10896.pdf324
28. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND

THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. European Commission. Brussels,16.12.2020 JOIN(2020) 18 final. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164327
29. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats. European Commission. Brussels, 6.4.2016 JOIN(2016) 18 final.URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN
30. EU External Cyber Capacity Building Guidelines. Council of the European Union. Brussels, 26 June 2018.URL:https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf330
31. EU CyberNet –the bridge to cybersecurity expertise in the European Union.URL:https://www.eucybernet.eu/
32. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. European Commission. Brussels, 13.9.2017 JOIN(2017) 450 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN
33. EU CyberNet work in Dominican Republic, first national cybersecurity exercise “Cyber llamas”. EU CyberNet. 21.05.2021.URL:https://www.eucybernet.eu/eu-cybernet-work-in-dominican-republic-first-national-cyber-llamas-exercise/335
34. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. European Commission. Brussels, 16.12.2020 JOIN(2020) 18 final. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164336
35. JOINT DECLARATION BY THE PRESIDENT OF THE EUROPEAN COUNCIL, THE PRESIDENT OF THE EUROPEAN COMMISSION, AND THE SECRETARY GENERAL OF THE NORTH ATLANTIC TREATY ORGANIZATION.URL:https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf
36. EU Cyber Defence Policy Framework (2018 update). Council of the European Union. Brussels, 19 November 2018.URL:https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf338
37. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. European Commission. Brussels, 16.12.2020 JOIN(2020) 18 final.URL:https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164
38. Declaration on PESCO projects (2018) Declaration on PESCO projects (bijlage bij 21501-02,nr.1813).URL:https://www.consilium.europa.eu/media/32020/draft-pesco-declaration-clean-10122017.pdf.
39. *High Level Group on fake news and online disinformation- European Commission*. (2018). A multidimensional approach to disinformation—Report of the independent High Level Group on fake news and online disinformation DOI:10.2759/739290). URL:

https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b4cea-11e8-be1d-01aa75ed71a1
40. *Hybrid CoE.* (2019). Countering disinformation: News media and legal resilience [COI Records]. European Centre of Excellence and the Media Pool, part of the Finnish Emergency Supply Organization in Helsinki. URL: https://www.hybridcoe.fi/wp-content/uploads/2019/11/News-Media-and-Legal-Resilience_2019_rgb.pdf
41. *NATO StratCom CoE.* (2019). Hybrid Threats: A Strategic Communications Perspective. NATO. URL: https://www.stratcomcoe.org/download/file/fid/80212
42. *NATO StratCom CoE.* (2020). About Strategic Communications | StratCom. URL: https://www.stratcomcoe.org/about-strategic-communications
43. *European Commission and the High Representative.* (2019). EU-China—A strategic outlook. URL: https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategicoutlook.pdf
44. *European Commission and the High Representative.* (2020). Tackling Covid-19 disinformation—Getting the facts right. URL: https://ec.europa.eu/info/sites/info/files/communication-tackling-Covid-19-disinformationgetting-facts-right_en.pdf
45. *Nato Standard ajp-3.10.1* Allied Joint Doctrine for Psychological Operations. Edition B version 1. With uk national elements. September 2014. URL: url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf
46. *Office of the Secretary of Defense.* National Security Strategy. URL: https://history.defense.gov/Historical-Sources/National-Security-Strategy/
47. *NATO Deterrence and defence* URL: https://www.nato.int/cps/en/natohq/topics_133127.htm
48. The Interim National Security Strategic Guidance. *Congressional Research Service*, March 29, 2021. URL: https://sgp.fas.org/crs/natsec/IF11798.pdf
49. *ALLIED JOINT DOCTRINE FOR PSYCHOLOGICAL OPERATIONS—AJP-3.10.1 EDITION B.* URL: https://nso.nato.int/nso/nsdd/main/standards/stanag-details/8458/EN?tab=ratifications
50. *NATO* 2030: MAKING A STRONG ALLIANCE EVEN STRONGER. URL: https://www.nato.int/nato2030/
51. *G7*. (2018). Charlevoix Commitment on Defending Democracy from Foreign Threats. URL: https://www.mofa.go.jp/files/000373846.pdf
52. *Nato Standard ajp-3.10.1 Allied Joint Doctrine for Psychological Operations*. Edition B version 1. With uk national elements. September 2014. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf
53. *Shared vision, common action.* A stronger Europe : a global strategy for the European Union's foreign and security policy. URL: https://op.europa.eu/en/publication-detail/-/publication/3eaae2cf-9ac5-11e6-

868c-01aa75ed71a1
54. *European Union Institute for Security Studies.* (2016). EU strategic communications with a view to counteracting propaganda. European Parliament. URL: http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf
55. Strategic communications as a key factor in countering hybrid threats (2021) By VillarGarcía JuanPablo, Carlota Tarín Quirós, Blázquez Julio Soria, Galán Carlos Pascual, Galán Carlos Cordero. *STOA. European Union*. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)656323
56. Where will the EU's Strategic Compass point? *European Parliamentary Research Service,* (2021). URL: https://epthinktank.eu/2021/10/07/where-will-the-eus-strategic-compass-point/
57. Borrell Josep (2021) A Strategic Compass for Europe. URL: https://www.project-syndicate.org/commentary/eu-strategic-compass-by-josep-borrell-2021-11?barrier=accesspaylog
58. Questions and answers: a background for the Strategic Compass. *EEAS.* (2021). URL: https://eeas.europa.eu/headquarters/headquarters-homepage/97895/questions-and-answers-background-strategic-compass_en
59. A Strategic Compass for a stronger EU security and defence in the next decade. *Council of the EU. Press release.* (2022). URL: https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/
60. A Strategic Compass for Security and Defence—For a European Union that protects its citizens, values and interests and contributes to international peace and security URL: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf
61. EU Rapid Deployment Capacity. *EEAS factsheet* URL: https://www.eeas.europa.eu/eeas/eu-rapid-deployment-capacity_en
62. A Strategic Compass for the EU. *EEAS factsheet* URL: https://www.eeas.europa.eu/eeas/strategic-compass-eu-0_en
63. Organisation chart of the EEAS. *EEAS*, (2021). URL: https://eeas.europa.eu/headquarters/headquarters-homepage/3602/organisation-chart-eeas_en
64. Strategic communication. *EEAS*. URL: https://eeas.europa.eu/headquarters/headquarters-homepage/100/strategic-communications_en
65. Strategic Communication Press and Information Officer. *EEAC*. URL: https://eeas.europa.eu/headquarters/headquarters-homepage/83986/strategic-communication-press-and-information-officer_en
66. *Joint Communication to the European Parliament and the Council.* Joint Framework on countering hybrid threats a European Union response. Brussels, (2016) 18 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018
67. European Agenda on Security—Legislative documents. *European Commission*. URL: https://ec.europa.eu/home-affairs/what-we-

do/policies/internal-security/european-agenda-security-legislative-documents_en
68. EU Global Strategy. *EEAS*. URL: https://eeas.europa.eu/topics/eu-global-strategy_en
69. European Defence Action Plan. Roadmap. URL: https://ec.europa.eu/smart-regulation/roadmaps/docs/2016_grow_006_cwp_european_defence_action_plan_en.pdf82. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013) 1 final. URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
70. *Communication from the Commission to the European Parliament and the Council.* European Energy Security Strategy /* COM/2014/0330 final */. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52014DC0330
71. European Union Maritime Security Strategy as adopted by the Council (General Affairs) (June 2014). URL: https://data.consilium.europa.eu/doc/document/ST%2011205%202014%20INIT/EN/pdf
72. Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. Brussels, 6.4.2016 JOIN (2016) 18 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018
73. *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions.* Tackling online disinformation: a European Approach. COM/2018/236 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236
74. Questions & Answers: Reinforcing democracy and integrity of elections. *European Commission*, URL: https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_6212
75. European Democracy: Commission sets out new laws on political advertising, electoral rights and party funding. *European Commission.* URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6118
76. Code of Practice on Disinformation. *European Commission.* URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
77. *Joint Communication to the European Parliament, the European Council, the Council, the European Cconomic and Social Committee and the Committee of the Regions.* Action Plan against Disinformation. Brussels, 5.12.2018 JOIN (2018) 36 final. URL: https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf
78. Audit preview Information on an upcoming audit. EU action plan against disinformation. E*uropean Court of Auditors*, (2020). URL: https://www.eca.europa.eu/lists/ecadocuments/ap20_04/ap_disinformation_en.pdf