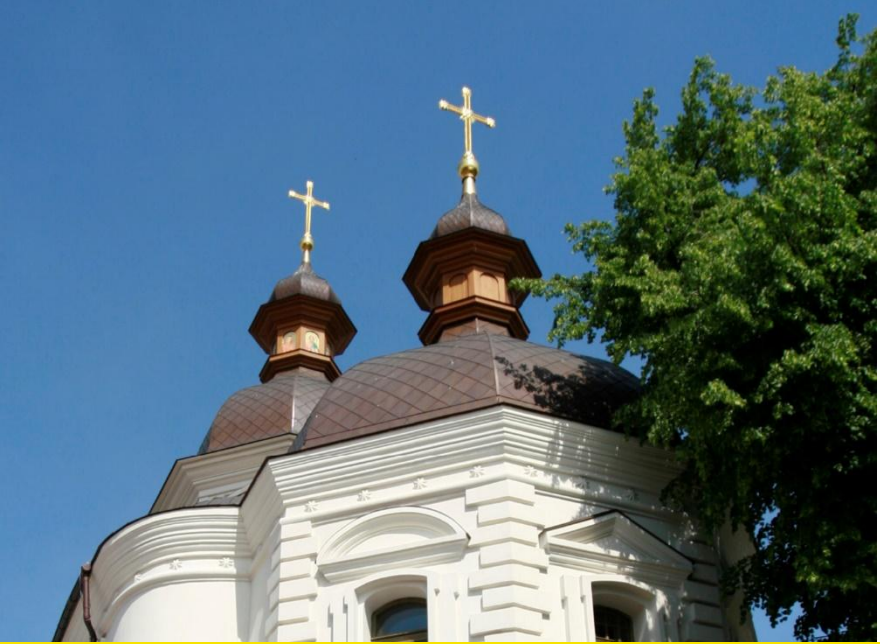
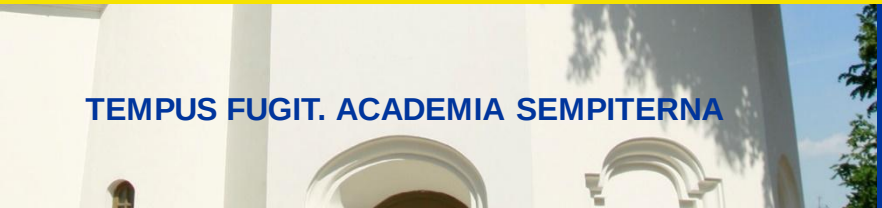


НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

Конкурси з тематичного напряму "Безпечні суспільства: захист свободи та безпеки Європи та її громадян " на 2020 рік програми "Горизонт 2020"



TEMPUS FUGIT. ACADEMIA SEMPITERNA

Підготовлено НКП НаУКМА

Загальна характеристика тематичного напряму

Security for all walks of life

Unit B4
Safeguarding
Secure Society

8 місій для напряму “Безпека”

1. Посилити стійкість Європи до криз та загроз (SU-DRS).
2. Захистити та покращити стійкість критичної інфраструктури, транспорту та ланцюгів промислового збуту (SU-INFRA or CIP).
3. Боротьба зі злочинністю, тероризмом, незаконним обігом, включно з розумінням та відстеженням ідей та вірувань терористів (SU-FCT).
4. Посилення безпеки шляхом ефективного управління кордонами (SU-BES).
5. Підтримка зовнішньої політики безпеки ЄС включно з попередженням конфліктів та мирного врегулювання (SU-BES).
6. Покращення кібербезпеки (SU-DS and SU-ICT).
7. Забезпечити недоторканність приватного життя та свободи, в тому числі в Інтернеті, та поглибити розуміння суспільством правових та етичних аспектів всіх ділянок безпеки, ризиків (SU-DS).
8. Підвищення стандартизації та операційної сумісності систем, в тому числі у надзвичайних ситуаціях.

Рекомендації European Security Research Advisory Board до проектів з Безпеки

- ❖ Дотримуватися підходу орієнтованого на визначені місії .
- ❖Посилювати залучення кінцевих споживачів до реалізації проекту.
- ❖Зблизити на європейському рівні “попит” та “пропозицію”.
- ❖Більше уваги приділяти соціальному виміру проблеми.
- ❖Пропонувати мультидисциплінарні проекти (інтеграція технологічних розробок з дослідженнями у галузі політичних, соціальних та гуманітарних наук).
- ❖Підтримувати конкурентоспроможність промисловості ЄС.
- ❖Забезпечити тіснішу координацію з діяльністю Європейського Агентства з Оборони (EDA) задля уникнення дублювання зусиль.
- ❖Посилити співпрацю з такими європейськими агенціями як: FRONTEX, EUROPOL, ENISA, EMSA, EU-LISA.

SU-INFRA Захист інфраструктури в Європі та людей в європейських розумних містах

- **Тип проекту: Інноваційний**
- **Рівень технологічної готовності продукту:** 7
- **Максимальна тривалість проекту:** 24 місяці
- **Бюджет одного проекту:** 7-8 млн євро
- **Виклик:** У 2020 році, зберігаючи охоплення оцінки ризиків, попередження, виявлення, реагування та пом'якшення наслідків, пропозиції мають також врахувати взаємозв'язок між різними типами критичної інфраструктури з метою розробки інструментів та методів для мінімізації каскадних ефектів та забезпечення швидкого відновлення обслуговування після інцидентів.

SU-AI 01-2020 Розробка дорожної карти досліджень у сфері штучного інтелекту на підтримку правоохоронної діяльності

- **Тип проекту:** Дії з координації та підтримки
- **Максимальна тривалість проекту:** 60 місяців
- **Бюджет одного проекту:** 1,5 млн євро
- **Виклик:** Пропозиції мають запропонувати дорожню карту ЄС з штучного інтелекту для правоохоронної діяльності, що відповідає конкретним оперативним потребам, шляхом визначення у довгостроковій перспективі: ключових ділянок, в яких штучний інтелект може бути корисним для правоохоронної діяльності, де він може містити загрозу для безпеки, вимоги кібербезпеки для технологій на основі штучного інтелекту, а також засоби уникнення використання штучного інтелекту для злочинної діяльності.

SU-AI 02-2020 Безпечні та тривкі технології, інструменти та рішення для штучного інтелекту на підтримку правоохоронної діяльності та захисту громадян, операцій з кібербезпеки, а також попередження та захисту від ворожого штучного інтелекту

- **Тип проекту:** Інноваційний
- **Максимальна тривалість проекту:** 60 місяців
- **Приблизний бюджет одного проекту:** 17 млн євро
- **Виклик:** розробка інструментів та рішень у сфері штучного інтелекту для правоохоронної діяльності у повсякденній роботі. Проекти мають охоплювати комбіновані апаратні та програмні рішення, такі як робототехніка або обробка даних природними мовами, з метою ефективнішого попередження, виявлення злочинної діяльності, тероризму, та реагування на них та прикордонний контроль.

- **Тип проекту:** Дії з координації та підтримки
- **Максимальна тривалість проекту:** 24 місяці
- **Приблизний бюджет одного проекту:** 1,5 млн євро
- **Виклик:** Пропозиції мають містити вичерпний аналіз гуманітарних, соціальних та організаційних аспектів (включно з гендерними), пов'язаних з використанням інструментів штучного інтелекту у правоохоронній діяльності, як у кібербезпеці, так і у боротьбі зі злочинністю, тероризмом. Необхідно врахувати точки зору та застереження громадян та влади. На основі цього аналізу пропозиції мають запропонувати підходи, які необхідні для подолання цих проблем, які б стимулювали прийняття інструментів штучного інтелекту громадянським суспільством та правоохоронними органами. Суспільний вимір має бути в центрі пропонованих активностей.

SU-BES Безпека кордонів та зовнішня безпека

SU-BES 01-2020 Людські фактори, соціальні, організаційні аспекти безпеки кодонів та зовнішньої безпеки

- **Тип проекту:** Дослідницький
- **Максимальна тривалість проекту:** не визначена
- **Приблизний бюджет одного проекту:** 5 млн євро
- **Виклик:** Розробка індикаторів загроз на зовнішніх кордонах ЄС на основі надійних методологій оцінки ризиків та вразливих місць. Прикордонникам ЄС доводиться мати справу з різними серйозними проблемами на зовнішніх кордонах, наприклад, управління великими потоками людей, контрабандою, використанням підроблених документів тощо. Дослідження, які б оцінили вплив різних загроз на зовнішню безпеку ЄС та запропонували модель для порівняння цих загроз, допоможуть покращити обізнаність осіб, що приймають рішення у цій сфері на рівні ЄС. Пропозиції мають бути спрямовані на підвищення ефективності прикордонного контролю, включно з повітряними, морськими кордонами та суходолом, шляхом розробки динамічних комбінованих показників загроз, щоб можна було порівняти різні загрози, що виникають одночасно і пропонувати пріоритети для їхнього пом'якшення.

SU-BES 02-2020 Технології покращення безпеки кордонів та зовнішньої безпеки

- **Тип проекту:** Дослідницький
- **Максимальна тривалість проекту:** не визначена
- **Приблизний бюджет одного проекту:** 7 млн євро
- **Виклик:** Підривні технології для неінтрузивної ідентифікації прихованих товарів. Виявлення та ідентифікація нелегальних товарів, схованих у контейнерах, залізничних вагонах та вантажних автомобілях на зовнішніх кордонах ЄС є спільною задачею прикордонних, митних та правоохоронних органів. Незаконні товари, включно з наркотиками, зброєю, вибуховими та радіоактивними речовинами, ввозяться в Європу злочинними угрупованнями з використанням різних методів та інструментів (наприклад, деякі наркотики можуть бути перетворені на рідину, яка стає твердою у місті призначення) і адаптуються до конкретних прикордонних умовах. Дослідження мають бути зосереджені на використанні технологій зондування. Наявність системи датчиків, які б дозволяли отримати детальну та зручну для використання тривимірну інформація про внутрішній склад контейнерів і тип вантажу, що перевозиться за обмежений проміжок часу.

SU-BES 03-2020 Демонстрація прикладних рішень зі зміцнення безпеки кордонів та зовнішньої безпеки

- **Тип проекту:** Інноваційний
- **Максимальна тривалість проекту:** 18 місяців
- **Приблизний бюджет одного проекту:** 5 млн євро
- **Виклик:** Вдосконалення системи спостереження за суднами, аналіз поведінки та автоматичне виявлення аномалій. Чинна система морської звітності дозволяє отримувати величезні обсяги даних, які не можуть бути безпосередньо використані операторами-людьми у різних центрах морського контролю. Очікується, що ця проблема ще поглибиться, оскільки обсяг даних зросте із запровадженням Системи обміну даних. Крім того доступні неоднорідні джерела інформації про судна, які забезпечують доступ або до відкритих, або до закритих даних, які можуть бути використані для аналізу ризиків за кожним окремим судном, що плаває в європейських водах. Традиційні системи звітності самі по собі недостатні для виявлення аномалій. Тому дослідження з цієї теми мають бути зосереджені на інноваційних рішеннях, які б поєднали всі три елементи: дані систем звітності та спостереження, відповідні інформаційні бази даних і дані в реальному часі.

SU-DRS Суспільства, стійкі до загроз

SU-DRS 01-2020 Людські фактори, соціальні та організаційні аспекти суспільств, стійких до загроз

- **Тип проекту:** Дослідницький
- **Максимальна тривалість проекту: не визначена**
- **Приблизний бюджет одного проекту:** 5 млн євро
- **Виклик:** Стійкість суспільств значною мірою залежить від того, як її громадяни поводять себе індивідуально або колективно, а також від того, як уряд та громадські організації розробляють та реалізують політику зі зниження ризиків, підготовки до лих, реагуванню на них, подоланню та аналізу уроків. Поширення нових технологій та ЗМІ призводить до різких змін у поведінці окремих осіб та спільнот, і вони у непередбачуваний спосіб впливають на суспільство. Для підвищення стійкості суспільства та громадян до стихійних лих треба краще розуміти і запровадження цих нових технологій та ЗМІ, а також їхній потенціал для підвищення обізнаності громадян, формування культури ризиків, забезпечення ефективного реагування з боку населення, покращення функціональної організації у найбільш чутливих групах.

SU-DRS 02-2020 Технології першого реагування

- **Тип проекту:** Дослідницький
- **Максимальна тривалість проекту: не визначена**
- **Приблизний бюджет одного проекту:** 7 млн євро
- **Виклик:** Методи та посібники з передгоспітального збереження життя та тріажу. Розробка інноваційних інструментів, методологій та європейських принципів догоспітального обслуговування для співробітників медичних служб, що надають першу допомогу, пожежників, поліції тощо для того, щоб забезпечити швидку та ефективну оцінку та контроль за численними постраждалими внаслідок стихійних лих і/або надзвичайних ситуацій. При цьому слід взяти до уваги досвід військової медицини. Мета полягає у забезпеченні більш ефективного тріажу з відповідним цифровим відстеженням дій і передачі даних у лікарні, в тому числі через адміністративні та політичні кордони.

SU-DRS 03-2020 Переднормативні дослідження та демонстрація для суспільств, стійких до загроз

- **Тип проекту:** Інноваційний
- **Максимальна тривалість проекту: не визначена**
- **Приблизний бюджет одного проекту:** 6 млн євро
- **Виклик:** Перша допомога у розгортанні, навчанні, технічному обслуговуванні та дистанційної координації транспортних засобів. Для ефективного використання ресурсів під час великої кризи, пов'язаної з будь-якими стихійними лихами (в тому числі, викликаними екстремальними кліматичними явищами) або антропогенними катастрофами, і безпосередньо після події, наприклад, у випадку масової евакуації з міст, необхідні удосконалені стандарти та загальні механізми обміну комунікаційними даними. Пропозиції мають бути спрямовані на ті події, щодо яких відбувається активна міжгалузева, транскордонна, міжієрархічна координаційна діяльність, і відповідно, постає проблема функціональної сумісності.

SU-DRS 04-2020 Хімічний, біологічний, радіологічний та ядерний (ХБРЯ) кластер

- **Тип проекту:** Дослідницький
- **Максимальна тривалість проекту: не визначена**
- **Приблизний бюджет одного проекту:** 3,5млн євро
- **Виклик:** Технології та інновації в області (ХБРЯ) розробляються компаніями, які часто стикаються з труднощами під час виведення їх на ринок. Можна виокремити як мінімум три причини: вони звертаються до місцевих, невеликим нішевим ринкам; ці компанії не мають ані можливостей, ані стратегічний цілей виходу на зарубіжні ринки; окремі технології,які вони розробляють можуть вийти на ринок у випадку якщо вони інтегровані з іншими інструментами інших компаній, які мають можливості та стратегії виходу на світовий ринок.

SU-DS Цифрова безпека. Кібербезпека

SU-DS 02-2020 Інтелектуальне управління безпекою та конфіденційністю

- **Тип проекту:** Дослідницький, Інноваційний
- **Максимальна тривалість проекту: не визначена**
- **Приблизний бюджет одного проекту:** 2-5 (для інноваційного), 3-6 (для дослідницького) млн євро
- **Виклик:** З метою зниження ризиків для безпеки системи ІКТ мають інтегрувати сучасні підходи до управління безпекою та конфіденційністю у цілісний і динамічний спосіб. Організації мають постійно прогнозувати, контролювати та оновлювати данні про безпеку своїх ІК систем, спираючись на штучний інтелект та автоматизацію, знижуючи ризик необхідного людського втручання. Загрози безпеки для складних інфраструктур ІКТ, які представляють собою багаторівневі та взаємопов'язані архітектури, можуть мати каскадний ефект. Для протидії таким загрозам організації мають співробітничати і безперешкодно обмінюватися інформацією, пов'язаною з управлінням безпекою та конфіденційністю. Поширеність Інтернету речей та штучного інтелекту розширює простір для атак та підвищує ризик їхнього поширення. Для цього необхідні інструменти автоматичного моніторингу та зниження ризиків для безпеки. .

SU-DS 03-2020 Цифрова безпека та конфіденційність для громадян, а також малих та середніх підприємств і мікропідприємств

- **Тип проекту:** Інноваційний
- **Максимальна тривалість проекту:** не визначена
- **Приблизний бюджет одного проекту:** 3-4 млн євро
- **Виклик:** Деякі члени цифрового суспільства в ЄС більш вразливі, оскільки вони меншою мірою протистоять кібератакам. Масштаби, цінність та чутливість особистих даних в кіберпросторі зростають і громадяни, як правило, не впевнені в тому, хто контролює, управляє їхніми особистими даними. З метою захисту свободи, безпеки та конфіденційності, також забезпечення захисту персональних даних громадян Європи, громадяни повинні мати можливість оцінити ризики, пов'язані з їхньою цифровою діяльністю і налаштувати власні параметри безпеки, а також механізми контролю. Крім того, необхідно підвищити здатність громадян модулювати рівень і точність інструментів моніторингу (наприклад, за допомогою файлів cookie). Більшість МСП не мають достатньої обізнаності та мають обмежені ресурси – як технічні, так і людські, - для протидії кіберугрозам, тому вони є легшою мішенню (наприклад, для атаки з метою викупу), ніж великі організації.

SU-DS 04-2020 Кибербезпека в електроенергетичній системі (EPES): броня проти кібератак, атак на конфіденційність, а також витоку данних

- **Тип проекту:** Інноваційний
- **Максимальна тривалість проекту:** не визначена
- **Приблизний бюджет одного проекту:** 6-8 млн євро
- **Виклик:** Електроенергетична система (EPES) має ключове значення для економіки, оскільки всі інші галузі залежать від електрики, тому відключення електрики може напряму впливати на доступність таких послуг як транспорт, фінанси, водопостачання, телефонний зв'язок, коли резервне електропостачання недоступно або час відновлення електропостачання виходить за рамки автономії резервного енергопостачання. З переходом до децентралізованої енергетичної системи цифрові технології відіграють важливішу роль в EPES: вони сприяють зниженню енергоспоживання, дозволяють інтегрувати відновлювані джерела енергії і сприяють створенню більш енергоефективнішої системи. В той же час, зі зростанням використання цифрових засобів зв'язку та систем, на EPES все більше впливають зовнішні загрози, такі як віруси, хакери, порушення конфіденційності даних тощо.

SU-GM Загальні питання

SU-GM 01-2020 Панєвропейська мережа практиків та інших акторів у сфері безпеки

- **Тип проекту:** Дії з координації та підтримки
- **Максимальна тривалість проекту:** 60 місяців
- **Приблизний бюджет одного проекту:** 1,5-3,5 млн євро
- **Виклик:** У 2020 р. пропонуються 2 опції: 1) служби безпеки і розвідки. Стійка терористична загроза стає складнішою і різноманітнішою. Нові технології не тільки посилюють цю загрозу, але і відкривають нові можливості . Служби безпеки та розвідки держав-членів ЄС та партнерів відіграють важливу роль у забезпеченні безпеки європейських громадян. Європейська технологічна автономія особлива важлива у сфері розвідки; спецслужби можуть мати потребу у дослідженнях, що відрізняються від потреб правоохоронних служб; 2) боротьба з кіберзлочинністю. Була запроваджена низка ініціатив для виявлення пробілів і потреб правоохоронних органів у сфері боротьби з кіберзлочинністю, розроблені "дорожні карти". Але у сфері кіберзлочинності сценарії розвитку технологій розвиваються такими темпами, що ця робота потребую постійного оновлення. Досі відсутня точна картина конкретних можливостей органів держав-членів. Крім того, оскільки кіберзлочинність і злочини, що скоюються в онлайн-режимі, відбуваються без кордонів, необхідно виявляти спільні виклики і рішення, щоб максимально ефективно використовувати ресурси.

SU-GM 02-2020 Стратегічні передкомерційні закупівлі інноваційних, передових систем для забезпечення безпеки

- **Тип проекту:** Передкомерційні закупівлі
- **Максимальна тривалість проекту:** не визначена
- **Приблизний бюджет одного проекту:** 2-12 млн євро
- **Виклик:** Інноваційні рішення необхідні у тих випадках, коли для тіснішого співробітництва потрібні ресурси з різних країн. Такі рішення сприяють розвитку Союзу безпеки ЄС. Спеціалістам-практикам із декількох країн пропонується працювати над загальними вимогами будь якої системи, яка може знадобитися їм в майбутньому для зміцнення безпеки кордонів та зовнішньої безпеки, боротьби зі злочинністю та тероризмом, захисту інфраструктури або підвищення життєздатності суспільства, а також для заохочення відповідальних закупівельних органів до майбутніх закупівель.

SU-FCT Боротьба зі злочинністю та тероризмом

SU-FCT 01-2020 Людські фактори, соціальні, суспільні, організаційні аспекти вирішення проблем у боротьбі зі злочинністю та тероризмом

- **Тип проекту:** Дослідницький
- **Максимальна тривалість проекту:** не визначена
- **Приблизний бюджет одного проекту:** 5 млн євро
- **Виклик:** Розробка науково обґрунтованих підходів до оцінки та подальшого розвитку ініціатив з попередження насильницької радикалізації та боротьби з нею. Особливий інтерес становлять наступні аспекти: фактори та шляхи радикалізації; фактори, що впливають на стійкість до радикалізації з акцентом на групи, що потребують особливої уваги (наприклад, діти); зв'язок між насильницьким екстремізмом та іншими формами злочинності; насильницький екстремізм в мережі; соціальні мережі та терористична пропаганда; оцінка та вплив контрпропаганди та альтернативних наративів; робота з екстремістами після їхнього повернення з в'язниці (із залученням пенітенціарних служб та правоохоронних органів); гендерні та соціоекономічні аспекти радикалізації; оцінка національних і місцевих превентивних стратегій. Пропозиції не обов'язково мусять охоплювати всі аспекти, достатньо обрати один або декілька.

SU-FCT 02-2020 Технології для посилення боротьби зі злочинністю та тероризмом

- **Тип проекту:** Дослідницький
- **Максимальна тривалість проекту:** не визначена
- **Приблизний бюджет одного проекту:** 7 млн євро
- **Виклик:** Розробка та запровадження технологій, інструментів та відповідної інфраструктури з метою оперативного виявлення в онлайн-режимі терористичного контенту та попередження його повторному завантаженню. Для боротьби з терористичним контентом в Інтернеті ЄК прийняла 12 вересня 2018 р. регламент, згідно з яким всі держави-члени мають вжити низку заходів. Зокрема, постачальники послуг хостінгу (що охоплює соціальні мережі, хмарні служби, обмін файлами тощо), мають вжити низку заходів: наприклад, строк в одну годину для видалення або відключення терористичного контенту після отримання розпорядження від правоохоронних органів (враховуючи, що терористичний контент є небезпечним в перші години його появи в мережі), а також превентивні засоби, включно з автоматичним виявленням з метою швидкого та ефективного видалення терористичного контенту.

SU-FCT 03-2020 Управління потоками інформації та даних з метою боротьби з кіберзлочинністю та тероризмом

- **Тип проекту:** Інноваційний
- **Максимальна тривалість проекту:** 24 місяці
- **Приблизний бюджет одного проекту:** 7 млн євро
- **Виклик:** Обсяг даних, що генерується та збирається у рамках розслідувань кіберзлочинів, збільшується у геометричній прогресії, створюючи тим значні проблеми для правоохоронних органів. Ефективність правоохоронної діяльності напряму залежить від здатності підвищувати якість даних та перетворювати великі та неоднорідні масиви даних (зображення, відео, геопросторова розвідка, дані про трафік тощо)в оперативні дані. Ці можливості можуть бути значно розширені за рахунок специфічних інструментів, застосунків для аналізу великих масивів даних, розроблених для потреб слідчих.

SU-FCT 04-2020 Хімічні речовини: розвідка, виявлення, криміналістика

- **Тип проекту:** Інноваційний
- **Максимальна тривалість проекту:** 36 місяців
- **Приблизний бюджет одного проекту:** 5 млн євро
- **Виклик:** Злочинці, в тому числі терористи, постійно шукають нові шляхи розробки та активації небезпечних хімічних речовин (вибухових речовин, нейротоксинів, нових наркотиків тощо). Способи виробництва та комбінування таких хімічних речовин постійно розвиваються, що ускладнює роботу спеціалізованих правоохоронних органів та референтних лабораторій. Дослідження мають попереджувати таку проблему шляхом розширення знань про ці загрози, розробляти технології протидії інцидентів та реагування на них, розширення знань про небезпечні хімічні речовини.

Корисні посилання з тематики "Безпека"

- **1) Action plan protection of public spaces**

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_action_plan_to_improve_the_protection_of_public_spaces_en.pdf

2) Seventeenth Progress Report towards an effective and genuine Security Union

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20181211_com-2018-845-security-union-update-17_en.pdf

3) European Agenda on Security

https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en

Дякуємо за увагу

Україна, 04070, м. Київ, вул. Сковороди, 2
www.h2020.ukma.edu.ua