ПРОЕКТ

Концепт білої книги про результати кампанії дезінформації COVID-19 у Росії та Китаї, як частина Стратегії інформаційної безпеки України

Резюме/Короткий зміст (Executive Summary)

Політика по спротиву російській дезінформації відсутня на державному рівні в Україні, хоча Міністерство інформаційної політики формально існує проте немає затвердженої стратегії щодо протидії дезінформації з боку іноземних держав і РФ зокрема. Відповідно і дезінформація з боку РФ і Китаю не була виявлена і ідентифікована державними органами Україні, відповідно і відсутні були дії щодо її нейтралізації. Оскільки, проблема дезінформації з боку іноземних держав в українському інформаційному просторі існує (а це і системна дезінформація з метою дестабілізації з боку РФ і її сателітів, таких як Угорщина, на глобальному рівні Китай) необхідно розробити і впроваджувати відповідні політики по захисту інформаційного простору України та належній просвіті українських громадян. Оскільки інформаційна агресія є однією з головних складових гібридних війн сучасного світу і Україна має мати належний захист своїх інтересів у даній сфері. Саме через інформаційний аспект гібридної агресії здійснюється дестабілізація в середині країни через її громадян, створюється ситуація хаосу, яка виникає через недовіру громадян до владних інституцій власної держави. Для отримання ефективних результатів по захисту інформаційного поля України, необхідно розробити стратегію інформаційного захисту та протидії дезінформації, прийняти низку нормативно-правових документів, внести необхідні статті в бюджет, організувати і забезпечити конкретний підрозділ у міністерстві інформаційної політики, призначити відповідальних у обласних державних адміністраціях за виконання рішень щодо протидії дезінформації.

Передумови: Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» (Введено в дію Указом Президента України від 14 вересня 2020 року № 392/2020) https://www.president.gov.ua/documents/3922020-35037

Проект Стратегія інформаційної безпеки України.

Стратегія має на меті створити передумови і задати рамку розвитку нормативно-правової бази для інформаційної безпеки України.

У даній Стратегії під інформаційною сферою розуміється сукупність інформації, об'єктів інформатизації, інформаційних систем, мережі Інтернет, мереж зв'язку, інформаційних технологій, суб'єктів, діяльність яких пов'язана з формуванням і обробкою інформації, розвитком і використанням названих технологій, забезпеченням інформаційної безпеки, а також сукупність механізмів регулювання відповідних суспільних відносин.

У цій Стратегії вживаються в такому значенні:

- національні інтереси України в інформаційній сфері (далі - національні інтереси в інформаційній сфері) - об'єктивно значущі потреби особистості, суспільства і держави в забезпеченні їх захищеності та сталого розвитку в частині, що стосується інформаційної сфери;

- загроза інформаційній безпеці України (далі - інформаційна загроза) - сукупність дій і чинників, що створюють небезпеку заподіяння шкоди національним інтересам в інформаційній сфері;
- інформаційна безпека України (далі - інформаційна безпека) - стан захищеності особистості, суспільства і держави від внутрішніх і зовнішніх інформаційних загроз, при якому забезпечуються реалізація конституційних прав і свобод людини і громадянина, гідні якість і рівень життя громадян, суверенітет, територіальна цілісність і сталий соціально-економічний розвиток України, оборона і безпека держави;
- забезпечення інформаційної безпеки - здійснення взаємопов'язаних правових, організаційних, оперативно-розшукових, розвідувальних, контррозвідувальних, науково-технічних, інформаційно-аналітичних, кадрових, економічних та інших заходів з прогнозування, виявлення, стримування, запобіганню, відбиття інформаційних загроз і ліквідації наслідків їх прояви;
- сили забезпечення інформаційної безпеки - державні органи, а також підрозділи і посадові особи державних органів, органів місцевого самоврядування та організацій, уповноважені на рішення відповідно до законодавства України завдань щодо забезпечення інформаційної безпеки;
- засоби забезпечення інформаційної безпеки - правові, організаційні, технічні та інші засоби, що використовуються силами забезпечення інформаційної безпеки;
- система забезпечення інформаційної безпеки - сукупність сил забезпечення інформаційної безпеки, які здійснюють скоординовану і спланована діяльність, і використовуваних ними засобів забезпечення інформаційної безпеки;
- інформаційна інфраструктура України (далі - інформаційна інфраструктура) - сукупність об'єктів інформатизації, інформаційних систем, мережа Інтернет і мереж зв'язку в межах України.

Національними інтересами в інформаційній сфері є:

- забезпечення і захист конституційних прав і свобод людини і громадянина в частині, що стосується отримання і використання інформації, недоторканності приватного життя при використанні інформаційних технологій, забезпечення інформаційної підтримки демократичних інститутів, механізмів взаємодії держави і громадянського суспільства, а також застосування інформаційних технологій в інтересах збереження культурних, історичних і духовно-моральних цінностей, національних цінностей;
- забезпечення сталого та безперебійного функціонування інформаційної інфраструктури, в першу чергу критичної інформаційної інфраструктури і мереж електрозв'язку, в мирний час, в період безпосередньої загрози агресії і у воєнний час;
- розвиток галузі інформаційних технологій і електронної промисловості, а також вдосконалення діяльності виробничих, наукових і науково-технічних організацій по розробці, виробництву і експлуатації засобів забезпечення інформаційної безпеки, надання послуг в галузі забезпечення інформаційної безпеки;
- доведення до громадськості достовірної інформації, запобігання фейкам;
- сприяння формуванню системи міжнародної інформаційної безпеки, спрямованої на протидію загрозам використання інформаційних технологій з метою порушення стратегічної стабільності, на зміцнення рівноправного стратегічного партнерства в області інформаційної безпеки, захист суверенітету України в інформаційному просторі.

Основні інформаційні загрози

Транскордонний обіг інформації використовуються в якості гібридних методів для досягнення геополітичних, терористичних, екстремістських, кримінальних та інших протиправних цілей на шкоду безпеці і стратегічній стабільності в Україні і світі.

Виклики:

- Спеціальні служби іноземних держав, насамперед Російської Федерації, продовжують розвідувально-підривну діяльність проти України, намагаються підживлювати сепаратистські настрої, використовують організовані злочинні угруповання і корумпованих посадових осіб, прагнуть зміцнити інфраструктуру впливу.
- Деструктивна пропаганда як ззовні, так і всередині України, використовуючи суспільні протиріччя, розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність. Відсутність цілісної інформаційної політики держави, слабкість системи стратегічних комунікацій ускладнюють нейтралізацію цієї загрози.
- інформаційно-технічного впливу на інформаційну інфраструктуру в військових цілях.
- Кібер-розвідки щодо українських державних органів, наукових організацій і підприємств оборонно-промислового комплексу,
- фоні розгортання пандемії COVID-19: збільшення кількості людей, які працюють віддалено (використовуючи ІТ, але не маючи належних знань та досвіду); збільшення електронних платежів (що збільшує увагу шахраїв); збільшення кількості випадків фішингових атак; потенційна можливість для інформаційних та кібератак з метою дестабілізації ситуації,
- інформаційно-психологічний вплив, спрямованого на дестабілізацію внутрішньополітичної та соціальної ситуації і приводить до підриву суверенітету і порушення територіальної цілісності України зокрема. Ця діяльність здійснюється через релігійні, націоналістичні, спортивні, етнічні, правозахисні та інші справжні і організації-клони організації, активно використовуються інформаційні технологій.

Стратегічні цілі і основні напрямки забезпечення інформаційної безпеки

Стратегічною метою забезпечення інформаційної безпеки в області оборони країни є захист інтересів особистості, суспільства і держави від внутрішніх і зовнішніх загроз, пов'язаних із застосуванням інформаційних технологій у військово-політичних цілях, спрямованих на підрив суверенітету, порушення територіальної цілісності держави, що суперечать Конституції України та міжнародному праву.

Державний суверенітет, територіальна цілісність, демократичний конституційний лад та інші життєво важливі національні інтереси мають бути захищені також від невоєнних загроз з боку Російської Федерації та інших держав, зокрема спроб спровокувати внутрішні конфлікти. Пріоритетними завданнями правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їх компетенції є:

- активна та ефективна протидія розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді;
- запобігання, виявлення та припинення проявів сепаратизму, тероризму, екстремізму, припинення діяльності незаконних збройних формувань, політично мотивованого насильства та інших зазіхань на конституційний лад;
- отримання повної і достовірної упереджувальної інформації про ситуацію в Україні та світі, протидія зовнішнім загрозам національній безпеці України, сприяння реалізації національних інтересів України;
- системна освіта цільових груп: державних службовців, працівників силових структур, працівників ЗМІ, вчителів, журналістів, викладачів, військових щодо розпізнавання пропаганди, основам критичного мислення і розпізнаванню фейків,
- впорядкування українського законодавства що регулює діяльність масової інформацію з на предмет, ліквідації можливості мовлення пропагандиським ЗМІ афілійованим з іншими країнами на території України.

Організаційне забезпечення інформаційної безпеки

Система забезпечення інформаційної безпеки є частиною системи забезпечення національної безпеки України. Забезпечення інформаційної безпеки здійснюється на основі поєднання законодавчої,

правозастосовної, правоохоронної, судової, контрольної та інших форм діяльності державних органів у взаємодії з органами місцевого самоврядування, організаціями та громадянами.

Організаційну основу системи забезпечення інформаційної безпеки складають: Президент, ВРУ, РНБО, МОУ, МВС, МІБ, МЦТУ, МОНУ, МФУ, МЮУ, органи місцевого самоврядування, органи судової влади, які беруть в відповідно до законодавства України участь у вирішенні завдань щодо забезпечення інформаційної безпеки.

Учасниками системи забезпечення інформаційної безпеки є: власники об'єктів критичної інформаційної інфраструктури і організації, які експлуатують такі об'єкти, засоби масової інформації і масових комунікацій, організації грошово-кредитної, валютної, банківської та інших сфер фінансового ринку, оператори зв'язку, оператори інформаційних систем, організації, що здійснюють діяльність по створенню і експлуатації інформаційних систем і мереж зв'язку, по розробці, виробництву і експлуатації засобів забезпечення інформаційної безпеки, з надання послуг у сфері забезпечення інформаційної безпеки, організації, що здійснюють освітню діяльність в цій галузі, громадські об'єднання, інші організації та громадяни, які в відповідно до законодавства України беруть участь у вирішенні завдань щодо забезпечення інформаційної безпеки.

Діяльність державних органів по забезпеченню інформаційної безпеки грунтується на наступних принципах:

а) законність суспільних відносин в інформаційній сфері і правова рівність всіх учасників таких відносин, що ґрунтуються на конституційному праві громадян вільно збирати, зберігати, використовувати і поширювати інформацію будь-яким законним способом;

б) конструктивну взаємодію державних органів, організацій і громадян при вирішенні завдань щодо забезпечення інформаційної безпеки;

в) дотримання балансу між потребою громадян у вільному обміні інформацією і обмеженнями, пов'язаними з необхідністю забезпечення національної безпеки, в тому числі в інформаційній сфері;

г) достатність сил і засобів забезпечення інформаційної безпеки, яка визначається в тому числі за допомогою постійного здійснення моніторингу інформаційних загроз;

д) дотримання загальновизнаних принципів і норм міжнародного права, міжнародних договорів.

Завданнями державних органів в рамках діяльності щодо забезпечення інформаційної безпеки є:

а) забезпечення захисту прав і законних інтересів громадян і організацій в інформаційній сфері;

б) оцінка стану інформаційної безпеки, прогнозування і виявлення інформаційних загроз, визначення пріоритетних напрямків їх запобігання і ліквідації наслідків їх прояву;

в) планування, здійснення і оцінка ефективності комплексу заходів щодо забезпечення інформаційної безпеки;

г) організація діяльності та координація взаємодії сил забезпечення інформаційної безпеки, вдосконалення їх правового, організаційного, оперативно-розшукової, розвідувальної, контррозвідувальної, науково-технічного, інформаційно-аналітичного, кадрового та економічного забезпечення;

д) вироблення і реалізація заходів державної підтримки організацій, що здійснюють діяльність з розробки, виробництва і експлуатації засобів забезпечення інформаційної безпеки, з надання послуг у сфері забезпечення інформаційної безпеки, а також організацій, що здійснюють освітню діяльність в цій галузі.

Завданнями державних органів в рамках діяльності щодо забезпечення інформаційної безпеки є:

а) забезпечення захисту прав і законних інтересів громадян і організацій в інформаційній сфері;

б) оцінка стану інформаційної безпеки, прогнозування і виявлення інформаційних загроз, визначення пріоритетних напрямків їх запобігання і ліквідації наслідків їх прояву;

в) планування, здійснення і оцінка ефективності комплексу заходів щодо забезпечення інформаційної безпеки;

г) організація діяльності та координація взаємодії сил забезпечення інформаційної безпеки, вдосконалення їх правового, організаційного, оперативно-розшукової, розвідувальної, контррозвідувальної, науково-технічного, інформаційно-аналітичного, кадрового та економічного забезпечення;

д) вироблення і реалізація заходів державної підтримки організацій, що здійснюють діяльність з розробки, виробництва і експлуатації засобів забезпечення інформаційної безпеки, з надання послуг у сфері забезпечення інформаційної безпеки, а також організацій, що здійснюють освітню діяльність в цій галузі.

Завданнями державних органів в рамках діяльності щодо розвитку та вдосконалення системи забезпечення інформаційної безпеки є:

а) зміцнення вертикалі управління і централізація сил забезпечення інформаційної безпеки на міжрегіональному, регіональному, муніципальному рівнях, а також на рівні об'єктів інформатизації, операторів інформаційних систем і мереж зв'язку;

б) вдосконалення форм і методів взаємодії сил забезпечення інформаційної безпеки з метою підвищення їх готовності до протидії інформаційним загрозам, в тому числі шляхом регулярного проведення тренувань (навчань);

в) вдосконалення інформаційно-аналітичних та науково-технічних аспектів функціонування системи забезпечення інформаційної безпеки;

г) підвищення ефективності взаємодії державних органів, органів місцевого самоврядування, організацій і громадян при вирішенні завдань щодо забезпечення інформаційної безпеки.

Контроль над реалізацією Стратегії покласти на РНБО, виконання на МІПУ.