

С Т А Н О В И Щ Е

относно дисертационен труд за присъждане на образователната и научна степен „доктор” по научна специалност „Международно право и международни отношения”

Автор на дисертационния труд: Йосиф Йорданов Кочев

Тема на дисертационния труд: **„Политиката на Европейския съюз по проблемите на киберсигурността”**

Научен ръководител: Проф. д-р Стойко Стойков

Изготвил становището: проф. д-р Владко Мичов Иванов -
ръководител катедра „Опазване на обществения ред“
в Академията на МВР – гр. София,

I. Актуалност, значимост и съдържание на дисертационния труд

Дисертационният труд е преминал процедурите и е представен от катедра „Международно право и международни отношения”, Правно-исторически факултет към ЮЗУ „Неофит Рилски” – Благоевград. Изискващите се материали са на разположение на интернет страницата на университета.

Кандидатът Йосиф Йорданов Кочев получава магистърска степен през 2012 г., специалност “Международни отношения”. Понастоящем е асистент в катедрата, която го представя. Учебните дисциплини, които води, участието в проекти и технически дейности на университета благоприятстват анализите по темата.

Актуалността на дисертационния труд е свързана с радикалните промени в разбирането за сигурност в информационната епоха. Разработката съдържа увод, три глави, заключение, библиография, приложения и списък със съкращенията с общ обем от 224 страници. Използваните и цитирани източници са на български, английски и руски език и са солидна основа за разгръщане на изследването.

Уводът предпоставя ясна и целенасочена композиция. Политиката на Европейския съюз по проблемите на киберсигурността постоянно е във фокуса на изследването в съответствие с целите. Трудът достига до множество изводи още в хода на анализите.

Съдържанието е разпределено хармонично в три основни части.

Глава първа е правно-теоретична основа на изследването. Успешно са намерени, изведени и обяснени основните понятия и термини в политиката на Европейския съюз по проблемите на киберсигурността. Интердисциплинарният подход на автора представя и обобщава заплахите и проблемите на държавите от ЕС, юридическите лица, предоставящи комуникационни услуги и интернет, неправителствения сектор и гражданите. Аргументирано е показано изоставането на регулациите от темпа на информационните и комуникационните технологии. Надделява разбирането, че революционното развитие на кибернетичните, асиметричните и хибридните заплахи обезсмислят днешните стратегии за сигурност и зададените правни рамки. В отговор авторът предлага по-гъвкави определения, характеристики и концепция за контрол на интернет технологиите и предизвикателствата пред индивидуалната и колективна киберсигурност, обществения ред, икономическия просперитет и политическата свобода. Авторът залага на много критерии, класификации и изводи за киберсигурността.

В Глава втора кандидатът синтезира резултатите от изследването в полето на институциите, правните актове и механизмите за киберсигурност в Европейския съюз. Подборът на материята, онагледяването с фигури и схеми, и личното мнение очертават визията на ЕС в тази сфера. Авторът показва, че е образован и се чувства сигурно в научна специалност „Международно право и международни отношения”.

В Глава трета е използван сравнително-правният подход, за да се демонстрират системите, постиженията и застъпването на визиите за киберсигурност на ООН, НАТО и ЕС. Много добре са съпоставени реактивният и проактивният подход към заплахите от кибертероризма до сигурността на личните данни. Видян е проблемът за доминацията на системите на НАТО над ЕС. Логично са достигнати проблемите на малката държава и е направено предложение за модел на стратегия за киберсигурност на Република България. В предложения модел са посочени заплахите за сигурността и принципите, по които следва да бъде изграден националният подход за управление на кибернетичното пространство.

Дисертацията е предшествана от три самостоятелни статии на български и английски език в авторитетни сборници с научна редакция. На базата на горното приемам дисертационния труд за завършено, осмислено, самостоятелно съчинение с открояваща се образователна част и перспективна научна насока.

II. Оценка на резултатите и приносите в дисертационния труд

Считам, че авторът като цяло успешно е очертал правното, теоретичното и приложното поле на заплахите, идващи от информационната основа на днешния живот в международен, европейски, национален, фирмен и личностен план. Обобщавам приносите в дисертационния труд в няколко основни нива.

На лице е ясна визия и допълнение в системния анализ относно проблема за глобалната киберсигурност и фокусиране на познанието върху ЕС. Обобщени са основните фактори за оптимизация – обединяване на субектите (общностни, национални, частни, лични) заинтересовани от

киберсигурност, съсредоточаване на финансовите ресурси и подготовка на човешкия фактор.

Селектирана и ефективно е анализирана огромната материя за информационна сигурност. Изследването и приложените документи на Европейския съюз и ООН, свързани с киберсигурността са научен продукт, източник на знания и качествено приложно обучение.

Разкрита е системата и политиката на Европейския съюз за киберсигурност от интердисциплинарна гледна точка. Познаването и систематизирането на актовете от ПЕС, дейността на институциите, правните киберрискове и управлението на киберсигурността са в обхвата на научната специалност „Международно право и международни отношения” за която претендира авторът.

Дисертационният труд ясно установява проблема на ЕС в сферата на киберсигурността. Като цяло съюзът следва международноправните условия, но липсват мащабни обединителни актове в Правото на ЕС, които установяват единни стандарти особено в сферата на отбраната, разузнаването, дипломацията. Авторът вижда инертност в защитата на хардуера и софтуера. Малките държави и техните национални правни системи трудно противодействат на предизвикателствата.

Изследването се базира на обобщени визии, определения и класификации на заплахите. Направен е сравнителен анализ на национални стратегии за киберсигурност в редица държави.

Общностното противодействие на киберпрестъпността компетентно е разгледано в обединителния пръстен на CEPOL, Европол, Frontex и Евроюст, както и други международни организации като Интерпол и НАТО.

Анализът откроява и посочва причините за изоставането на държавите от източната периферия на ЕС и нарастващите предизвикателства свързани с киберсигурността – технологично

изоставане, липса на ресурси, забавена координация и сигурни сигнали от Брюксел. Предлагат се множество семпли, но ефективни мерки за защита на киберпространството в ЕС – нова система от правни инструменти, нова мрежа за обмен на информация по съдебни въпроси и добри практики при разследване и наказателно преследване на престъпления в кибернетичното пространство, единни стандарти за подготовка на специалисти.

Обобщенията убедително сочат, че политиките за киберпространството са реактивни и бавни. На този фон България няма приета стратегия по дискутираните проблеми, което само по себе си е риск. Авторът предлага консолидиране на достиженията в ЕС и модел на стратегия за киберсигурност на Република България с органи, функционални дефиниции и задачи.

В заключение, дисертационният труд е изчерпателно и завършено изследване с правен и организационен ефект. То дава обобщаващо системно познание с насочващ приложен потенциал в сферата на киберсигурността в ЕС. Ценното е, че авторът образова, предлага решения и създава предимства за по-смели и обосновани стратегии.

III. Критични бележки и препоръки към докторанта

Считам, че в бъдещите си трудове кандидатът трябва да развие познанието за киберсигурността като арена на безкомпромисно съревнование между държавите и съюзите, където субектите, силата и печалбите заобикаля правилата. За сега институциите на ЕС разглеждат иновативните страни на глобалната мрежа предимно като възможност за глобализиране на престъпната дейност. Подценява се политическата конфронтация, шпионажът, подривната дейност и финансовата манипулация. Новият подход в ПЕС трябва да изправи не машината, а човека в центъра на проблема. Подценяването на субекта доведе до Wikileaks, Едуард Сноудън, разкритията за АНС и пр.

Феноменът на социалните мрежи и глобализацията на медиите също бяха подценени от правната регулация като фактор в киберпространството. Това направи възможни скоротечните социални катаклизми, ескалира миграцията и хибридната война – все нови кибернетични заплахи за малките държави от периферията на ЕС.

IV. Заключение и окончателно становище по дисертационния труд

Предлагам препоръките си като част от научната дискусия и възможност за бъдещо израстване на автора. Като цяло той се е справил с анализа, вярно и иновативно е представил проблема за киберсигурността на ЕС. Категорично потвърждавам, че кандидатът убедително демонстрира образователна и научна кондиция в дисертационния труд. Той има качествата на самостоятелна гносеологическа система и визия за киберсигурността, плод на неоспоримо лично интелектуално дело.

Горното ми дава пълно основание да демонстрирам положително становище и да предложа на научното жури да присъди на автора на представения дисертационен труд Йосиф Йорданов Кочев образователната и научна степен „доктор“ по научната специалност „Международно право и международни отношения“.

06.07.2015 г.

София

Изготвил становището:

(проф. д-р Владко Иванов)