СОФИЙСКИ УНИВЕРСИТЕТ
„СВ. КЛИМЕНТ ОХРИДСКИ“

ФИЛОСОФСКИ ФАКУЛТЕТ
КАТЕДРА „ПУБЛИЧНА АДМИНИСТРАЦИЯ“

АВТОРЕФЕРАТ

НОВИ АСПЕКТИ НА ПОЛИТИКИТЕ ЗА НАЦИОНАЛНА СИГУРНОСТ В КОНТЕКСТА НА ЕКСПАНЗИЯ НА ТЕХНОЛОГИИТЕ И КИБЕРПРОСТРАНСТВОТО

Автореферат на дисертационен труд

за присъждане на образователна и научна степен

„Доктор“ по професионално направление 3.3

Политически науки (Публична администрация)

Изготвил:
Ангел Ковачев
Докторант на самостоятелна подготовка

София, юни 2021 г.

Съдържание

I. Обща характеристика на дисертационния труд

С развитието на технологиите и проникването на глобалната информационна мрежа във всички аспекти на живота ни светът постепенно се придвижва към едно ново състояние на перманентна свързаност, което изцяло променя не само начините, по които комуникираме, но и фундаментално предефинира редица обществено-икономически взаимоотношения. Този процес драматично рефлектира върху социалните връзки, създавайки обективни предпоставки за актуализиране на базови понятия, върху които съществуваше трайно обществено съгласие и бяха възприети като константни през годините.

Пример за такава фундаментална промяна е налице и в сектор „Сигурност“, където постепенно еволюира самата парадигма за това понятие, поставяйки редица въпроси пред ангажираните с изготвяне на политиките по опазването й, като например: Какво представлява днес и какво точно предполага понятието „сигурност“ в различните си измерения - за съвременния човек от една страна, за бизнес организациите от друга и за модерната държава от трета? Как да се изгради ефективна система за сигурност в един глобално обвързан, динамичен и взаимозависим свят? Какви структури са нужни и как следва да бъдат разпределени различните отговорности по опазването й ? Всички тези въпроси предполагат нееднозначни отговори, които следва да бъдат търсени чрез широк обмен на нови гледни точки и ангажимент за извличане на обратна връзка от реалния живот, чрез събиране на доказателствата за това какъв подход или кои мерки работят и какво вече не е актуално като тенденция или решение.

Актуалност на темата

Все по-често ставаме свидетели на случаи, които илюстрират растяща неадекватност на мерките и инструментите за прилагането им от политиките по информационна и кибер сигурност. Примерите от последните години с изтичането на данни от НАП на милиони български компании и физически лица са само върха на един огромен айсберг, който има потенциал да причини мащабни негативни последици не само от икономически характер, но и в чисто физически план за гражданите в страната ни. Разбира се тези заплахи отдавна са известни, при това не само на експертната общност, но и за широката общественост, но изглежда политиките и мерките за превенцията им сякаш изостават драстично от скоростта на развитието на процесите и съответно предизвикателствата на киберпространството.

В опит да обхване рамките на този относително нов за света проблем през вече далечната 2012 г ОИСР провежда сравнителен анализ на стратегиите за киберсигурност от нов тип на множество държави, резултатите от който показват, че процесът на създаване на политики в сектора се намира в повратна точка. Като основни причини за това са посочени няколко нови ключови аспекта, настъпили в следствие на постоянно ускоряващата се технологична и информационна динамика. На първо място е идентифицирана нарастващата зависимост на процесите в почти всички аспекти на живота от информационната обезпеченост и интернет свързаност, а на второ - като закономерно следствие от развитието на този процес, постоянното нарастване на количеството генерирани данни и респективно увеличаващото се количество информация, което се обменя в мрежата. Особено внимание тук е обърнато на проблема с използването на личните данни, чиято умишлена злоупотреба може да окаже съвсем реално измерение във физически план и да се превърнат в основен проблем за националната сигурност.

Съвсем естествено на този фон съображенията за суверенитет в киберпространството се превръщат във все по важни - както за отделния индивид, така и за различните бизнес организации и правителствени национални структури. Поради тази причина днес вече за много държави киберсигурността е приоритизирана и подкрепена не просто ресурсно, а и чрез силно лидерство, като всички нови стратегии за действия в различни сфери постепенно се интегрират с нея и усложняват чрез взаимодействието си. Актуалната тенденция в подхода към киберсигурността като фундаментален компонент на националната сигурност е холистичен, като стремежът е да бъдат обхванати множество аспекти - икономически, социални, образователни, правни, технически, дипломатически, военни и разузнавателни. Това е основната причина да се търсят нови възможности за изработка на по-ефективни мерки и политики за гарантиране на сигурността в киберпространството както на индивидуално, така и на национално, а и на международно ниво. В допълнение към това нарастващият темп на глобализация на процесите в социума рязко повишава изискванията към политиките за национална сигурност и по специално тези аспекти от нея, които имат за цел да управляват областта информационна и киберсигурност. Освен че е нужно да бъдат радикално модифицирани, за да са адекватни на новата реалност и нововъзникналите предизвикателства, е необходимо те да бъдат постоянно осъвременявани с оглед динамичните промени в информационните общества.

Източници по темата на дисертационния труд

В процеса на създаването на настоящата разработка са използвани два типа основни източници:

А) публикации в различни видове научни и научно-популярни списания, доклади, статии и ревюта, имащи отношение към различните аспекти на изследваната проблематика - технологии, киберсигурност, защита на лични данни, политики за НС.

Б) публикации в интернет сайтове, он-лайн страници на различни издания на периодичния печат и някои от популярните социални медии.

За набиране на емпирични информация са проведени :

А) интервюта с ключови участници във формирането на политиките по киберсигурност в областта на личните данни и националната сигурност.

Б) дискусии във фокус групи, с представители на различни сфери на бизнеса, държавната администрация и академичната общност. Тук основна цел е да се дефинира от една страна същността на проблема с личните данни за участниците, а от друга – да се представи тяхното разбиране за важността на опазването на неприкосновеността им и да се идентифицират проблемите, с които те се сблъскват в процеса. Получените данни са обработени и анализирани за целите на дисертационния труд, като са представени различните обобщени изводи, препоръки и становища.

Обект, предмет, цели и задачи на изследването:

Основен обект на настоящото изследване е процесът на формиране на националните политики по сигурността и прилагане на предвидените от тях мерки, обезпечаващи ефективното им функциониране в условията на ускорено развитие на ИКТ. Разглеждат се актуалните тенденции и възникващите предизвикателства свързани с тях в областите на информационната и киберсигурност, като се анализират съществуващите решения, примери и добри практики от различни държави с традиции и установен напредък в тази област.

Като **основен предмет** настоящата разработка разгръща изследователския си потенциал върху ускоряващите се информационно-технологични промени и възникващите като резултат от тях социални следствия, които оформят специфични предизвикателства при създаването на политики, подходи и решения за управление на националната сигурност в аспекта на кибер пространството.

Фокус се поставя върху изследване процесите на преплитане на виртуалния и физически аспект в съвременния социум, като пряк резултат от интензивното информационно-технологично натрупване. Разглежда се начинът по който виртуалното пространството постепенно започва да оказва силно въздействие върху съзнанието (и респективно действията) на модерния човек, като по този начин пренарежда социалните отношения през 21-ви век.

Изследват се увеличаващите се предизвикателства при създаването на ефективни политики по сигурността с оглед постоянно усложняваща се информационна среда- от една страна и растяща взаимосвързаност и от друга – върху възможностите за решаването им. Всичко това е представено през призмата на значимостта на личните данни, като ключов елемент за политиките по информационна и киберсигурност, които са подложени на задълбочен преглед на настоящото изследване.

Цели на изследването:

Като основен приоритет научната разработка има за цел да оцени степента, в която актуалните политики в областта на националната сигурност адресират нарастващите предизвикателства в информационната среда, зададени от ускоряващата се технологична среда, в която оперират. Амбицията е не просто да се разкрие важността на технологичния аспект от киберпространството върху опериращите към момента системи и политики, ангажирани с опазването на националната сигурност, а представлява опит за поглеждане отвъд традиционните модели на обвързаност между управление на процесите в социума, насочени към гарантиране на целостта и сигурността на държавата и същевременно защитавайки личното пространство и неприкосновеността на нейните граждани.

Друга съществена цел на работата е свързана с прилагане на научен подход в изследването на един нов феномен – постепенното преплитане на киберпространство и реалност, като се изследва въздействието му върху когнитивните процеси на потребителите, с оглед разкриване на нови и малко познати аспекти на сигурността в информационните общества, като част от един много по-мащабен проблем, чиито рамки далеч надхвърлят технологично превъзходство и доминация на една държава/политически съюз/ над друга. Основание за подобни твърдения се търсят в множество резултати от съществуващи научни изследвания за влиянието на информационното пространство върху съзнанието, мотивацията и поведенческата психология на хората, които в последващ план имат реално отражение във физическата реалност.

Задачи

Основните задачи на настоящия труд са свързани с провеждане на изследване на няколко отделни компонента, които са логически подредени съобразно естеството на взаимовръзките им с оглед доказване основната теза на работата и респективно се представят в три обособени части като отделни глави.

Задача 1 - изследване на феномена „технологии“ и въздействието му върху процесите в социалната среда през 21-ви век с фокус върху промените в сферата на сигурността в новите информационни общества.

С оглед изясняване в максимална степен на различните аспекти на изследваната проблематика тази задача е разделена условно на три подзадачи, които включват:

А) Извършване на обстоен преглед на протичащото интензивно технологизиране при което се разкрива не само скоростта на проникването на технологиите в различните сфери на живота, а и ускореното им усложняване и взаимообвързване. Изследва се процесът на превръщането на цифровите данни в своеобразен стоков нематериален актив (комодитизация), който постепенно става гръбнакът на съвременните икономическите взаимоотношения. (Data is the new oil). Разкриват се ползите и заплахите от растящия потенциал на изкуствения интелект, изпълнявайки ролята на основна трансмисия за конверсията на информацията в знание. Разкрива се как ефективната обработка на огромни масиви от данни (Big data), става възможна от една страна поради нарастващата изчислителна мощ на съвременните процесори при постоянно смаляващ се обем и постоянно усъвършенстващите се софтуерни алгоритми за анализ – от друга.

Б) Анализ на ефекта и интензитета на по-горе изследвания феномен и проявленията му в социален аспект. т.е. - ако първата е насочена към разкриване на количествените измерения, тук се анализират качествените промени, които настъпват в процесите, дефиниращи обществените отношения в новата цифрова среда. Проследява се процеса на еволюция на информационното пространство и в частност на киберпространството до състояние на паралелна (нефизическа) реалност, в която текат изключително динамични процеси, отразяващи се пряко върху процесите, формиращи физическата действителност в социума.

В) Изследва се как влияе технологичното натрупване с подчертан акцент в сферата на ИКТ върху различни компоненти на сигурността, като се проследява развитието на този процес – от възникването и развитието на информационното (кибер) пространство и еволюцията му до своеобразна паралелна реалност, оказваща все по-голямо влияние върху процесите в реалния живот. Представя се нов прочит на

сигурността с оглед на растящото значение на личните данни, като резултат от проникването на технологиите и киберпространството в бита на съвременното информационно мрежово общество. Поставя се фокус върху разкриване важността на релацията Данни – Информация – Знание, като ключов компонент за еволюцията на процесите в съвременните общества.

Задача 2 - Извършване на преглед на развитието на политиките по национална сигурност с оглед отразяване динамиката на процесите и многообразните предизвикателства в условията на интензивно развитие на технологиите и еволюцията информационното пространство. Прави се анализ на модерните концепции в областта на киберсигурността, дефиниращи рамките за функциониране на съществуващите актуални решения в сферата във водещите технологични държави – САЩ, Китай, Русия, Израел, като накрая се сравняват със съществуващите такива в България. Разглеждат се различните подходи при търсенето на решения в страни с различни социално-културни икономически и технологични специфики, които се отразяват още на ниво дефиниране на ключови понятия по отношение на националната сигурност във виртуалното пространство и съответно на начините и похватите за нейното гарантирането и дългосрочно обезпечаване.

Задача 3 - Разкриване на най-съществените предизвикателства при разработката и имплементирането на ефективни мерки по осигуряване на сигурността в киберпространството– както на ниво държава, така и на ниво организации и отделни лица, като ключови фактори за развитието на информационното общество в новия век. Прави се оценка на състоянието на проблема, като се ползват различни методи и инструменти на изследването, включително сравнителен и риск анализ, както и кабинетни проучвания. Тук са идентифицирани и съществуващи добри практики за изграждане ефективни решения за приоритизиране на информационната и кибер сигурност с оглед все по-засилващото се въздействие върху националната безопасност.

Задача 4 - Провеждане на анализ на отделен случай - личните данни и политиките за гарантиране на сигурността им, като конкретен пример, показва как в съвременната технологично обвързана среда личните данни на потребителите придобиват все по-голяма стойност и могат да бъдат използвани като катализатор на събития, застрашаващи не само личната им сигурност, но и сигурността на ниво държава, общност или икономически съюз. По този начин се доказва съществуващата пряка зависимост между информационната сигурност на ниво индивид / група от хора или организация и националната сигурност. Освен това се разглеждат и възможностите за постепенно

приоритизиране на ролята на личните данни и гарантиране на тяхната неприкосновеност като ключов компонент на киберсигурността.

С цел максимална аргументация на заявената теза е проведено комплексно изследване, което се разгръща в няколко основни направления, организирани върху три компонентна структура, включващи следните подзадачи:

А) Анализ на конкретни политики в областта на защитата на личните данни. Тук се поставя фокус върху изследването на GDPR като водещо глобално решение на съществуващата проблематика, но наред с него се разкрива и опитът на водещите технологични държави извън ЕС в тази сфера. За целта се извършва преглед на съществуващата изследователска и нормативно-правна литература в областта, като акцентира върху анализ еволюцията на мерките по отношение управлението на данните, които постепенно се превръщат в основен фактор за формиране на модерните политики за информационна, кибер и национална сигурност, осигуряващи последващо икономическо, културно и социално развитие.

Б) Анализ на политиките за защита на личните данни в България.

Анализира се постигнатото до този момент в българското законодателство по отношение на предвидените мерки за защита на личните данни, като се прави преглед на няколко съществени документа – влезлият в сила от 25 май 2018 Регламент на ЕС 2016/679 относно защита на физическите лица във връзка с обработването на лични данни и относно свободното им движение, както и Закона за защита на личните данни и релевантните подзаконови нормативни актове, имащи отношение към разглежданата тема. Анализират се мерките които те предвиждат за гарантиране сигурността и неприкосновеността на личните данни както на ниво държава, така и в корпоративния сектор и на индивидуално ниво, като се оценява тяхната ефективност и ефикасност.

Г) Изследване на съществуващи решения и създаване на практически предложения относно възможностите за имплементиране на политики по управление на личните данни, базирани на технологията blockchain в действащите системи на електронното правителство. Работният вариант е базиран на проведено изследване на подобен тип решения в други страни, като е съобразен със спецификата на конкретната ситуация в България, както в икономико-технологичен аспект, така и в социално-културен и политически. Представен е анализ, чрез който се инициализират редица неизползвани възможности за по-ефективното им управление, като същевременно се изследва връзката между сигурността на личните данни и потенциала им за въздействие върху сигурността в на индивидуално, организационно и национално ниво.

Изследователска хипотеза

Основната теза на дисертационния труд е свързана с разбирането, че в края на второто десетилетие на 21-ви век в следствие на повсеместното проникване на информационно-комуникационните технологии протича интензивен процес на трансформиране на обществата от пост-индустриален тип в нов вид глобално-информационен мрежови социум, характеризиращ се преди всичко с огромна степен на свързаност и взаимозависимост на процесите.

В тази нова среда политиките за национална сигурност вече не могат да функционират ефективно, базирайки се на принципите за гарантиране на безопасността на страната, бизнеса и гражданите, обслужвали индустриалната епоха..

Основен аргумент за това твърдение е, че в прехода от пост-индустриално към информационно общество се променя структурата на самата реалност в следствие еволюцията на информационното пространство, което постепенно се превръща в своеобразен конструктор (дефинитив) на реалността. Спешната необходимост от приоритизирането на този феномен за политиките по национална сигурност се явява логическо следствие от нарастващата технологична зависимост на процесите в социума през последните десетилетия.

Предизвикателствата тук са свързани с факта, че в тази технологично обусловена среда мрежовите функции на отделните социални единици и групи вече са достигнали нивото, при което лесно могат да катализират „ефект на пеперудата“ и реално да се причинят както значими поражения, така и огромен положителен ефект върху компактни маси от населението на планетата. Това изисква комплексно изследване на проблематиката, свързана с опазването на личните данни в новата информационна среда, като през анализа на този специфичен елемент от политиките за сигурността се разкрива ключовото им влияние на индивидуално-групово, организационно, държавно и национално ниво.

Изследователски подход и методи на изследване

Основните методи, използвани при провеждане на изследванията, предмет на настоящата работа, включват изследване на съществуващата литература в областта, преглед на различни стратегически и юридически документи, провеждане на кабинетни проучвания.

На следващо място от научния инструментариум се използват дискусии във фокус групи, с представители на различни сфери на бизнеса, държавната администрация и академичната общност. Тук основна цел е да се дефинира от една страна същността на проблема с личните данни за участниците, а от друга – да се представи тяхната перцепция за важността на опазването на неприкосновеността им и да се идентифицират проблемите, с които те се сблъскват в процеса. Това е особено полезно в процеса на полагане систематични усилия за преначертаване на „менталните карти", които обикновено съществуват в управляващите по отношение разбирането за сигурността в условията на ускорено технологично развитие и интензивни социални промени и способността им да катализират ефективното й управление. За набиране на емпирични информация са проведени и интервюта с ключови участници във формирането на политиките по киберсигурност в областта на личните данни и националната сигурност.

Като трети елемент в изследователската дейност са използвани различни похвати от съществуващия научен инструментариум за анализ и по-специално:

- Сравнителен и контент анализ – извършен чрез позоваване и сравнение с налични решения в сектора на националната сигурност в други държави и съществуващи добри практики в сферата на киберсигурността,
- PEST анализ - за определяне на дългосрочни ефективни политики, базирани на получена реалистична информация за средата от инструменти за идентифициране, проследява, прогнозиране и оценка на промените в политическата, икономическата, социално-културната и технологичната среда и съответните движещите сили, които ги предизвикват.
- SWOT анализ – като инструмент за стратегическо планиране е използван за определяне на силни и слаби страни, възможности и заплахи, свързани с политиките за защита на сигурността у нас.

Целта е чрез използване на тези инструменти за анализ да бъде формиран качествен информационен ресурс по отношение наличните възможности за създаване на мерки по управление на процесите в киберпространството. На второ място да се оцени възможността и ефективността от тяхното приложение като инструмент на политиките за национална сигурност на база реална оценка на съществуващите рискове в средата

чрез тяхното правилно идентифициране, оценка и разработване на мерки за минимизиране на въздействието им.

Използван е и похватът на сценарийното планиране за идентифициране и формиране на предположения за бъдещето в конкретни стратегически планове в качеството му на инструмент за валидиране на прогнози, направени с помощта на различни конвенционални средства. Освен ефективността на този похват по отношение дефиниране база за проследяване на промените в характеристики на средата за сигурност, той гарантира избягване на субективизма и прекаления оптимизъм по отношение на бъдещи нейни състояния в краткосрочен и средносрочен план.

Ограничения и допускания

С оглед на факта, че киберсигурността постепенно се превръща в интегрална част от политиките по национална сигурност настоящата разработка основно изследва проблематиката на сигурността в триъгълника: технологии (в частност ИКТ), виртуално пространство (като паралелен свят, оказващ влияние върху физическия) и лични данни (като фактор за управление на сигурността в новата дигитална среда).

Фокус в процеса на научно-изследователска работа е поставен върху разкриване на нови и малко познати аспекти от проблематиката свързана с личните данни, с цел да се идентифицират нови възможности за създаване на модерни гъвкави и ефективни политики по отношение на тяхното опазване и гарантиране на личната неприкосновеност като фактор с ключово значение за националната сигурност. Съзнателно не са представени обстойно техническите аспекти на обезпечаване на мрежова и информационна сигурност (като обезпечаване на софтуерната и хардуерната защита на сървърите за съхранение на данните и поддържане на оперативна непрекъснатост на мрежите, гарантираща тяхната преносимост и неприкосновеност), предвид това, че те са обект на множество допълнителни изследвания.

II. Структура и съдържание на дисертационния труд

Структура на дисертационния труд

Изследването е структурирано в уводна част, 3 глави и заключение, като съдържа:
Общ обем: 239 страници, от които същинският текст е 227 страници;
Литература: 24 източника на български език; 45 на английски език; 5 на руски език, 29 електронни източника; Таблици: 2, Графики и фигури: ... (5 фигури; 3 графики);

Структурата на основното съдържание на труда включва:

ГЛАВА I – СОЦИАЛНИ ЕФЕКТИ ОТ РАЗВИТИЕТО НА ТЕХНОЛОГИИТЕ И ЕВОЛЮЦИЯТА НА КИБЕР ПРОСТРАНСТВОТО

Технологии – генезис, развитие и приложения

Аспекти на технологичното натрупване в ИКТ сектора

А) нарастване на изчислителна мощ и минимизиране на размера

Б) темп на генериране на информация

В) възможности за съхраняване на информация

Г) интернет потребление и свързаност

Данните като основен ресурс в новата информационна среда

- Лични данни
- Отворени данни
- Метаданни
- Големи масиви от данни (big data)

Аналитични алгоритми за обработка на данни

Възникване, развитие и еволюция на информационното пространство

Социални ефекти на технологичния напредък

- Финансово - икономически аспекти
- Дигитализация на физическия свят
- Етични проблеми с технологичните платформи

Нови измерения на сигурността в информационната среда

- Повишаване на несигурността
- Информационно-технологична зависимост
- Кибер пространството като арена на реален сблъсък

ГЛАВА II – ПОЛИТИКИ ЗА НАЦИОНАЛНА СИГУРНОСТ (ПНС) КАТО ФУНКЦИЯ НА ПРОМЕНЯЩАТА СЕ ИНФОРМАЦИОННА СРЕДА

Парадигми на националната сигурност

Еволюция на науката за национална сигурност

Киберсигурността, като приоритет за политиките по национална сигурност във водещи военно - технологични държави

Понятиен апарат на политиките по киберсигурност

ПНС в някои от водещите военно-технологични държави в света

- Съединени американски щати
- Китай
- Русия
- Израел

Политики за национална сигурност в България

- Стратегически и нормативни рамки на сигурността
- Информационна и киберсигурност като ключов аспект на НС
- Органи и функции

Общи изводи и препоръки

Стратегически предизвикателства при управлението на киберсигурността

PEST анализ на рамката за изграждане на ефективни политики за киберсигурност

SWOT анализ на действащата рамка за опазване киберсигурността в България

ГЛАВА III – ЛИЧНИ ДАННИ И ПОЛИТИКИ ЗА НАЦИОНАЛНА СИГУРНОСТ

Нови тенденции и проблеми в областта на личните данни и сигурността

Лични данни като фактор за национална сигурност

GDPR като отправна точка за стандартизиране опазването на личните данни в страните на ЕС

- Принципи
- Органи
- Дефиниции
- Проблеми с имплементацията на регламента
- Права
- Санкции

Правна защита на личните данни извън страните на ЕС

- Съединени американски щати
- Русия
- Китай
- Израел

Политики за сигурност на личните данни в България

Изводи и препоръки

Възможности и предизвикателства пред имплементиране на технологични решения от типа на blockchain при защита на личните данни

ЗАКЛЮЧЕНИЕ

БИБЛИОГРАФИЯ

Съдържание на дисертационния труд

Научното изследване е представено в три отделни глави, които са логически подредени съобразно естеството на изследваната проблематика, с оглед доказване основната теза на разработката.

Глава I – Социални ефекти от развитието на технологиите и еволюцията на кибер пространството

В тази глава се разглеждат процесите на технологично натрупване, обуславящи последващата експанзия на информационното пространство, в следствие на ускореното създаване и обмяна на данни в мрежата. Изследват се различните проявления на този феномен и се анализира информационната свързаност, като съществен елемент за обезпечаване на ефективността на ключови социално-икономически и политически процеси в съвременните общества.

Описва се съвременният дигитализиран свят, като се акцентира върху технологичната наситеност във всички сфери. Търсят се аргументи в подкрепа на твърдението, че технологиите до такава степен са се развили и проникнали в ежедневието ни, че на практика го дефинират. Това натрупване води след себе си и рязко увеличаване на генерираните данни и респективно на обменяната информация. изцяло променя средата на обитание на съвременния човек. По този начин се извършва концептуална качествена промяна в системата и начинът, по който оперират обществата. Аргументира се необходимостта от нов подход в решаването на проблемите, свързани със сигурността в новата среда, обусловен от наличието на многофакторност и висока степен на взаимообвързаност на процесите.

Изследва се еволюцията на киберпространство до ниво на паралелна реалност, характеризираща се със своя собствена динамика, принципи, структура и проблематика и постепенното му превръщане в основен слой, в който текат процеси тясно обвързани със събитията във физическия свят, като се акцентира върху изследване на взаимовръзките между тези два свата. Изводите, направени на база изследването, показват, че е нужна не просто промяна на модела, а в създаване на нови архетипи в обществата, способни не просто да се адаптират към промяната, а да я управляват и да оползотворят потенциала на нацията.

Технологии – генезис, развитие и приложения

Изследването започва с преглед на технологичния аспект от развитието на съвременните общества, като прави преглед на съществуващите варианти на дефиниции за технология, а именно: „Практическо приложение на знания в определена сфера". Друго определение гласи: „Технология е знание и използване на средства, техники, системи или методи за организация за решаването на проблем или за нуждите на друга цел. Технологиите значително въздействат върху способността на човека и на другите животински видове да контролират и да се адаптират към тяхната естествена среда".

Поставя се акцент на „прилагане на знание", чрез което в последствие се въздейства върху средата. Това е особено важно в светлината на разглежданата проблематика в настоящата разработка, а именно – способността на човека да влияе върху заобикалящата го действителност, с оглед осигуряването на безопасното му съществуване и интензивното му развитие при оптимално и ефективно използване на наличните ресурси. Това уточнение е важно, защото днес светът е тотално доминиран от технологиите, при това до степен, при която резонно възникват опасения относно зависимостта на човешките същества и способността им да се развиват без тях.

Аспекти на технологичното натрупване в ИКТ сектора

За цялостното изясняване на различните аспекти на технологичната еволюция този процес е разгледа през призмата на няколко ключови дименсии, чиито синергичен ефект в голяма степен определя качествените изменения на информационната среда.

А) Нарастване на изчислителна мощ и минимизиране на размера

Б) Темп на генериране на информация

В) Възможности за съхраняване на информация

Г) Интернет потребление и свързаност

На база на до тук информация, по отношение на технологичното натрупване, ще представим йерархично всички изброени основните фактори, определящи динамиката на развитието на информационното пространство:

- развитие на изчислителна мощ за обработка на информация
- способност за създаване обмен на информация – текст, графика и др.
- наличие на информационни носители и създаване на масиви от данни,
- възможности за достъп до информационните масиви,
- брой активни ползватели на информацията
- скорост на дистрибутиране/трансфер на информацията.

Възникване и еволюция на информационното пространство

Проследява се как технологичното натрупване служи за основата на възникването и развитието на информационната глобална мрежа Интернет, което от своя страна в последствие създава рамката, върху която възникват информационното и киберпространство. Въз основа на представената информация относно се прави извода, че то постепенно еволюира до паралелна реалност, в която протичат изключително динамични процеси и дневно са ангажирани мозъците на близо 4.5 млрд. души.

Обръща се внимание на няколко фундаментални фактора, които в голяма степен се явяват катализатор за формирането, развитието и ефективното функциониране на нов по своята същност информационен слой на планетата, за чието съществуване се заговаря още през далечната 1927 г. от френските философи ле Роа и Теяр дьо Шарден. Те лансират за първи път теорията за наличието на нематериален слой, който обхващаща земята подобно на "мислеща" обвивка, формирането на която е свързано с възникването и развитието на човешкото съзнание и разглеждат ума като специален природен феномен. В последствие украинският учен В. И. Вернадски дефинира този слой като „ноосфера“ (от гръцки. nóos - разум) - сфера на взаимодействие между природата и обществата, в чиито рамки разумната дейност на хората става главен, определящ фактор за развитие (за обозначение на тези сфера се употребяват също така сходни термини: техносфера, антропосфера, социосфера).

Данните като основен ресурс в новата информационна среда

Данните днес представляват изключително ценен актив, който е гръбнакът на информационните общества и чрез който стана възможно експонентното развитие на съвременните процесите на оптимизация и глобализация на производството на стоки, услуги и търговията. По същият начин, по който изкопаемите горива са в основата на

индустриалния възход на човечеството, днес информацията е фундамент на радикални процеси, преначертаващи рамките на функциониране на обществата през новия век. Като аналогът може да бъде доразвит и по отношение на работата с основния ресурс – ако преди нефтът се е рафинирал и това е допринесло не просто за развитието, а за възникването на цели индустриални сектори от съвременната икономика, то днес същото се случва и с информацията: тя не просто се генерира, а се обработва, записва, структурира, класифицира, анализира.

Въз основа на това се прави извода, че нуждата от качествена информация ще се приравнява все повече на нуждата от храна за физическо оцеляване на индивида. Сам по себе си този извод поставя множество сериозни въпроси за решаване, особено когато се касае за управление на процесите в киберпространството, свързани с опазване на личната информация, конфиденциалност и като цяло информационната сигурност.

Аналитични алгоритми за обработка на данни

Наличните решения за ютилизация на данните възникват като резултат от развитие на информационната мрежа и растящото количество данни, които естество провокираха и еволюцията на софтуерните инструменти за обработка, клъстериране, категоризация и последващ анализ. Възхода на социалните мрежи увеличи интереса към идентификация на обекти в текста като инструмент за наблюдаване на общественото мнение по определени теми чрез проследяване на движението на сентимента към тях сред потребителите. Предлагат се даже услуги за изчисляване на настроението на публикации в социалните мрежи в реално време чрез API за достъп до услугата.

В този смисъл може би най-точно можем да синтезираме ситуацията в края на второто десетилетие на 20-ти век в следните три важни фундаментални извода, дефинирани от Ц. Семерджиев, обобщаващи всички постижения, а именно:

- създаването на ефективни технологии за автоматично извличане и обработка на знания оказва решаващо влияние върху процесите на формиране на онтологичните концепции и модели за устройството на света и води до смяна на начина на мислене и общоприетите възгледи.
- авангардните информационни технологии необратимо формират нов клас интелект, съществуващ извън човешкия разум;
- знанието е “окото на разума” на изкуствения интелект, а компютърната обработка на естествения човешки език придава смисъл на идеите и концепциите, като продукти на този разум;

Социални ефекти на технологичния напредък

В тази част изследването проследява качествените промени, които възникват в начините, по които функционират обществата, като следствие от количествените изменения, описани в предходните части. Използват се аргументи в подкрепа на твърдението, че "*Технологичните промени до голяма степен са отговорни за подобряването на човешкото благосъстояние, независимо от размера на населението, удължаването на продължителността на живота, нивото на образование, жизнения стандарт, промените в работата, телекомуникациите, здравеопазването, както и ефектите на човешките дейности върху нашата среда*" (Ник Бостром, 2007)

Въпреки че посочените примери за технологичен напредък са главно от сферата на телекомуникационната и компютърна индустрия, идентично развитие имат почти всички сфери на науката с приложение в реалния живот. Съществени постижения могат да бъдат посочени в областта на медицината – проектите за разкодиране на човешкия геном и за картографиране на човешкия мозък, които станаха възможни сериозен тласък с миниатюризацията на процесорите и паралелното развитие на нано-технологиите, комбинацията от които създава почти нереални възможности за диагностика, лечение и превенция на различни болестни състояния у хората.

Финансово - икономически аспекти

Изследват се основните причини за нарастващото чувство за несигурност у хората, като се доказва , че в голяма степен те са следствие от това, че светът в момента минава през дълбока форма на трансформация, която засяга изначално всички сфери на съществуването на съвременния хомо-сапиенс. Икономическите проявления на този феномен могат да бъдат намерени в почти всички аспекти от бизнес средата – предлагане на споделени услуги и ресурси, автоматизация на транспорта, дигитализация на процесите, възход на крипто валути и алтернативни форми на банкиране и много други.

Все по-често хората днес се сблъскват с предизвикателствата на съвременния социум, създадени при условия за нарастващо объркване от множеството избори и възможности, които ни се предлагат. Наред с това в новият динамичен и технологичен век се създава огромен психологически натиск върху хората, като резултат от постоянното въвеждане на нови и нови технологии в почти всички аспекти на социалните отношения и процеси. Постепенно стана така, че ученето през целия живот се появи като основно изискване за развитие на хората в съвременните общества.

В този аспект е важно да се подчертае, че технологичното развитие на света не може да се разглежда едностранно само като позитив от еволюцията на науката. До голяма степен именно то предопредели и генезиса на множество проблеми и събития от глобален характер през последните десетилетия, които стават естествен фокус на политиките, ангажирани с националната сигурност.

Естеството на този модерен феномен е следствие от извършващия се фундаментален преход на обществата към качествено нов стадий на функциониране на взаимоотношенията в тях. А това стана възможно чрез интензифициране процеса на информационен обмен, което предостави възможност не само за натрупване на информация, но и за нейното ефективно трансформиране в знание. Тук е моментът да се подчертае, че за разлика от материално-веществените активи, информационният актив се подчинява на съвсем различни принципи, които обуславят и неговата употреба по изключително различен начин при конверсията му в крайния продукт - знание. Съответно двата основни източника, които се използват, за да се извлече то, са информацията и данните.

Етични проблеми в технологичните платформи

Друг основен проблем, върху който се акцентира в тази част е свързан с това, че личните данни постепенно придобиват все по-голяма важност по отношение на сигурността, като тяхното влияние е многопластово и често пъти остава скрито за неангажирани с темата лица. За съжаление в публичното пространство този проблем все още се разглежда просто като фактор на персоналната сигурност и не се приемат в достатъчна сериозност от обикновените хора извън отражението им върху личния живот.

В този смисъл най-често срещаните притеснения са свързани с потенциално изтичане на финансова информация, с която може да се злоупотреби – акаунти за онлайн банкиране, номера на кредитни карти и т.н. Друг аспект от съображенията за опазване на персоналните данни е свързан с изтичането на лична информация – текст, снимки, видеа – на лица в интернет, които потенциално могат да нанесат имиджов ущърб или да се използват за злепоставянето му, като тук отново ще подчертаем, че често пъти дадено лице може дори да не подозира, че свързана с него информация може да бъде оперативно интересна за трети лица или в конкретен момент да е от важност поради една или друга причина за публиката.

Тук отново е необходимо да се подчертае, че в условията на почти повсеместна обвързаност на информация, комуникации и процеси в обществото често пъти

сигурността на информацията на един индивид може да има огромни последици върху сигурността на други конкретни хора, групи или организации, включително и на ниво държава. В този контекст защитата на личните данни и поверителността е естествено да се приоритизира до степен на важност не по-ниска от нивото на изправност и функционална способност на мрежите и защита на хардуерната инфраструктура като елемент на киберсигурността.

Мерките за защита обаче не бива да бъдат налагани от някакъв конкретен закон или директива, а трябва усилено да се работи върху образованието и разпространяване на знание за необходимия санитарен минимум от действия, които потребителите трябва или не трябва да извършват, за да запазят информацията си сигурна или поне да ограничат в голяма степен възможностите за нейното дискредитиране.

Друг важен елемент от тази част е свързан с изследване на въздействието на ИКТ върху децата, като особено беззащитни и особено силно предразположени към негативното влияние. Отбелязва се, че от години водещи психолози и педиатри предупреждават за опасностите и щетите, които нанасят постоянното излагане на детското съзнание на различните дигитални устройства - телефони, таблети, телевизори и т.н., които предоставят възможност децата да консумират (често пъти безогледно) разпространявано през интернет медийно съдържание. Ефектите особено върху деца в ранна възраст - 2-5 години са особено деструктивни по отношение на влиянието върху когнитивните им способности и възможности за социална интеграция. Наблюдава се нарастваща агресивност, тенденция към развитие на остри форми на различни психични разстройства, липса на емпатия и затруднение за комуникация в реални битови ситуации. Причините за това са разбира се много и разностранни, но основния проблем е в конкретния икономически модел, който е гръбнака на тези технологични устройства, които се използват като прокси за доставка на малки дози допамин в мозъка.

На този принцип е създадена и оперира успешно повече от десетилетие цялата плеяда от социалните мрежи - Facebook, Instagram, Snapchat и др., като въздействащият фактор принципно е абсолютно същият, както е и с цигарената индустрия. Във филмовата класика от края на 90-те - вътрешен човек, пресъздаваща реалните събития свързани със заведено дело срещу тютюневите гиганти в САЩ - главният герой (известен инженер-химик, ангажиран в голяма компания от бранша), свидетелства пред комисията, която разследва никотиновия картел - 5те големи компании. Той обяснява от гледна точка на технологията, какво представлява за компаниите цигарата - устройство за доставяне на никотин. И съответно колкото по-силно е въздействието върху мозъка на

потребителя, толкова по лесно е той да бъде закачен (hooked) завинаги, превръщайки човека в страстен пушач, който с нетърпение купува следващата кутия с цигари за да задоволи този глад. Днес се заклеймява повсеместно употребата на тежките наркотици, които са прецизно направени от други инженер-химици, като тяхното въздействие е в пъти по силно и съответно по-смъртоносно от това на цигарите, превръщат хората буквално в безволеви марионетки, които биха направили всичко само и само да получат следващата си доза.

Не е много по-различно обаче начинът по който действат социалните мрежи. Принципът на „харесванията“ (likes) е внимателно обмислен и прецизно поднесен на потребителя от екипи психолози, които дълго време са изучавали възможностите за влияние върху съзнанието на потребителя. При получаване на харесване на публикуваното съдържание, мозъкът на потребителя отделя малки количества допамин, в следствие на това, че някой в мрежата е счел за интересно нещо, което е качено в дадената социална мрежа. Постепенното трениране на мозъка да продуцира подобно вещество в малки дози, но на чести порции създава аналог на състоянието абстиненция при наркоманията, при което съвременния човек все по често посяга към различните си електронни устройства - понякога за да си провери статусите в социалните мрежи, или мейла, или да погледне новините, или да види поредният видео клип в "YouTube”.

Всичко това е внимателно инженирано от създателите на различните уеб-базирани услуги, като бизнес моделът им е основан на следното - максимално дълго задържане на потребителя активен. Реално това представлява постоянно сменящи се кратки порции информация.

Съществуващите изследвания в областта на влиянието на интернет и информационните технологии върху човешкото съзнание и мотивационните вериги на съвременните потребители на мрежата ясно започват да очертават наличието на множество проблеми, произтичащи от постепенното обвързване на индивида със съществуващите технологични решения. Основна част от тях са заложени още в дизайна им и принципа, на който се основават – монетизиране на личните данни, чрез неправомерното им използване за максимизиране на печалба.

Нови измерения на сигурността в информационната среда

Тук се изследват нововъзникващите предизвикателства при опазване на сигурността, като следствие от масовото навлизане на микропроцесорите и силиконовите чипове в ежедневието на хората и развитието на възможностите за

комуникация. Днес се обменят милиарди битове информация в секунда, при скорост на движение, която позволява тя да бъде предавана и обработвана от хората в различните части на планетата на практика едновременно. Това води до ново качество в процеса на глобализиране заплахите в света, защото възможността отделни индивиди или групи от различни места да участват едновременно в едно и също събитие, без да е необходимо физическото им присъствие на едно място, фундаментално променя сигурността.

В тази коренно нова за представите ни среда, наситена с участници от нов тип е нормално да се очаква, че ще възникват аналогични на проблемите във физическия свят колизии. И тъй като войните за надмощие са били неизменна част от историята на човечеството и съвсем естествено е в новосъздадената среда да катализира процеси на доминиране и пренареждане на силите. Очакванията на мнозина изследователи в тази област бяха свързани с началото на новия век и последващото повсеместно проникване на технологии да доведат до нов тип сблъсъци в информационното пространство, което все по-отчетливо започва да доминира ежедневието ни като тенденция.

Множество изследователи застъпват аргументирано тезата на база преглед историята на човечеството от началото на новото хилядолетие, че в края на второто десетилетие на двадесет и първи век светът се характеризира с безпрецедентно технологично натрупване, в следствие на което е налице засилване на влиянието на няколко основни фактора:

- висока степен на комуникационна свързаност, непозната до този момент като състояние за света;
- глобализиране на процесите и голяма част от живота на планетата, взаимообвързаност,
- засилена диспропорция в социално-икономическо развитие не просто на отделните гео-политически и културни райони, неравнопоставеност.

Сигурността винаги е била основен приоритет в живота на хората през вековете. Не случайно тя е позиционирана на второ място веднага след базовите физиологични нужди в популярната „Пирамида на Маслоу“. Съответно ценността на този елемент за населението винаги е била висока, а това естествено обяснява защо в постоянно менящата се среда на обитаване за съвременния Homo Sapiens (до голяма степен функция на технологичния скок от последните 50 години), огромна част от населението на планета живее в една постоянно растящо чувство за несигурност, тъй като не успява да навакса степента на развитие на иновациите и тяхното проникване във всички сфери на социума.

Повишаване на несигурността

Наблюденията в тази част са насочени към дълбокия процес на трансформация, граничещ с тектоничните промени от прехода между феодалния към индустриалния строй, като това провокира нарастващото чувство за несигурност, която засяга изначално всички сфери на съществуването на съвременния човек. Ако в десетилетията след Втората световна война можеше ясно да се дефинират различията между двата враждуващи политически лагера – комунизъм с/у капитализъм – и да се прогнозират вероятните действия на едната или другата страна със сравнително голяма точност (принципа на реципрочен отговор), то в днешния технологично зависим и взаимообвързан глобален свят, нещата далеч не са толкова опростени.

Във време, в което дете с компютър с връзка с интернет може да предизвика повишаване на нивото на терористична заплаха в 2 американски щата, или възрастна жена в Тбилиси по невнимание да прекъсне оптичен кабел, осигуряващ интернет за почти цяла Грузия и Армения , обвързаността на националната сигурност със технологиите става все по-голямо предизвикателство за правещите политики в тази изключително важна сфера.

На фона на всичко това еволюцията на човека като съзнание, като отговорност се превръща в ключов елемент, който ще определи посоката за развитието на света. Защото технологията сама по себе си не е нито добра, нито лоша. Тя е просто инструмент за човека. Точно както ядрения синтез може да бъде преобразуван в енергия, захранваща електричеството за милиони семейства, така и в друга форма и използван за други цели, може да бъде причина за гибелта на същите тези човешки същества.

В този свят на нарастваща диспропорция в развитието на отделните региони и общества, технологиите имат силата / потенциала да изградят мостът към едно по-добро бъдеще, където ресурсната обезпеченост ще бъде далеч по-ефективна. Към днешна дата е налице уникалната ситуация, при която човечеството произвежда все повече, налични са все повече блага и паралелно с това расте броят на гладуващите, умиращите от болести и процентът на неграмотното население.

Глава II – Политики за национална сигурност (ПНС) като функция на променящата се информационна среда

В тази част на изследването се фокусира върху две основни направления:

Извършване на преглед на развитието на политиките по национална сигурност с оглед отразяване динамиката на процесите и многообразните предизвикателства в условията на интензивно развитие на технологиите и еволюцията информационното пространство. Прави се анализ на модерните концепции в областта на киберсигурността, дефиниращи рамките за функциониране на съществуващите актуални решения в сферата във водещите технологични държави – САЩ, Китай, Русия, Израел, като накрая се сравняват със съществуващите такива в България. Разглеждат се решения в страни с различни социално-културни икономически и технологични специфики, които се отразяват още на ниво дефиниране на ключови понятия по отношение на националната сигурност във виртуалното пространство и съответно на начините и похватите за нейното гарантирането и дългосрочно обезпечаване.

Разкриват на най-съществените предизвикателства при разработката и имплементирането на ефективни мерки по осигуряване на сигурността в киберпространството– както на ниво държава, така и на ниво организации и отделни лица, като ключови фактори за развитието на информационното общество в новия век. Прави се оценка на състоянието на проблема, като се ползват различни методи и инструменти на изследването, включително сравнителен и риск анализ, както и кабинетни проучвания. Изследва се как киберсигурността става крайъгълен камък или отправна точка при изграждане на всяка една система за сигурност – било тя отбранителна, икономическа, финансова, енергийна, социална, културна и т.н. Принасят се доказателства към тезата, че тя става все по-важен елемент от националната сигурност поради фактът, че информационната среда се превърна в носещ слой на всички останали видове социални системи.

Парадигми на националната сигурност

Основните изследователски усилия в тази част са насочени към подхода за анализа на средата, която ще определи обхвата на едни ефективни политики за национална сигурност е особено важно да се вникне в същността на произтичащите процеси на глобализиране във всички сфери на живота

Понеже днешните информационни общества имат съвсем други потребности, които към момента са или латентни или в много начален стадий на своето развитие, то е

нормално да се предполага, че новите политики, насочени към сигурността, биха имали съвсем друг характер. Липсата на унифицирани действия по отношение на управлението и контрола на новата среда от страна на водещите държави е разбираем, предвид това, че в момента света е буквално в нова ера на велики, макар и не географски открития. Подобно на тях обаче те ще имат определящо въздействие върху бъдещото развитие и оформяне на информационните общества и отношенията в социума

Ако в предходната част бе описано как експонентното развитие на технологиите оказва огромно влияние върху темпа на развитие на средата, то тук е направен извода, че поради все по-голямото обвързване на различните аспекти от живота ни с информационната среда може да се очаква, че в бъдеще този процес ще се ускорява. А това неминуемо ще увеличава както предоставяните възможности, така и съществуващите рискове в средата. Проблемът основно се състои в това, че поради динамиката на процеса не винаги е налична адекватна информация относно съществуващия риск, което прави изключително трудно последващото му неутрализиране.

В следствие на това в съвременния свят понятието „национална сигурност“ отдавна излезе от клишето на разбиране на ниво приравняването му с военна сигурност и последващите от това заключения, че една държава е толкова силна, колкото силна е й армията, като съответно колкото повече отделя от БВП за отбрана и въоръжаване, толкова по-гарантирани са безопасността и спокойствието на населението й. Разбира се не трябва да се подценява и чисто военните аспекти на понятието, но те все повече отстъпват пред технократичната вълна, обхванала света в началото на 21 век. Технологиите позволиха на някои държави да се откъснат толкова напред в развитието на военните си разработки, че на практика войната с тях на страни от 2-ри ешелон , се свежда до това едната да мобилизира цялата си налична армия, ресурси, а другата буквално чрез няколко елитни звена, управляващи високо-технологични оръжия, да неутрализират бързо, ефективно и ефикасно въпросният конфликт. Примерите от началото на новия век са много – операциите на САЩ в Ирак и Афганистан от 2003-та, конфликтът Русия – Грузия от 2008 г., размириците в ивицата Газа между Израел и Палестина и др.

С технологичният възход през последните десетилетия в една толкова сложна сфера каквато е сигурността, възникнаха множество нови предизвикателства пред ангажираните с правене на политики по осигуряването й. До голяма степен причината е, че в новата технологично обусловена, постоянно променяща се взаимообвързана среда е

налице промяна в основната парадигма – Кой е основния производител на услугата национална сигурност (дали това е само държавата) и кой потребителя (дали са само гражданите на дадената държава). Същевременно е налице миграция от индустриалния модел, при който е налице ясно дефинирана заплаха (враг) и симетричните свързани с нея заплахи, към ситуация, в която основният проблем се явява липсата на достатъчно информация за заплахата (чисто практически от кого се пазим – друга държава, терористична група, климатични и здравни катастрофи. На лице е промяна в самата система за национална сигурност, при която функционирането на конкретните й параметри се определя от типа, интензитета и сложността на заплахата.

Друг важен момент от изследването в тази част е свързан с процеса на създаването на ефективни политики в сферата на сигурността в една силно глобализирана среда. Което до голяма степен прави всяка една действаща система за национална сигурност неизбежно функция и съответно източник на несигурност за събития, които могат да имат глобално въздействие. Причини – свързаността на процесите в социума са стигнали до такова ниво, при което действия, насочени към пробив в сигурността на една държава се извършват с висока степен на вероятност в различни части на света при съответната координация и споделяне на ресурси – технологии, знания, капитал, хора и т.н. С оглед на това изграждането на съвременни политики за сигурност днес е изключително сложен и ресурсоемък процес, с оглед на еволюцията и на самата концепция за опазването й.

Отбелязва се, че съществуват условно три подхода при формиране на теоретичната постановка на националната сигурност, като разделението се базира на обхвата и структурата на парадигмите, които определят и последващото наблюдение на проблематиката:

- Класическо възприятие на националната сигурност – най-общо може да се определи като индустриална представа за сигурността на една страна, под формата на географска цялост, неприкосновеност на границите и безопасност на гражданите. Присъщо за този тип схващане на сигурността е основаване на предимствата на една страна в чисто военно, икономически и политически аспект. Концепцията – колкото повече, толкова по-добре (количествени натрупвания в ресурсите по осигуряване на сигурността) на практика е основна при изграждането на политиките в този аспект. Ролята на армията и вътрешните сили за сигурност – полиция, разузнаване – са ключови за гарантирането й.
- Постиндустриален/информационно-технологичен/ подход – налице е еволюция в разбирането на националната сигурност под формата на увеличаване на

зависимостта й от други фактори – не чисто военни – или поне не в чистия вид на многобройна армия, въоръжена с конвенционални оръжия. Тук започва да се създава и акцента върху технологичното/информационното предимство. Все по-малко хора и все повече технологично съвършенство са необходими за воденето на войни и опазване на сигурността на страната. Възниква дефиницията за информационна сигурност, като компонент на националната. Тук много ясно започва да се откроява уязвимостта на една държава от отделни, фокусирани удари по обекти от критично значение за здравето, живота на гражданите и инфраструктурни обекти, върху които почива нормалното функциониране не обществото – електроцентрали, водоизточници, информационни хъбове, преносна мрежа и т.н.

- Глобалистичен подход – тук поле на националната сигурност е цялата планета. Осъзнават се възможностите и потенциала на средата, в която съществува света, да пренасят ефекта от удар по една държава върху останалите. Примери – потенциален срив на американската финансова система би причинил тотален икономически колапс в почти всички държави в света. Съответно интензитета на поражение ще зависи от количествената и качествена свързаност.

Използват се нов тип информационно-технологични оръжия за масово поразяване: така например такива, които работят върху околната среда (климатични оръжия), оръжия за електромагнитно поразяване (ЕМИ), информационно-психологични оръжия (фалшиви новини и др.), които изискват изцяло нов тип система за сигурност на страните, чиято основна характеристика вече е свързана с интегритета им. Поради тази причина днес водещите в технологично отношение държави развиват целенасочено и своите кибер армии, тъй като информационната структура на отбраната в 21-ви век е абсолютен приоритет.

Тук са разгледани основните функции на политиките за национална сигурност. ПНС като рамка, в която се описва как една държава осигурява сигурността на страната и гражданите си, като често всичко това е представено в един документ – стратегия за национална сигурност. В нея е очертана настояща и бъдеща роля, дефинирайки основните интереси на нацията и определяне на насоки за постигането им, както и справянето с текущи и перспективни заплахи и пълноценно използване на идентифицирани възможности. Обикновено те са с по-висок приоритет и интегрират приоритети на други политики за сигурност като военна доктрина, вътрешна сигурност, стратегия и др., които се отнасят до националната сигурност по отношение на нея конкретни агенции или проблеми.

Друг елемент който ги различава от другите политики е свързан с обхвата на темите, с които се занимават ПНС. Така се създават възможност за идентифициране както на вътрешни, така и на външни заплахи, като се стремят да интегрират и координират приноса на участниците в националната сигурност в отговор на интересите и приоритетните заплахи.

С оглед на това естествено ПНС определят най-важните национални интереси: физическата сигурност на нацията и нейния народ, поддържането на конституционната система и ценностите на страната и международната среда, благоприятстваща просперитета на нацията. За водещ документ, разкриващ същността на тези политики обикновено се счита стратегията за национална сигурност, който указва не просто как се предвижда да бъдат постигнат целите на политиките по НС, но определя и водещите органи и инструменти за имплементацията им. В този документ по принцип следа да бъдат идентифицирани и приоритизирани най-важните интереси на държавата, заплахите за тези интереси и целите, които тя трябва да преследва, за да осигури тези интереси. Тя трябва да определи ясни цели, както и средства за тяхното постигане, съобразени с моментната ситуация и способности за акумулиране на необходимия човешки, финансов, технологичен, интелектуален и културен ресурс.

Еволюция на науката за национална сигурност

Изследването на науката за националната сигурност е продиктувано от необходимостта да се отбележи постепенното изменение в различни нейни аспекти с навлизането на света в информационната епоха. И тъй като осигуряването на националната сигурност не е нещо, което може да бъде променяно лесно, поради естеството на генезиса си. Обикновено за ефективното и функциониране се изготвят стратегии с минимум 25 годишен поглед, а политиките внимателно се прецизират, за да се осигури тяхната кохерентност и ефикасност. В този смисъл авторът е наясно, че това изисква координираните усилия на голяма част от елита на обществото – управленски, административен, научен, граждански. Не трябва обаче трябва да се пренебрегва фактът, че националната сигурност вече оперира в една много по-динамична среда, където степента на промяна и непредвидимост рязко се повиши през последните години и тази тенденция не само ще се запазва, а ще се ускорява.

Проблемът с глобализацията на изследванията на националната сигурност, която фактически се прояви през последните две десетилетия, е, че сравнително малко на брой заплахи за сигурността са наистина глобални по своя характер. Ако с изменението на

климата например, както скептиците, така и поддръжниците обикновено признават, че този проблем ще засегне различни региони по много различен начин. Най-уязвимите обикновено се намират в по-слабо развитите райони, които и без това са по-предразположени към конфликти, глад и мор от развитите страни.

Но това важи и в особена сила за заплахите, свързани с болести и епидемии, като настоящата пандемия от COVID-19 е типичен пример. Както отбелязва проф. Кристиан Енемарк, „моментът, в който тежестта на дадена болест се определя като непоносима, обаче, до голяма степен е въпрос на политическа преценка“. Следователно прагът за секюритизация на подобна заплаха може да варира в различните държави и при различните болести. В такива условия ясно се вижда, че различни аспекти от сигурността въпреки, че могат да се управляват глобално (като идентифициране на мерки за защита и напътствие за реакция) от СЗО, ООН и др., то тяхното локално изпълнение варира значително в зависимост от конкретните икономически, властови, здравни и чисто културно-битови особености на съответните общества. Тук е особено важно да се открои важността на информационния аспект от политиките за национална сигурност, като конкретната ситуация нагледно показа как подценяването на този компонент може да има трагични последствия.

ПНС в някои от водещите военно-технологични държави в света

В неотдавнашната оценка (2016 г.) на заплахите в световен мащаб на разузнавателната общност на САЩ "кибернетиката и технологиите" са посочени като основен приоритет пред други до скоро значими заплахи, включително тероризма, разпространението на оръжия за масово унищожение и контраразузнаването. За да се разбере интензитета на нарастване на значимостта на тази сфера, трябва да се отбележи, че само преди десетилетие те бяха на края на този списък, което е аргумент за отделяне на бъдещо значително внимание на тази проблематика. Като се има предвид това обстоятелство, едва ли е изненадващо, че през последните десетилетия водещите световни военно-икономически и технологично напреднали държави в света масово инвестираха огромни ресурси (човешки, организационно-технически и разбира се финансови),. за да гарантират киберсигурността си. Само в САЩ през 2017 г. бяха предоставени на Министерството на отбраната 6,7 млрд. долара за кибероперации (Lyngaas, 2016), а държавата разполага с със специализирано Киберкомандване още от 2009 г.

С оглед изясняване на същността на проблематиката свързана с киберсигурността тук е направен обстоен преглед на понятийния апарат на политиките по киберсигурност. Един от проблемите при изследване на проблематиката е свързан с масовото навлезлите нови понятия в следствие развитието на интернет и постепенното му масово проникване сред все по-големи социални слоеве, които често пъти се използват без да се разбират достатъчно. В сектора на сигурността специално често се бъркат информационна и киберсигурност, като се считат за взаимнозаменяеми, макар че между тях съществуват важни разлики по отношение на обектите за които се използват.

В нашето съвремие киберсигурността е толкова дълбоко вплетена в тъканта на обществените отношения, че едва ли можем да назовем компонент от социума, който да не е в една или друга сфера повлиян от динамиката на дигиталния домейн. Поради тази причина е много трудно да се дефинира стриктно какво точно съдържа в себе си това понятие, поради факта, че то до такава степен е проникнало в съвременната действителност, че на практика това влиза в контекста на „сигурност на всичко и нищо“ (В. Милина). Или ако цитираме Доналд Ръмсфелд „Киберсигурността все повече започва да прилича на онова нещо, за което всички говорят но никой не го е виждал“.

По отношение на класическата система от компоненти, върху които се гради всяка национална сигурност, са изследвани ключовите елементи:

На първо място са представени стратегическите документи, които разкриват визията и посоката на развитие, както и целите, заложени за постигане от всяка една.

На следващо място е изследвана нормативната база в сферата на сигурността, която дава рамките и основата, върху която се определят отделните специализиран структури.

И на трето място са представени техните способности и правомощия за постигане на различните цели, указани в стратегическите документ.

Като следваща част от е направен преглед на ПНС в държавите САЩ, Китай, Русия, Израел, като накрая е представена ситуацията в България, като се прави структуриран анализ в три направления:

1) Стратегически и нормативни рамки на сигурността
2) Приоритизиране на информационна и кибер-сигурност
3) Структури и ресурсно обезпечаване

Разгледани са приоритетно политиките в сектора по сигурността в **САЩ**, като се отбелязва, че ако през 90-те е бил налице период на относително спокойствие поради липса на ясно отличим враг и заплаха, в началото на новото хилядолетие и по-специално след 11 септември 2001 г. проблема със сигурността и обществения дебат по нейното осигуряване рязко се покачва.

Представен е преглед на основни елементи от "Доктрината Буш" – отразени в Стратегиите за национална сигурност на САЩ от 2002 и 2006 г., водещи след себе си сериозни реформи в съществуващите разузнавателни структури в страната. В последствие са разгледани промените, настъпили в сектора с последващото избиране на Барак Обама за президент през 2009 г , където в Стратегията за национална сигурност от 2010 г. вече се определя, че САЩ играят глобална роля в поддържането на международния ред и че те ще се опитат да разпространят своите ценности в света, но не са готови да бъдат единствено гарант за поддържането на международния мир, като се отбелязва, че за първи път се повдига въпросът за кибервойната като ново предизвикателство пред световния ред. Проследена е промяната в отношението към Китай и Русия през вторият мандат на президента, който приоритизира в много отношения въпросите на националната сигурност на САЩ и по-специално кибер сигурността като аспект на националната сигурност. Прегледът завършва с обзор на промените в сектора след избора на Тръмп за 45-ти президент на САЩ оказва сериозно влияние върху приоритетите на сигурността на страната, като съответно се изследва как се отразява това във водещите стратегически документи.

По отношение на приоритизирането на кибер сигурността са изследвани трите стратегии за киберсигурност на САЩ от 2009 до 2020 като е направен обзор на основните приоритети в тях , а именно:

- Класифицирането на киберпространството като бойна среда

- Разширяване на принципите на колективната сигурност в областта на информацията и телекомуникациите. Кибератаките срещу критичната инфраструктура (КИ) се приравняват към военните атаки

- Въвеждане на понятието „Мрежоцентричност“, което се дефинира като характеристика на информационните среди, в които данните са основен и постоянен ресурс, отделен от софтуера, което ги прави достъпни за широк набор от аналитични инструменти в рамките на областта и извън нея.

По отношение ситуацията с ПНС в **Китай (КНР)** е запазен подхода на анализ на основните стратегически документи в сферата на сигурността, като е отличено, че теоретичната основа на съвременната китайска политика за национална сигурност са идеите на Дън Сяопин, на които се основават както официалните китайски ръководители, така и учените в страната.

Националната стратегия за развитие е в основата на китайската политика за национална сигурност. Основата на националната стратегия за развитие е, първо, теорията за социализма от началния период и, второ, теорията за социалистическата пазарна икономика. Същността на тази стратегия е следната. Националното развитие на Китай трябва да се осъществява в среда на политическа стабилност и национална сигурност. Основната дългосрочна цел на китайския народ е да превърне страната си в просперираща, силна, демократична и цивилизована съвременна социалистическа държава. По отношение на кибер-аспектите от националната сигурност е важно да бъде подчертано, че Китай е сред водещите суперсили в света, които разработват свои собствени теоретични рамки в областта на киберсигурността. С оглед на това, че в глобалното киберпространство към настоящия момент липсва международна правна система, която да установява по законен начин норми и правила за поведение в тази сфера, афинитетът към нея с оглед нарастващото й значение за националната сигурност е разбираем дори за неспециализирания читател.

Водещата роля на Китайската комунистическа партия в процеса на създаването на пълноценна структура за киберсигурност и контрол на интернет, разбира се не може да бъде подценяван, като се счита че разработването на подходяща правна рамка с одобрено от закона разделение на гражданските и военните функции, ще гарантира ефективно националната сигурност в киберпространството. Съответно представени са двата водещи документа в сектора - Стратегията за киберсигурност на Китай и законът за киберсигурност от 2017 г.

Представени са накратко някои от водещите технологични проекти по отношение на сигурността в Китай като : Проект „златен щит“, част от който е добилият известност в света „голям китайски файъруол“, лимитиращ достъпа от и доо китайското информационно пространство, както и инициативата „система за социален кредит“, която функционира от началото на 2021 г. официално.

В заключение са представени звената и структурите, ангажирани с опазване на киберсигурността в страната, като специално внимание е отделено на 56-ти и 57-и научно изследователски институти, които основните звена на китайската кибер-армия.

По идентичен начин е разгледана и ситуацията в **Русия** с респективните стратегически рамки, закони, органи и мерки насочени към опазване на сигурността и по-специално информационната и кибер сигурност.

Стратегията за национална сигурност на РФ определя стратегическите национални приоритети в сферата на сигурността. Тя очертава и най-важните задачи, свързани със социалните, политическите и икономическите трансформации в модерния свят за създаване на безопасни условия за прилагане на конституционните права и свободи на гражданите на Руската федерация, като по този начин гарантира осъществяването на устойчиво развитие на страната, запазване на териториалната цялост и суверенитета на държавата.

Важни нови елементи, които са посочени като приоритет пред националната сигурност включват: „*Осигуряване опазването на културното и духовното наследство, достъпността на информационните технологии, както и информация по различни въпроси от обществено-политическия, икономическия и духовния живот на обществото*;

и чл. 80 „*Основните заплахи за националната сигурност в сферата на културата са доминирането на продукти на масовата култура, насочени към духовните потребности на маргинализираните слоеве, както и незаконните посегателства върху обекти на културата.“*

Направен е преглед на Доктрината за информационна сигурност“, която представлява система от официални възгледи за гарантиране на националната сигурност на Руската федерация в областта на информацията, като съдържа няколко важни общи положения и дефиниция на редица понятия. Тук са идентифицирани факторите, на които се дължи нарастването на заплахите за националната сигурност като:

Желанието на отделни държави да използват софтуерни и технологични предимства, за да доминират в международното информационно пространство;

Засилване на действията, насочени към манипулиране на психологическото състояние на гражданите, и извършване на действия, които нарушават суверенитета, териториалната цялост и вътрешната стабилност на Руската федерация.

Изследването в тази част приключва с преглед на системите за национална и кибер сигурност на **Израел**, която е избрана поради множество специфики и съответни иновативни решения, които тази държава прилага в решаването на проблематиката в сферата на кибер сигурността.

Естеството на външните заплахи за Израел са разкрити в 4 основни категории:

А) Конвенционални заплахи от страна на държавни военни сили или недържавни организации, действащи като държавни военни сили.

Б) Неконвенционални заплахи, състоящи се главно от усилия за постигане на военен ядрен капацитет.

В) Субконвенционални заплахи, които включват партизанска война и тероризъм от участници както на територията на Израел, така и извън нея.

Г) Киберпространство и информационни заплахи.

Отчита се, че докато останалите държави по света се трансформират, за да посрещнат предизвикателствата на дигиталната ера, Израел сякаш изпреварва промените и успява да създаде модел на киберсигурност, който постига впечатляващи резултати. Добрите практики в сектора служат като пример за подражание, а чрез споделяне на знания и ноу-хау държавата се позиционира като основен източник на обучение за другите ключови играчи в сектора. Дори САЩ в ролята им на глобален лидер в областта на информационните технологии признават напредъка на Израел в киберсигурността. В този смисъл водещото място на израелския случай в изследването на киберсигурността и политиките в тази област е безспорно.

И ако доскоро учените се фокусираха предимно върху военния компонент в приложението на киберсигурността, то цялостната визия на Израел за политическата значимост на феномена киберпространството, тотално промени това. Последните научни трудове в областта, разглеждащи архетипни модели на киберсигурност, започнаха да изследват задълбочено тази проблематика. Независимо от важните им приноси, те се съсредоточиха главно върху организационните и историческите аспекти, което отчасти се дължи на факта, че концептуалният аспект на израелския подход стана публично достъпен едва наскоро, с публикуването на първата израелска национална стратегия за киберсигурност през 2017 г.

Отчита се като особено важно, че гарантирането на сигурността в киберпространството изисква усилия на национално равнище, които надхвърлят защитните кибернетични дейности и включват проактивни офанзивни действия - кибернетични и кинетични - от страна на органите на правоприлагането и националната сигурност срещу държавните и недържавните инициатори на атаката. Докато "стабилността" е отговорност единствено на организацията, като държавата играе стимулираща и подпомагаща роля, "устойчивостта" е съвместно начинание на организацията и държавата, "защитата" е в изключителните правомощия на държавата.

Политики за национална сигурност в България

В тази част на изследването се прави анализ на сектора сигурност у нас, като се разглежда цялостната законодателна и оперативна картина за политиките, ангажирани с осигуряването й. Направен е извода, че политиките за национална сигурност е необходимо да бъдат разглеждани не просто като отделни механично свързани компоненти, а да се разбират като взаимно допълващи се и неразривно свързани елементи на сложна система, чието ефективно функциониране се обуславя от синергичната работа на отделните звена.

Самото понятие се разглежда в дълбочина и се анализира обхвата и рамката му, далеч отвъд обичайното разбиране за националната сигурност в пост-индустриалните общества като сигурност на националните граници и опазването им чрез военна сила. Днес в условията на постоянно усложняващи се връзки между отделните сфери на живота през 21 век националната сигурност е далеч по-комплексна и е необходимо да се анализират множество фактори, които влияят върху формирането и ефективното и приложение. Заплахите вече са трудно предвидими и освен, че се разрастват по мащаб, увеличават своята сложност и комплексност, включващи предизвикателства от нетрадиционен, асиметричен или хибриден характер. Това изисква специфичен подход за противодействие и в този смисъл класическото разбиране за национална сигурност като „ние срещу другите“ вече очевидно не работи в новата среда.

Посочените фактори изискват нужда от радикално нов подход в самото разбиране и предефинирането на парадигмите, върху които се градят политиките за национална сигурност, като се акцентира върху създаването на модерни сили за сигурност и отбрана, притежаващи необходимите способности които да предложат адекватен отговор на възникнали предизвикателства от нов тип.

Разработката се фокусира както върху генезиса на проблема с киберпространството като потенциален вектор за информационна и физическа атака върху системата за сигурност на модерните държави, така и върху развитието на принципите, начините и средствата за осигуряване на безопасността в киберпространството като фундаментална част от политиките по национална сигурност в държавата ни.

Направеният цялостен анализ на база преглед на стратегическите документи в сектора, изследване на мерките по сигурността и функциите на органите, ангажирани с тяхното прилагане показва няколко основни проблема :

1. Технологиите по същество винаги ще изпреварват законотворческата дейност, ангажирана с тяхната регулация.

2. Усложняването на взаимовръзките в информационната среда и цялостната и еволюция винаги ще изисква по-високи разходи по осигуряване защитата на информационните активи, отколкото разходите за тяхното увреждане, кражба или злоупотреба.

3. Необходимо е и цялостно осъзнаване на фундаментално новия тип среда на сигурност и комплексността на това понятие в съвременния цифрово обезпечен свят, където динамиката на процесите освен че се интензифицира, се променя и качествено.

Комплексното разбиране за техническите аспекти на киберсигурността заедно с прозрения от хуманитарните науки по отношение взаимовръзките между виртуалния и физическия свят е от изключителна важност за националната сигурност, особено за тези държави, които са достатъчно развити в информационно-технологично отношение. Нарастващия брой киберинциденти, увеличаващата им се сложност и комплексност и спектър на въздействие са солидно доказателство за този аргумент. Следователно киберсигурността е ключов въпрос на националната сигурност, който трябва да бъде анализиран внимателно и задълбочено, като се изследват скрити взаимовръзки по отношение на влиянието на превръщащата се в паралелна реалност кибер среда за процесите във физически план на съвременния дигитално зависим социум.

С оглед идентифицирането на възможни аспекти за промяна, както и отделни конкретни мерки, които могат да бъдат имплементирани са направени съответно PEST и SWOT анализи, като резултатите от тях са представени таблично. Някои от изводите на база тази информация включват:

- Необходимост от създаване на специализирани структури за кибер отбрана, като основополагащ елемент от модерната армия
- Създаването на български технологични решения (хардуер/софтуер) в областта на информационната и кибер сигурност
- Приоритизиране на елемента „Устойчивост“ в кибер-аспекта на способностите за реакции при инциденти.
- Повишаване общата „киберхигиена“ на обществото
- Ютилизация на човешкия потенциал като ключов при изграждането на ефективна система за кибер сигурност.

Глава III – Лични данни и политики за национална сигурност

Тази глава е насочена към изследване същността на проблематика, касаеща сигурността и неприкосновеността на личните данни в информационното и киберпространството, като акцентира върху ограничеността на съществуващите парадигми по отношение на тяхната важност за множество процеси. Масовото разбиране е, че този елемент от общата сигурност касае една конкретна личност и нейните права да поддържа своята анонимност при работа с информационните ресурси на мрежата. Но в действителност ситуацията е далеч по-сложна и многопластова преди всичко поради повсеместното проникване на информационните технологии и тяхното пропиване в ежедневието ни до степен на пълната му зависимост от тях. В тази среда личните данни на един човек могат да бъдат използвани злонамерено, за да бъде причинена съзнателна вреда на друго лице, компания или дори да имат пряк ефект върху сигурността на ниво държава или над-държавно военно-политическо или икономическо обединение. Поради това модерните политики по кибер сигурност все по отчетливо се нуждаят от съществено преосмисляне както на значението на този фактор по отношение общата му тежест върху надеждността им, така и върху обхвата на действието на съществуващите правила и мерки, необходими за ефективното им осигуряване.

В тази част е направен преглед на водещите постижения в света по отношение изготвянето на нормативно-правната рамка, в която се дефинират личните данни и политиките за гарантиране на личната неприкосновеност. Разгледани са съществуващи политики в областта в развитите технологично държави, въз основа на което е изготвен обстоен анализ на ситуацията в страната. Изведени са основните предизвикателства пред развитието на адекватна правна форма, обслужваща нарасналите нужди от защита на личната информация и процесите по нейното съхраняване, трансфер, обработка и заличаване.

Нови тенденции и проблеми в областта на личните данни и сигурността

Тук основен акцент е поставен върху темата за събирането и нерегламентираното използване на личните данни на потребителите в киберпространството като фактор за въздействие върху персоналната, корпоративната или националната сигурност се радва на засилен интерес. Съвсем естествено тя се превърна в обект на задълбочени проучвания с оглед нарастващата им важност им за огромна част от населението на планетата. Особено след като през 2017 Facebook обяви, че компанията е предоставила материали на комисия в Конгреса на САЩ, разследваща евентуалната руска намеса в

президентските избори миналата година посредством използването на лични данни на ползващите социалната мрежа за разпространение на фалшиви новини. Макар че предизвика сериозно медийно внимание за съжаление този конкретен казус далеч не представлява единичен случай, а е само върха на айсберга наречен “privacy abuse” от страна на големите играчи в ИКТ сектора, тъй като порочните практики за нерегламентирано използване на личните данни на потребителите отдавна се ползват и от петте мастодонти в сектора – (GAFAM) , както и от множество производители на хардуер в това число HP, Lenovo, Huawei и др. И макар този аспект на злоупотреба с поверителна информация за клиенти да е сравнително нов като технологичен феномен по своята същност и ефект, подценяването му като фактор на въздействие към настоящия момент представлява реална опасност не просто на ниво отделен потребител, но и косвено за ефективното функциониране на системите за национална сигурност. Това е и основната причина изследователските усилия на настоящата разработка да бъдат насочени в тази конкретна тематика, която сякаш остава недостатъчно застъпена в голяма част от научните изследвания в сферата на информационната и киберсигурност.

Разкрива се, че злоупотребата с личните данни и поверителността на потребителската информация далеч не е приоритет само на големите доставчици на ИТ услуги или хардуерни решения. Огромна част от разузнавателните агенции по света (предимно в страните известни като „Петте Очи“), Китай, Русия, Израел и др.) са превърнали събирането на информация за потребителите във фундаментален елемент от своята оперативна дейност, като естествено съображенията за конфиденциалност и неприкосновеност на данните за индивидите са с минимална степен на приоритет и то само и доколкото е специфично ограничена от действащите в съответната страна регулативна рамка (в случаите когато такава изобщо съществува).

Не са пропуснати и различните представители на ъндърграунда в лицето на множество хакерски групировки или недобросъвестни самостоятелни единици, чиято основна дейност е насочена към търгуването на лични данни в интернет или Darknet на стотици хиляди, понякога дори и милиони потребители, извлечени от регистрите и базите данни на глобалните компании, чиито сървъри са успели да пробият.

Не на последно място интересът към настоящата тема е свързан и с процеса на постоянното нарастване на важността на личните данни чрез постепенното им превръщане в „стока“ (commodity), обект на засилена размяна с цел монетизиране на стойността им. Причини за възникването на този феномен могат да се търсят в лавинообразното развитие на информационните технологии през последния четвърт век

и съпътстващото ускорено натрупване на информация. С развитието на информационните технологии и постоянно нарастващия брой потребители в кибер-пространството ескалацията на проблеми и конфликти в информационната среда стана неизбежно. До голяма степен тази проблематика е продиктувана преди всичко от силно усложнената и взаимообвързана информационна среда, в която обитава съвременния жител на цифровите общества. В тези условия личните данни естествено еволюират до степен на ключов информационен актив, чиято важност все повече започва да се проявява по отношение въздействието и в чисто физически план.

Представено е разбирането, че реално всеки от нас се явява субект на личните данни, а нормативните рамки се създават с цел да обезпечават и защитават правата и свободите на гражданите при обработката на неговите лични данни. В това число правото на неприкосновеност на личния живот, личната и семейна тайна. С развитието на информационното пространство и комуникациите се появи остра необходимост от по – ефективно правно регулиране на проблематиката, свързана със защита на личната информация и правата на субектите, които я притежават.

Днес автоматизираната обработка на данните силно облекчава възможностите за получаване и използване на сведения за една личност, което от своя страна прави живота на хората буквално „прозрачен“, както за държавата като централен орган, така и за различни компании или криминални елементи. В този аспект и нормативно правната рамка, касаеща опазването на персоналните данни в глобалната информационна мрежа се развива интензивно през последните години, тъй като с основание предизвиква обществения интерес. Изхождайки от приоритета по защита на гражданите в цифровите общества, тя обезпечава относителен баланс между техните права и правата на други заинтересовани лица в сферата на информация за субектите.

За нуждите на настоящото изследване нека направим кратка съпоставка на проявленията на личните данни в двата им аспекта – физически и виртуален.

Във физически план най-често използваните идентификатори за даден човек включват обичайно повечето от следните компоненти:

- Имена на лицето Х
- Дата на раждане
- ЕГН
- Номер на идентификационен документ (издаден от МВР - ….)
- Местоживеене
- Ръст, цвят на очи, коса и тн

- Семейно положение
- Родители / деца

С оглед на развитието на информационните технологии във виртуалния свят горепосочените данни могат да се транспонират в следното:

- Име на потребител (алиас)
- Профилна снимка
- Номер на акаунт и дата на активация
- IP адрес, на който е регистриран + Гео-локация
- MAC адрес на устройството от което е извършена регистрацията
- Операционна система (среда), браузър,
- Пиъри – Контакти

С напредъка на технологиите и масовото им проникване в ежедневието ни съвсем естествено голяма част от тези данни ние предоставяме на доставчиците на различните видове услуги, които ползваме за работата си в глобалната мрежа. Всичко това разбира се генерира огромно количество информация, която трябва освен да бъде надлежно съхранена, да бъде подготвена за последваща обработка. Това се постига чрез сегментиране и клъстеризация на данните, които после се поднасят в подходящ вид за аналитичните алгоритми. За съжаление в повечето случаи обикновения потребител не си задава въпроса – как се съхраняват тези данни, кой има достъп до тях и за какво се използват. Защото със същите тези данни, които притежават за нас, доставчиците постоянно могат да следят за активността на потребителя съобразно зададени от него параметри – ползване на т.нар. бисквитки (cookies) както и следене на другите сайтове, които се посещават от неговия браузър. По този начин много лесно и бързо те са в състояние да монетизират притежаваните от тях данни за нас, като ние дори не сме в състояние да контролираме начина, по който тези данни се използват.

Лични данни като фактор за национална сигурност

Изследването акцентира върху този елемент като ключов за ПНС, поради цялостното неглижиране или неразбирането за неговата същност. В новата информационна епоха личните данни постепенно се превърнаха в особено ценен актив предвид цялостното обвързване на процесите в мрежата и физическата реалност. Стана възможно манипулацията на информацията в интернет директно да влияе върху реални активи и да създават проблеми от мащабен характер. Посочени са и конкретни примери в тази посока, като известния пробив на профила в Twitter на Associated Press от 2013 г,

когато там се появява следното съобщение: „Експлозии разтърсиха Белия дом, а президентът Барак Обама е ранен“. И макар че този туит е фалшив, пазарната реакция на информационно обвързаната икономика е съвсем реална. Съответно инвестиционният индексна Dow Jones в рамките на няколко минути се понижи драстично, а S&P 500 SPX загубиха 136.5 милиарда долара според пазарната си оценка. Хакерска група, наричаща себе си Сирийската електронна армия, по-късно потвърждава, че е била отговорна за това, след като е придобила данни на журналист от медията с достъп до акаунта на Associated Press в Twitter. Този пример е само един от многото през последното десетилетие, в които може да се види директната връзка между сигурността на личните данни на едно лице с корпоративната такава и да се проследи как точно пробиви в тяхното опазване могат да застрашат директно и националната сигурност на една държава.

Представен е преглед на някои от масивните кибератаки през последните години и пораженията от тях. Само през 2019 г. киберпрестъпниците са компрометирали данните на милиони потребители по света. Масово са извършвани пробиви в iOS на Apple, Visual Studio на Microsoft и други системи, които бяха считани за особено защитени. Лични данни на милиони притежатели на кредитни карти стават жертва на различни по своето естество фишинг, фарминг или рансомуер, чрез които постоянно се заразяват корпоративни, лични и институционални компютри по целия свят.

За съжаление, освен че честотата и интензивността на тези злонамерени нарушения нарастват с тревожни темпове, също така нараства и пропастта между свързана с работната сила, притежаваща необходимите знания и умения, за да се справи с тези сложни хакерски набези. Данни на CyberSeek[1] за 2019 година в САЩ показват, че от 715 000 работни места в сектора е налице реален недостиг от 314 000 обучени специалисти по киберсигурност, като това е 50-процентно увеличение спрямо данните от 2015 г. Така на практика киберпространството се превърна в поредната сфера, в която започнаха да се извършват и чисто военни действия – на същия принцип както преди години класическата война се водеше по суша, въздух и вода. Но кибер средата има едно основно предимство пред останалите – ако действията в един от другите три аспекта на войните са форма на взаимно допълващи се елементи за доминиране върху силите на противника, то днес киберпространството се явява форма на обединяващ слой за всеки един от предходните.

[1] Cyber Seek е проект на Националния институт за стандарти и технологии към (NIST) към U.S. Department of Commerce.

GDPR като отправна точка за стандартизиране опазването на личните данни в ЕС

Тази част от изследването е посветена на може би най-важният документ, приет в страните на ЕС, като един от най-значимите опити в досегашната ни история да бъде предложена достатъчно обхватна и ефективна правна рамка, която регламентира мерки за работа с личните данни на потребителите. Не случайно тя стана основание за страни извън евро зоната да ускорят процеса на адаптиране на техните законодателства с реалностите в новата цифрова епоха по отношение на личните данни. Въпреки че регламентът налага сериозна административна тежест за обработващите лични данни под формата на редица мерки, този документ до голяма степен се превърна в крайъгълен камък, върху който се изградиха в последствие политиките в сферата на личните данни и поверителността в света.

Разгледани са дефинициите, принципите и органите, които той определя, като се изследват основно аспектите, които имат отношение към сигурността и по-специално понятията: профилиране, неприкосновеност на личния живот, право на забравяне и др. Посочени са и редица проблеми, появили се при имплементацията на регламента в различните страни-членки, като са разгледани и възможните санкции за неизпълнение.

Представени са органите, ангажирани с обработката на данните, като са дефинирани и техните функции

- Администратор на лични данни (data controller)
- Обработващ лични данни (data processor)
- Длъжностно лице по защита на данните (data protection officer)

Като съществен елемент от въвеждането на Регламента в нормативното пространство на страните членки на Евросъюза е представено това, че с него също така се определят редица права върху данните на субектите - физическите лица, за които се отнасят личните данни, които се изпълняват от администраторите:

- Право на достъп до информацията
- Право на корекция
- Право на изтриване (или правото да бъдеш забравен)
- Право на ограничаване на обработването
- Право на преносимост на данните
- Право на възражение

Защита на личните данни извън страните на ЕС

С оглед изготвянето на качествен сравнителен анализ по отношение политиките и мерките за опазване личните данни тук е направен преглед на съществуващата правна рамка в някои от водещите в технологично отношение държави от различни континенти. Изследвани са подхода и начините, по които се адресира проблематиката с личните данни в отделните държави, като се използват съответно няколко ключови компонента за сравнение, а именно – дефиниране на понятията, принципите и ключовите елементи от системата за опазване на личните данни в информационното пространство. „Общото право“ като система от принципи и съдебна практика внимателно регламентира и охранява личните права и свободи, в това число и „правото да бъдеш оставен намира/насаме“. С оглед предоставяне на аналитична информация за нуждите на настоящото изследване са представени и легислативните уредби в другите водещите в информационно-технологични държави по отношение на законодателните рамки, регламентиращи работата с лични данни и неприкосновеността. Изследват се действащите нормативни документи в областта , преглеждат се основните дефиниции и накрая се отбелязват различните санкции.

Политики за сигурност на личните данни в България

Тук се акцентира върху изследване на ситуацията в страната, като се отбелязва, че по отношение на защита сигурността на личните данни у нас далеч не може да се говори за традиции в нашето законодателство, което беше буквално насила адаптирано към действащите правила в ЕС по отношение изискванията за тяхната сигурност и в последствие приемането на GDPR, които бяха вкарани едва ли не насила в действащата регулативна уредба.

Подобно твърдение може и да изглежда пресилено, но практиката показва, че все още голяма част от гражданите и представителите на малкия и среден бизнес не са особено склонни да отделят необходимия времеви, финансов и интелектуален ресурс за гарантиране сигурността на техните данни.

Действителното иницииране на фокусирани действия у нас обаче в посока създаване на нормативна база за регулация на личните данни започва в края на 90-те години с оглед необходимостта от привеждане законодателството ни в тази област в съответствие с достиженията на правото в ЕС съюз, като резултат от получената покана за присъединяване.

Възможности и предизвикателства пред имплементиране на технологични решения от типа на blockchain при защита на личните данни

Тази част от изследването се ангажира с търсене на алтернативни технологични решения на проблема със сигурността на личните данни, като акцентира на технологията "blockchain", което доби широка популярност дори сред не толкова грамотните технологично среди. Основното й предимство се проявява в няколко аспекта – отчетност и прозрачност за участниците, участващи в даден процес, като запазва поверителност и конфиденциалност. Наред с това тя е полезна за премахване на т.нар. „точките на триене", които винаги са съществували в традиционните бизнес процеси. blockchain бързо се превърна в дигитален гръбнак върху който се развиха криптовалутите, като се създадоха предпоставки да се имплементират принципите на осигуряване на процеса на търговията с виртуални пари в почти всички сфери, където има дигитални активи. Съответно тази тенденция може да се използва и при личните данни, които също могат да бъдат разглеждани като актив, който може да бъде притежаван, наеман и продаван по нови начини. В подкрепа на това твърдение са описани примерни blockchain проекти в контекста на личните данни и разпоредбите на GDPR, илюстриращи както възможностите, така и предизвикателства за прилагане на технологията в тази сфера.

Преди всичко обаче трябва да се има предвид, че Blockchain не е и не може да бъде решение на всички предизвикателства свързани с GDPR, но може да се разглежда като механизъм за подпомагане на контрола при използването на лични данни. Налице са определени възможности, които могат да се използват и моментът за действие в тази област изглежда назрял за първи стъпки.

Представени са няколко основни аспекта, където тази технология може да се приложи сравнително лесно, тъй като няма да изисква съществени инвестиционни ресурси за обезпечаване технологичния преход.

- Сигурност на обработката на личните данни
- Приложения на blockchain в одитиране и съхранение на логове

Направените изводи от изследването й са систематизирани, като не са пренебрегнати и съществуващите проблеми пред внедряването на подобни решения. Отчита се че тази нова технология добавя и важни елементи като отчетност, прозрачност за участниците във веригата, като същевременно запазва поверителността и конфиденциалността. И ако това е приложимо за проблемите, съществували в традиционните бизнес процеси, в контекста на спазване задълженията и условията на GDPR, се обобщава, че са налице както редица възможности, така и множество

предизвикателства за прилагане й. Направен е извода, че със сигурност технологията не може да се счита за решение на всички проблеми, но може да се разглежда като механизъм за подпомагане на контрола.

Заключение

В същността на представеното изследване стои дълбокото убеждение на автора, че светът навлиза в повратна точка от своята история на развитие в следствие на интензифициране взаимозависимостта на физическата реалност от процесите в информационното пространство. За хората от 21-ви век данните и интернет представляват това, което са били изкопаемите горива и петролопроводите за индустриалния век. И ако природните дадености са материални, ограничени и естествено не могат да бъдат възстановени след употреба, то с информацията е точно обратното. На практика този актив не само има потенциала да бъде, а постепенно се превръща във все по-ключово конкурентно предимство за една нация, като съответно от възможностите, с които тя разполага за опазването, ефективната обработка, съхранение и дистрибуция ще зависи в голяма степен качеството на нейното бъдеще.

На следващо място интензивното развитие на ИКТ и постепенното им проникване във всички аспекти на съвременния живот доведе до фундаментална промяна в същността на понятието „сигурност“ и неговите проявления в различни измерения. Една от характерните особености на тази промяна е свързана с нарастване възможността отделен индивид/група или единично явление да оказват силно влияние върху процеси, рефлектиращи върху голяма част от населението - не само локално, но и в географски региони, силно отдалечени от тях.

Това естествено приоритизира проблемите, свързани с пълноценно използване на информационните технологии в сферата на националната сигурност, като темата е обект на дискусия за множество представители на обществено-икономическия, научно-техническия и политически елит. Въпреки това някои аспекти от нея все още остават сравнително непознати в светлината на силно променената среда, в която функционират политиките за национална сигурност през 21-ви век. Пример за подобни пропуски е проблемът с неправомерното използване на личните данни на потребителите и използването им от алгоритмите на изкуствения интелект за анализ и управление на поведението и мотивацията им.

Като допълнителен резултат от изследването са направени и следните аргументирани изводи:

Способността на една държава да създава, обработва, дистрибутира и използва пълноценно и в максимална степен информационния ресурс ще дефинира в голяма част позиционирането и като сила в глобалния свят на 21-ви век. Респективно и ролята на конвенционалната армия за обезпечаване на националната сигурност – от основен фактор се превръща постепенно в поддържащ, като човешкият фактор в ролята му на полева бойна единица в пост-индустриалната армия от класически тип постепенно ще намалява докато се редуцира в кръга на минимално тактико-стратегически избор на дейности. За сметка на това е налице растяща необходимост от добре обучена, гъвкава и многофункционална кибер армия, която да е в състояние да противодейства на все по-интензивните атаки върху националната или корпоративна информационна структура.

Изтъкнати са доводи в подкрепа на тезата, че съвременните политики за киберсигурност трябва не просто да управляват технологичния елемент, свързан с обмяна на данните и нормалното функциониране на информационната мрежа, а до голяма степен да са ориентирани към работа с крайните потребители – реципиенти на технологиите, тъй като те се явяват ключов обект за гарантиране на информационната сигурност. Съответно нужна е адекватна политика, съобразена с често изменящите се външни и вътрешни условия на функциониране в сектора.

Разбирането на автора е, че в усилията към създаване на ефективни политики по национална сигурност в киберпространството на първо място е необходимо да бъде разпознато и прието наличието на проблем като първата стъпка към неговото потенциално решаване. В конкретния случай това е, че сигурността на личните данни и конфиденциалността на индивида в информационното пространство са проблем на националната сигурност.

Представените примери илюстрираха пряката корелация между пробива през лична информация и повишаване риска от различни по тип на заплахите, които могат да причинят сериозни пробиви в редица аспекти на сигурността на ниво компания, сектор от икономиката или на национално ниво. Така бе доказано, че реално управление на сигурността е невъзможно без да се вземат в предвид предизвикателства при опазването на лични данни и информационната сигурност.

На база това е очевидна необходимостта от повишаване на информираността и популяризиране важността на личните данни като ключов елемент от сигурността на ниво индивид, корпорация или държава в тази нова среда. За да се засили потенциала и капацитета на страната ни в тази област е необходимо на първо място да се работи върху

преди всичко върху промяна манталитета на потребителите в информационното пространство и разбирането за същността на процесите, които протичат там.

Като фундаментален проблем по отношение ефективността на политиките в сектора у нас е важно да бъде поставен въпросът, свързан с ясно дефиниране визията на България относно бъдещето на националната й сигурност. Необходимо е да бъдат разпознати и приоритизирани актуалните предизвикателства в съвременния дигитално обвързан и взаимнозависим глобализиран свят, за да могат да бъдат идентифицирани и анализирани и рисковете и заплахите пред страната ни в дългосрочен план. А те са функция на една динамична информационна среда, в която принципите на взаимосвързаност между отделните елементи в обществото са вече много по-комплексни и не винаги ясно разпознаваеми. Трендът на развитие е в посока от индивидуална независимост към взаимозависимост, като проявленията на този процес могат да се наблюдават както на микро, така и на глобално ниво.

Затова стратегически важно е да бъде отчетено българското разбиране към настоящия момент относно уязвимостта ни на фона на останалите държави в ЕС през призмата на нашето геополитическо положение, нарастващата глобална несигурност в политически план и катализирането на нов тип заплахи от киберпространството.

III. Справка за приносите в дисертационния труд

В съвременната наука, характеризираща се с наситеност на почти всички области на знанието с научни изследвания настоящата разработка няма амбицията да притежава фундаментално научна стойност по отношение откриване нови аспекти в създаването и имплементирането на политики по сигурността на личните данни. Тя е по-скоро опит за нов прочит и синтез на вече съществуващи теории и модели, касаещи управлението на процесите в сферата на сигурността в информационното пространство.

Като съществен в научен аспект **иновативен принос** на разработката може да бъде посочен нейният новаторски прочит по отношение на информационното пространство, като основен дефинитив за реалността в съвременния дигитално пристрастен социум, както и анализа на процесите по натрупването на огромна по своя обем и обхват информация относно потребителите и техните навици, създава предпоставки за моделиране на техния психологически профил и предсказване на действията им с висока степен на вероятност. От тук и направения извод, че

съвременните политики за сигурност на личните данни, трябва да се разглеждат като неделим елемент от национална сигурност през 21-ви век.

На следващо място като важен научен резултат от изследването може да бъде посочен и доказателствения елемент за обосновка на твърдението, че освен чисто технологичния аспект на понятия като безопасност, неприкосновеност и право на забравяне, които трябва да гарантират политиките за киберсигурност (вкл. и по отношение на личните данни), е изключително важно те да включват мерки насочени към осигуряване на „незамърсено“ от гледна точка на негативно влияние върху обществото информационно пространство. По този начин се минимизират възможностите за въздействие върху индивид, група или големи сегменти от населението чрез нововъзникващи инструменти за хибридно влияние като фалшиви новини, фишинг или скам кампании.

Предложеният систематичен подход в анализа на съществуващи съществуващите политики, обезпечаващи сигурността и неприкосновеността на личните данни, пречупени през призмата на ефекта им върху националната сигурност и свързаността й с процесите в киберпространството, също трябва да бъде отличена като един от съществените приноси в теоретизирането на този сравнително нов и недостатъчно изследван аспект на проблематиката.

Авторът отчита, че някои от теоретичните предложения може би звучат сравнително предизвикателно за неангажирания с темата читател, като например, че съвременните войни се водят преди всичко за умовете на хората (потребителите) или че в съвременните общества контролът върху населението в глобален план е изключително фин и сложен за дефиниране поради своето преплитане в почти всички пластове от живота на планетата.

Научната значимост на резултатите от изследването могат да бъдат търсени в приноса на разработката в развитието на научната представа за възможностите, които съществуват за използване на информацията като основен актив при формулиране на ефективни политики в сектора на сигурността. Чрез систематичен анализ се разкрива същността и механизма на управление на личните данни в информационното и киберпространство, явяващи се обект на политиките за национална сигурност. Всичко това има реални предпоставки да служи за база за по-нататъшни научни изследвания в областта и да подпомогне изследователските търсения в този сравнително нов и недостатъчно изследван домейн.

Като основен **практически принос** на изследването следва да бъде отбелязано предложението за имплементиране на политики по управление на личните данни, базирани на технологията blockchain в действащите системи на едно бъдещо електронното правителство. Работният вариант на предложението е базиран на проведено изследване на подобен тип решения в други страни, като е съобразен със спецификата на конкретната ситуация в България, както в икономико-технологичен аспект, така и в социално-културен и политически.

Практическото значението на работата може да се търси и в разкритите нови възможности за формирането на ефективни политики по национална сигурност, базирани на нов прочит и предефиниране на утвърденото разбиране за личните данни. Предложено е едно нетрадиционно разбиране за тяхната нарастваща роля в усложнената и взаимообвързана с реалността информационна среда, като се разкриват недостатъчно изследвани аспекти на взаимовръзката между личните данни с киберсигурността и националната сигурност.

IV. Публикации и участия, свързани с дисертационния труд

1. Управление на информацията в мрежовите общества или как се преначертава когнитивна карта публични политики. ISSN 1314-2313) година 5 / брой 1 / март 2014.
2. Възможности и заплахи пред сигурността на гражданите в цифровите общества, свързани с ефективното управление на информация при ускоряващо се технологично развитие – годишник на докторанта / 2017 г.
3. Технологична и информационна зависимост на хората през епохата на цифровите общества – доклад – Докторантски четения / септември 2017 г.
4. Участие в работната група, ангажирана с изготвяне на Националната стратегия за кибер сигурност от 2016 г - „Кибер устойчива България 2020”