Нов български университет

Магистърски факултет

Департамент „Национална и международна сигурност“

Проф. д-р Николай Стефанов Радулов

Технологични и цифрови трансформации в сигурността. Сигурност 4.0

АВТОРЕФЕРАТ

на дисертационен труд

за присъждане на научна степен „доктор на науките“

в програма „Стратегии и политики за сигурност“ в област на висшето образование 9. Сигурност и отбрана, професионално направление 9.1. Национална сигурност

София

2019

Дисертационният труд се състои от 379 страници.

Основен текст – 366 страници.

Брой на литературните източници – 107.

Брой на публикациите по дисертацията – 10.

Дисертантът е ръководител на департамент НМС в НБУ и докторант в департамент „Национална и международна сигурност“ при факултет „Магистърски“ на НБУ.

Изследванията по дисертационния труд за извършени в НБУ и Научно техническия съюз, България.

I. Обща характеристика на дисертационния труд

1. Обем и структура на труда

Дисертацията е в обем от 379 страници. В структурно отношение трудът се състои от девет части, включително увод, заключение, библиография и списък на ключовите думи. Направени са 213 бележки под линия. Списъкът на използваната литература включва 107 източника, от които 2 на български език, 1 на руски език, и 104 на английски език.

2. Актуалност на изследването

Разглежданата тема е свързана с въпроси, които са изключително актуални, поради взривното развитие на новите технологии, което довежда до тяхното повседневно и повсеместно използване. Четвъртата промишлена революция, която е в ход, поставя нови предизвикателства пред специалистите от сигурността. Необходимо е да се състави пълна картина, в резултат на изясняване на връзките между технологиите, използвани или с потенциал да бъдат използвани в системата за сигурност, и предизвиканите от тях изменения както в самата система, така и в отделните ѝ елементи (подструктури), а също така в целокупната екосистема на Сигурност 4.0. Различни технологии създават преимущества и проблеми в сигурността. Това е така, защото сигурността е комплексно понятие, тя е изградена от множество взаимосвързани и взаимозависими компоненти, така че където и да се използва необмислено или злоумишлено иновация, нова технология, то общият ефект може да е занижена, застрашена, недостатъчна сигурност.

Досега проблемите на високотехнологичните и цифрови и технологично трансформации в сигурността не са разгледани никъде по света. ***Това прави настоящото изследване не само жизнено необходимо, а изключително перспективен продукт със стратегическа насоченост.***

Обект и предмет на изследването

Обект на изследването е съвременната сигурност със своите предимства и недостатъци, но най-вече в перспективната светлина на високите технологии и цифровизацията. Този обект е изключително динамично развиващ се, но неговото поставяне в светлината на новите възможности ще позволи обезпечаване на ново ниво на сигурност и безопасност на живота.

Предмет на изследването са съвременното състояние и перспективи на имплементиране в сигурността на качествено нов инструментариум, който да я постави на нивото на изискванията на света, разгледан от позицията на Промишленост 4.0.

3. Цели и основни задачи на изследването

Тезата на дисертационния труд е, че ***само енергичното въвеждане на високотехнологични и цифрови инструменти и последващо преструктуриране на специалните служби може да обезпечи сигурността на хората във високотехнологичната среда на Промишленост 4.0.***

С оглед на горното, целта на изследването е да се идентифицират онези аспекти на високите технологии и дигитализация, които биха допринесли за постигане на достатъчна сигурност за хората в бързо развиващия се технологичен свят – ***да се създаде визия за високотехнологична сигурност***. За постигането на тази крайна цел дисертантът си поставя следните задачи:

1. Изследване на връзката между технологичната революция, следствие на Промишленост 4.0 и сигурността, дефиниране на понятието Сигурност 4.0;

2. Идентификация на новите технологии, които могат да бъдат използвани в сферата на сигурността;

3. Анализиране на заплахите за сигурността на гражданите и националната сигурност, като възможен резултат от използване от престъпните среди на най-нови технологични инструменти и приложения. Идентификация на актуални технологични престъпления;

4. Моделиране на съществуващи и бъдещи възможности за изграждане на екосистема за сигурност, отговаряща на съвременните предизвикателства.

С оглед на значителното изоставяне на специалните служби в страната в разглежданата област, сравнения, препоръки и добри практики ще бъдат използвани на примера на най-активните и високо развити специални служби в света.

4. Методология

Дисертационния труд изследва една особена и до момента не разглеждана комплексно специализирана тематика. При анализиране на проблемите на сигурността в светлината на съвременните, екстензивно развиващи се технологии, фокусът е насочен към приложението и ролята на технологиите в два полюсно разположени аспекта – престъпление – противодействие, като стремежът на работата е да очертае възможността за проактивно поведение на специалните служби. Използването на единични решения за генериране на комплексни възможности изисква използване на логическите методи, най-вече анализ, синтез и дедукция.

Широко приложение намира обаче и индуктивният метод, тъй като тук се цели да се постави темата за сигурността като се започне от отделния индивид и се премине към ефекта върху гражданската и националната сигурност в един постепенно разширяващ се кръг, подобно на окръжностите, образуващи се върху гладката водна повърхност след хвърляне на камък – от сигурността на собствения дом, квартал – към града, региона, държавата, международната общност.

Чрез анализ и използване на метода на сравнение и адаптация на най-добри съществуващи практики и разработвани перспективи, са изведени съществуващите в момента и подготвящи се за въвеждане технологични инструменти, позволяващи оптимизиране на дейността и висока ефективност.

Индуктивният и дедуктивният метод, анализът, сравнителния анализ, анализът на анализа и синтезът се използват във всички части на изследването и те спомагат за индивидуализиране на проблемите и в същото време за извеждане на обобщенията и заключенията. Дисертационният труд залага в значителна степен на синтеза, като е представено разгърнато собствено виждане по всички основни въпроси на въвеждането на високотехнологичен инструментариум за създаване на съвременна екосистема на сигурността.

При представяне на проблематиката е използван и историческият метод, без да се изпада в обширна разказна форма и само там, където това е счетено за необходимо за поставяне на проблематиката в перспектива и да се демонстрира необходимата и неизбежна връзка между минало и настояще от Първата промишлена революция до Промишленост 4.0, за да се гарантира авторитетност на авторските заключения. Предвид нуждата процесите да бъдат изследвани в тяхното развитие през по-продължителен период от време, този метод намира ограничено приложение в началото на работата.

Като във всяко изследване от подобен род, е използван системният подход. Системният метод дава възможност да се изследва проблематиката във високите технологии, всеобщата цифровизация, всеобщата свързаност и въздействието им върху сигурността като единна система със съответните взаимовръзки между отделните компоненти.

Структурата е характерна за дисертационни изследвания. Това е така, от една страна, поради споменатия вече интердисциплинарен

характер на разглежданата тема – сигурност-високи технологии-цифровизация а, от друга страна – и поради целта, която си поставя дисертацията. Целта, както е отбелязано по-горе, е да създаде стратегическа база за високотехнологична сигурност от гледна точка на науката за сигурността. Това не изключва задълбочен анализ на локални добри практики, с който изобилства трудът. Напротив, изисква се такъв анализ, който да потвърди тезата за многото и значими предизвикателства пред високотехнологичния инструментариум в сигурността. Тези предизвикателства са толкова значими, че разрешаването им може да се постигне само с проектиране и изграждане на нов технологично-цифров и хуманен модел за сигурност. А щом тези предизвикателства са толкова значими, че водят до дълбоки изменения в самата структура на сигурността, то няма как да не касаят специалните служби и тяхното прогресивно преконструиране.

5. Приноси

Анализът по темата за вграждане на съвременните технологии и цифровизиране на сигурността е принос за България, а бих казал и в световен мащаб, доколкото изследванията ми показаха, че не е изработен подобен визионерски продукт за момента никъде по света. Съществуват отделни елементи разглеждани самостоятелно и в ограничението на индивидуални подходи за приложение. Сигурност 4.0, екосистема на сигурността, екосистемите на отделните приложения за противодействие на престъпността за пръв път се разглеждат комплексно в труда, а са дефинирани за пръв път от автора в отделни статии в рамките на последните две години.

Анализът на възможностите на новите технологии за генериране на нов тип престъпност е разглеждан в отделни материали, но никога досега в **единен труд, постигащ сравнителна комплексност и синергичност**. Разглеждането на цифровите престъпления до момента не е стигнало по-

далече от киберпрестъпленията, което силно стеснява възможното обмисляне и дискутиране на проблема от гледната точка на един безкрайно цифровизиран свят – свят на големите данни, интернет на всичко и виртуална реалност.

В по-широк план разглеждането на темата за сигурността през призмата на високотехнологичния свят и цифровото битие, но в един **комплексен аспект и по отношение на теорията на разузнаване, контраразузнаване и сигурност, е креативен и неизползван подход**. Тя развива редица проблеми, само загатнати в редица статии по частни въпроси на технологиите в сигурността, включително и мои.

Конкретен приносен елемент в изследването са дефинирането на понятията **Сигурност 4.0, Екосистема на сигурността**, както и техния структурен и смислов анализ.

Конкретен приносен елемент е също така **създаването и описването на модели за използване на съвременните технологии в теорията и практиката на сигурността, както и създаване на идейни модели за нови възможности за приложение и нови продукти в сигурността**.

6. Практическо значение на изследването

Както посочих по-горе, тезата на дисертационния труд е, че ***само енергичното въвеждане на високотехнологични и цифрови инструменти и последващо преструктуриране на специалните служби може да обезпечи сигурността на хората във високотехнологичната среда на Промишленост 4.0.*** Трудът доказва, че оптимално и съвременно развитие на специалните служби и достигане на качествена гражданска и национална сигурност е възможна само чрез енергичното въвеждане на високотехнологични и цифрови инструменти.

Дисертационният труд утвърждава, че моментът за такива промени е подходящ. Не само това, видно от изложената материя е, че във най-

развитите държави, службите за сигурност и обществен ред вече правят първите крачки по този път.

В момента развитието на българските специални служби е в стагнация и то в чисто организационен и ценностен план. Въобще не става и дума за коренна технологична промяна, за която светът е узрял, а гражданите се потърпевши дори от липсата на нейни наченки. За съжаление, макар и малко по-добро, но в не достатъчен план и обхват е състоянието на европейските специални служби. Далеч сме от достиженията на високотехнологичните организации за разузнаване и контраразузнаване на САЩ и Русия. Като че в малко по-добро състояние изглеждат френските специални служби и полиция, но и там засега не е демонстрирана обща концепция и реализация.

Липсва знание, кураж и най-вече визия за бъдещо развитие. Ако проследим правната и теоретична тематика в сферата на сигурността през последните години, ще видим стагнация, липса на идеи, безразличие и неразбиране на съвременното място на специалните служби.

От тази гледна точка настоящата работа дава рецепти за излизане от статуквото. Дава визия, възможни високотехнологични конструкции, адаптира и кооптира в единна система съществуващи разработки, действащи приложения и идейни проекти.

Ограничения

Ограниченията на анализа са свързани в най-висока степен с необятността на създаваните високотехнологични решения, разбираемото изоставане на изследването на приложението на технологични и цифрови инструменти в сигурността от тяхното скокообразно развитие. Във времето на изработване на настоящия труд към обема от големи данни са добавени стотици зетабайта ново съдържание, а процесорната мощ на компютрите се е удесеторила. Поради това стремежът на автора е да обхване процесите

в дълбочина и по принцип, като дава частни примери само за по-добро разбиране и илюстрация на тезите си.

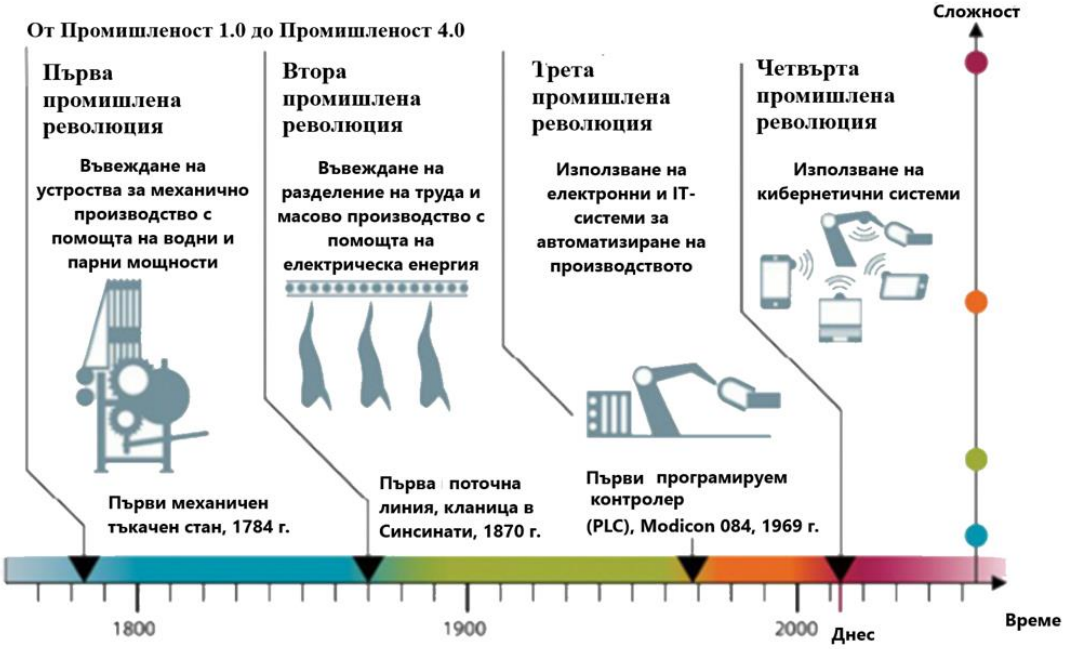
II. Основно съдържание на дисертационния труд

Въведение

Въведението има за цел да постави рамката на дисертационния труд. В него са обосновани актуалността, предметът и обектът на изследването, целите и задачите на работата, приложената методология. От поставените в него рамки логически следват следните няколко глави:

1. Глава първа. Промишлените революции

През последните 250 години са настъпили три индустриални революции (Фиг. 1). Те са променили процеса на изграждане и възприемане на ценности и света като цяло. По време на всяка от тях се развиват технологиите, политическите системи и социалните институции. Променя се производството, възгледите на хората за себе си, връзката помежду им и околната среда.



Фигура 1. Промишлените революции във времето (по DFKI, 2011 г.)

Развитието на системите за обществен ред и сигурност несъмнено следва развитието на икономиката и социалните отношения. Разработката на технологиите често се случва първо във военните организации и тези на сигурността, а впоследствие те се появяват и като продукти за цивилно ползване. Паралелно въздействие се отбелязва в развитието на криминалната среда. Престъпността е насочена към незаконно придобиване на блага от организирани и неорганизирани криминални групи.

На всеки етап от промишленото развитие съответства етап от развитие на системата за сигурност. Затова, когато размишляваме за сигурността в потока от идеи за Промишленост 4.0 – то имаме предвид иновативни парадигми, технологии и техники за обезпечаване на сигурност, съответстващи на високите технологии, които следва да обединим под общото название Сигурност 4.0.

2. Глава втора. Четвъртата промишлена революция и сигурността. Сигурност и несигурност

Авторът анализира и синтезира в единна система идеите на технологиите на Четвъртата промишлена революция мащабно, извън контекста на прост инструментариум, в тясна връзка и взаимозависимост, в светлината на идеята за синергичност, като търси възможностите, които от една страна да позволят на службите за сигурност и обществен ред да въздействат положително на качеството и нивото на националната и гражданска сигурност, а от друга – да се извличат и приоритетно развиват тези технологии и комбинации от тях, които да гарантират на хората, че секторът за сигурност работи само и единствено в тяхна полза и защита. Технологиите трябва да бъдат анализирани и от гледна точка на възможностите за тяхното използване от престъпниците, за да се създаде коцептуална среда за противодействие.

На базата на казаното до тук авторът прави няколко конкретни прогнози:

Кризисните явления в икономиката, сложността на навлизане в новата промишлена революция увеличават напрежението на пазара на труда, в междунационалните отношения, в мигрантската среда. Това влияе негативно върху сигурността, като нарастват както традиционните, така и нетрадиционните видове престъпления. Правозащитните органи в условията на дефицит на финансови средства за тяхното съществуване ще се налага да водят борба с две направления – традиционната и нетрадиционна престъпност. При това и сега е ясно, че правоохранителната система ще закъснява постоянно в действията си по противодействие на технологизацията на престъпния свят. Известно е, че загубилият инициативата в борбата, най-вероятно ще инкасира и крайната загуба.

При разкриването на престъпления трябва съвършено да бъде изменена системата на използване на нови технически средства за получаване на обективна информация за виновността на едно или друго заподозряно лице.

Нужно е да се премахнат архаичните, пещерни способи за разследване на криминални дела, изписването и прочитането на стотици томове от тези дела, без машинна обработка, особено по дела с икономическа насоченост и организирана престъпна дейност. Раздутата администрация може успешно да бъда заменена в повечето случаи от гъвкави компютърни системи, стъпващи на изкуствен интелект.

Необходима е революция в експертната дейност. Още сега се налага най-новите открития по редица направления в науката да се използват в тази сфера, която традиционно определяме като криминалистическа експертиза.

Скоро може да се окажем в ситуация, когато престъпниците ще използват квантови изчисления, а ние постарому ще продължаваме да перфорираме листа и да прошнуроваме папките на криминалните дела.

Включвайки нови и нови устройства, хората забравят, че всичко достъпно през мрежата може да бъде обект на взлом, рано или късно. Никакви съществуващи технологии и агентства за сигурност не са достатъчни за противопоставяне на растящата заплаха. Интернет се развива в пъти по-бързо от средствата за защитата му.

Необходимо е инициирането на нов проект, който да обедини усилията на най-добрите учени и изследователи, университети, правителствени и неправителствени организации, корпорации, гражданското общество. Трябва да бъдат привлечени предприемачи, политици, юристи, военни, анализатори – с цел създаване на пълноценна, всеобхватна защита, включваща по-безопасно оборудване, операционни системи и програмно обезпечаване като минимум на общодържавно, а още по-добре на глобално ниво.

За да изведе тенденциите в необходимото развитие на сигурността в „Промишлена революция 4.0“, авторът стъпва на стоящите пред нея задачи:

- Необходимост от справедливо разпределение на благата на Четвъртата промишлена революция;
- Контрол над негативните последствия и рискове от Четвъртата промишлена революция;
- Гарантиране, че Четвъртата промишлена революция ще се развива в интерес на хората и под човешки контрол;

От извършения анализ и предстоящите задачи авторът формулира четири принципа, които са изключително важни за формиране на адекватен начин на мислене в сигурността:

- Важно е не само да се разглеждат и внедряват технологиите в сферата на сигурността, но да се интегрират в система, водеща до синергичен ефект.
- Технологиите трябва да разширяват възможностите за противодействие на престъпността, а не да ги ограничават.
- Използване по замисъл, а не по мълчаливо подразбиране. Системното мислене трябва непрекъснато да анализира структурите и системите, обезпечаващи сигурност, и да определи подходи за това, как новите технологии могат да осъществят промени, водещи до повишен положителен ефект за хората;
- Ценностите трябва да се разглеждат като достойнство, а не като недостатък. Ценностите в сферата на сигурността, обусловени от технологиите, трябва да подлежат на устойчив смисъл и съдържание, но да са гъвкави по същество, за да могат динамично да се променят, без да изгубят заряда и достойнствата си.

Тези четири принципа съставят база за оценка, обсъждане и контрол на технологиите, които вече ни въздействат днес и ще променят света в бъдеще. Четвъртата промишлена революция може да роди системи, способни да направят обществото много по-благополучно, да увеличат продължителността на живота, да повишат нивото на сигурността в нейното широко и тясно разбиране, да разкрият нови възможности за съществуване и развитие. Налице е една спирала на технологично и техническо развитие, стимулирана или възпрепятствана от наличната среда на сигурност.

Следователно трябва да бъдат изведени няколко задължения при управление на сигурността – гражданска и национална:

- Идентифициране на ценностите, гарантиращи защита и сигурност, свързани с определени високи технологии;

- Изясняване как новите технологии влияят на вземаните от хората решения. Как новите технологии използвани от престъпниците влияят на вземането на решения, свързани с увеличаване на криминалната престъпност. Как новите технологии влияят на вземаните решения в сигурността и довеждат до ефективно противодействие на престъпността.
- Определяне на най-ефективните пътища на влияние на технологическото развитие с оглед на целите и интересите на службите за сигурност и обществен ред, подчинени на гарантиране на националната и гражданска сигурност.

В тази връзка авторът дефинира някои невралгични точки, даващи възможност за изучаване, анализ и влияние на ценностите, внедрявани в технологиите, гарантиращи сигурност:

- Създаване на образователни програми в сферата на сигурността;
- Финансиране и инвестиции в задължителни и неизбежни ресурси за сигурност;
- Изграждане на организационна и технологична култура в сигурността;
- Приоритетите се ранжират съобразно нуждите на сигурността, ресурсите, технологичните възможности;
- Нужно е създаване и ползване на операционни методологии за постигане на нужно ниво на сигурност;
- Не може да се реагира адекватно и ефективно без икономически поощрения за доказани достижения;
- Проектиране на високо технологични продукти в сигурността;
- Създаване и поддържане на ефективна и модерна техническа архитектура;
- Преодоляване съпротивлението на обществото;

- Обхващане на всички заинтересовани от националната и гражданска сигурност страни;

За да е в състояние „Промишлена революция 4.0“ да обезпечи процъфтяване, откритост и равенство за обществото и гражданите, е необходим съзнателен избор на технологични системи, които неизбежно ще оказват влияние върху сигурността. Това означава, че е необходимо наличие на съвременни парадигми и тяхното преформатиране, за да се постигне включване на всички заинтересовани участници.

В главата авторът обосновано дефинира ново понятие: **Екосистемата на Сигурност 4.0 представлява единство на хора, организации, високотехнологични елементи и среда, създаващи, обезпечаващи и защитаващи националната и гражданска сигурност.**

Назрялата необходимост от цифрова трансформация на системата за сигурност предполага комплексна иформатизация на процесите на управление на сигурността на основата на създаване и консолидиране на национални и европейски изчислителни и информационни ресурси, като:

- Да се обмисли и задейства разработване и внедряване на прилежащи общоевропейски, национали, регионални и общински цифрови платформи за обезпечаване на сигурност;
- Да се извърши постепенно редуциране на общото количество автоматизирани системи в сигурността на базата на прехвърляне на функциите им към интегрирани системи и формиране на единна национална цифрова екосистема за сигурност, като още на етап планиране да се предвиди последващо интегриране с европейската система.
- Да се обмисли и стартира изграждане на типови национални, регионални и общински платформи за сигурност, което ще улесни създаването на единна екосистема за сигурност. Необходима е

разработка на типови сценарии, протоколи, прогнозни и противодействащи модели.

Авторът определя и разглежда основните елементи, характеризиращи Екосистемата на Сигурност 4.0: 1. Високотехнологична среда; 2. Високотехнологични съвременни служби за обществен ред и сигурност; 3. Противник, разполагащ с възможности за технологично въздействие.

Класическото изискване за успешно противодействие на престъпността и контрашпионажа е структурите, които го извършват, да действат проактивно – загубата на инициатива е равна на проваляне на противодействието. Следователно изпреварващо реконструиране на специалните служби съобразно новите технологии е задължително за успешно обезпечаване на национална и гражданска сигурност.

И трите елемента на екосистемата Сигурност 4.0 са разгледани и изследвани в следващото изложение по отношение на наличието и прилагането на определящи, характерни и типични за Индустрия 4.0 технологични концепции като: Големите данни; Интернет на нещата; Блокчейн технологиите; Адитивните технологии; Виртуална, смесена и допълнена реалност.

3. Глава трета. Среда в екосистемата на Сигурност 4.0

3.1. Технологии и сигурност, възможности и промени

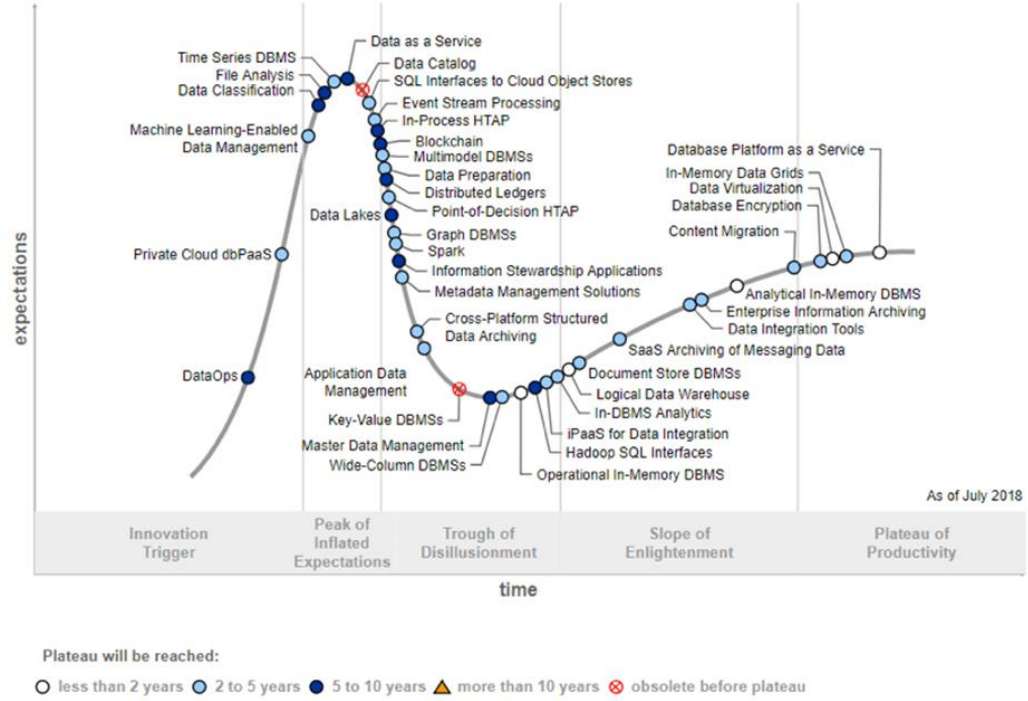
В тази глава средата е разгледана във фокуса на новите технологии, доколкото това позволява достатъчно коректно разглеждане на екосистемата на Сигурност 4.0. Разбира се, от значение са и останалите съставки на средата като социална, правна, демографска, екологична и др., но това ще доведе до ненужно усложняване и утежняване на материала, така че това е съзнателно възприето ограничение от страна на автора.

Обект на анализ в главата са новите изчислителни технологии в сигурността.

3.2. Големите данни (Фиг. 2)

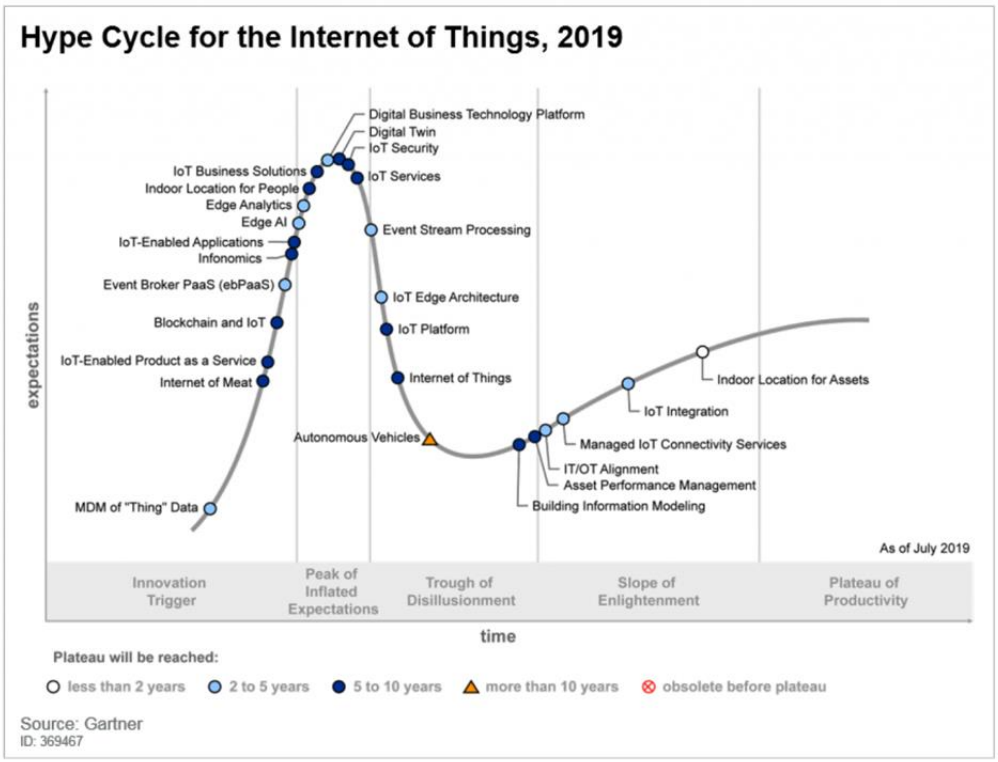
Извършен е анализ на техниките и методите на обработка и анализ на Големите данни като: Дълбочинен анализ (Data Mining); Краудсорсинг; A/B-тестване; Прогнозен анализ; Машинно обучение – изкуствен интелект; Мрежови анализ.

Анализирана е ползата от анализа на големите данни в сигурността, както и някои перспективни възможности за прилагане.



Фигура 2. Тенденция в развитието на технологиите на Големите данни. Източник: https://agileengine.com/megatrends-in-big-data/

3.3. Интернет на нещата (Фиг. 3)



Фигура 3. Тенденции в развитието на екосистемата на Интернет на нещата

IoT може да служи като инструмент за решаване на системни проблеми като ефективно използване на енергия, управление на трафика по пътищата и повишаване сигурността на придвижване – намаляване на катастрофите, замърсяването на околната среда. Фактически това е инструмент за достигане на сигурност било в широкия, било в тесния смисъл на термина – от сигурност на инфраструктурата, екологична сигурност, енергийна сигурност – до гражданска и национална сигурност.

Военен интернет на нещата (Internet of Battle Things – IoBT) Военният интернет на нещата става логично продължение на концепцията за мрежова ориентирана война, която стана популярна в началото на века, и концепцията за битката с множество домейни, т. е. борба чрез операциите в различни сфери: на сушата, морето, въздуха, пространството, киберпространството и електромагнитния спектър.

3.4. Блокчейн и технологиите на разпределен регистър

Технологията на блокчейна е основана на използването на разпределения цифров регистър, позволяващ безопасно да се обменят цифрови записи и да се гарантира съществуването само на един уникален запис без копия, като по този начин се запазва ценността на цифровия обект или информация. Тази технология довежда до изключителна сигурност на трансфера на информация и ценности, така че опосредствано влияе върху цялостната система за международна, национална и гражданска сигурност, предотвратявайки изкривяването и злоупотребата с информация.

В сигурността ресурсните възможности на специалните служби в различните държави са твърде различни – от огромни вложения от стотици милиарди, до санитарния минимум на десетина милиона. Иновативната същност на технологията в сигурността обаче трябва да бъде разбрана, адаптирана и превърната в предимство, разбира се, ако има политическо желание за това.

3.5. Изкуствен интелект

Изкуственият интелект вече преустройва цифровата икономика и скоро въобще ще промени икономиката на материалния свят. В началото на XXI век ИИ помага на автономните механизми да се ориентират в материалния свят и да взаимодействат с хората. В бъдеще системите с изкуствен интелект ще могат да решават комплексни системни задачи. На практика и днес, ако полицията разполага с качествени компютърни системи с интегриран ИИ, голяма част от рутинната канцеларска работа може да бъде извършвана от тях, което да доведе до разкриване на нови резерви за повишаване на полицейско присъствие в градските зони. ИИ вече обезпечава мониторинга на видеопотоци и данни, събрани от огромно количество датчици, и може да предупреждава службите за сигурност за подозрителна активност. Същевременно полицията използва роботи за

провеждане на издирвателно-спасителни операции, за обезвреждане на взривни устройства при терористична дейност и дори за унищожаване на въоръжени престъпници.

3.6. Адитивно производство и многомерно печатане

Тенденцията на ръста на 3D-печатането (Фиг. 4) показва, че то е в състояние да измени радикално цялата система на производство, включително промишлените, оръжейните, транспортните, логистичните, инфраструктурните, строителните, авиокосмическите, корабостроителните и др. компании и да окаже огромно въздействие върху правителствата, икономиките, пазара на труда както на развиващите се, така и на развитите страни. От това следва, че въздействието върху сигурността в общ и тесен смисъл също ще бъде огромно. На практика това значи масово производство по поръчка – от модни вещи до оръжие и напечатани човешки органи.

Фигура 4. Тенденция в развитието на 3D-печатането (https://www.3dnatives.com/en/gartner-hype-cycle-3dprintingpredictions-150120194/)

3.7. Виртуална и допълнена реалност

В сферата на сигурността могат да се прилагат за моделиране, интерактивно управление на силите и средствата, обучение, управление на

бази данни и системи за информация и анализ, визуализиране на платформи за разузнаване и контраразузнаване и др.

3.8. Дронове

Дроновете намаляват цената на разузнавателните операции, заменяйки пилотираните самолети, които струват 10-15 пъти по-скъпо. Използването им съкращава времето, необходимо за подготовка на личния състав и минимизира загубите, премахвайки опасността за управляващия машината.

3.9. Сигурност и биотехнологии

Биотехнологиите имат три важни отличия от цифровите технологии на „Промишленост 4.0“. Те предизвикват по-емоционална реакция на обществото, явяват се по-малко предсказуеми заради органичната си същност, а също така изискват повече капиталовложения и регулиране, поради което инвестиционният хоризонт е удължен. Освен това приемливостта и използването на различните биотехнологии зависят от дълбоките културно-исторически особености, които определя допустимостта на научните изисквания.

3.10. Невротехнологии

Понятието „невротехнологии“ включва широк набор от методики, позволяващи дълбоко проникване в механизма на работа на човешкия мозък и извличане на информация, разширяване на възможностите на сетивата, изменяне на човешкото поведение и взаимодействието със света.

3.11. Нови (умни) материали

Новите материали обикновено представляват стратегически суровини и ресурси и като такива се ползват от всички защитни мерки, които държавата прилага за запазване на монопола на производство и ползване. От друга страна, в сферата на сигурността новите материали се използват за защита, комуникации, маскировка, мониторинг.

3.12. Енергия и сигурност. Нови енергийни източници

Анализирани са възможностите за ползване на иновативни енергийни източници и тяхната връзка със сигурността. Подчертана е важността на енергийната независимост за сигурността.

3.13. Геоинжинеринг

Идеята на геоинжинеринга се състои в целенасочено ефективно управление на изключително сложната биосфера на Земята. Много учени обаче смятат, че технологиите, предназначени за намеса в тази област в най-добрия случай са незрели, а в най-лошия – носят заплаха за съществуването на човечеството и могат да доведат до непредсказуеми и неконтролируеми последствия.

3.14. Космически технологии

Специалните служби и военните използват възможностите на космическите технологии за наблюдение на повърхността, събиране на информация за противника, за трафика на военна техника, трафика на наркотици, трафика на хора. Големите престъпни организации не изостават от тях – има информация, че наемат сегменти от космически апарати за комуникация и контранаблюдение. Космическите технологии изискват средства, а както казахме по-горе, организираната престъпност разполага с достатъчно ликвидни средства.

4. Глава четвърта. Сили, средства и методи

Главата разглежда теоретичните постановки и практиката на подбор на служителите, изучаване и подготовка, работата със секретните сътрудници и специалните разузнавателни средства, както и методите на дейност и действие, характерни за специалните служби в светлината на иновативните технологии, анализирани в предната глава. Отделя се внимание и на възможностите на техническото разузнаване при използване на високотехнологични устройства.

Дефинира се нова парадигма в службите за сигурност, възникнала като следствие на новите технологии. темпорална разузнавателна

информация. Тя не е тясна методология за събиране на конкретни разузнавателни данни, която се фокусира върху определени източници, а цялостен подход за събиране и анализ на данни глобално и тотално. Тя предполага, че повечето хора и инфраструктури ще бъдат наблюдавани и че някои от данните могат да бъдат събирани, анализирани и съхранявани, генерирани за разузнаване и създадени нови. Крайната времева разузнавателна платформа на това, което се случва навсякъде, разбира се ограничена за конкретно, събитие, място и интерес, позволява събитието по желание да може да се мащабира, стопира, превърта назад (подобно на видео) – с пълен коментар за състоянието на физическото и психическото здраве на всеки човек или структура, подробности за които са получени с помощта на преносими устройства или гигантски вече количества интелигентни датчици.

В главата се прави кратък анализ на съществуващия инструментариум за работа с големи данни, активно използващ се от съвременните специални служби. Тези инструменти могат да се използват както в оригиналния си вид, така и като специализирани, целево променени разновидности за практикуване на специфична разузнавателна и аналитична дейност. Нека ги споменем за демонстрация на съществуващите възможности:

Бази данни: *Apache Hive, DRIL, Impala, Presto.*

Платформи Фреймуърк: *Hadoop, Spark, Storm.*

Аналитични платформи: *Deductor, Dell EMC Analytic Insights Module, Flume, IBM SPSS Modeler, IBM Watson Analitics, Informatica, KNIME, Microsoft Azure Machine Learning, Oracle Big Data Preparation, Pentaho Data Integration, Qlik Analytics Platform, RapidMiner, SAP BusinessObjects PredictiveAnalytics, SAS Enterprise Miner, Statistica, Teradata Aster Analytics, Windows Azure HDInsight, World Programing System, Zookeep*

Това кратко изложение има за цел да покаже, че е наличен разнообразен инструментариум за работа с ГД, позволяващ на аналитиците в специалните служби да го използват с лекота. Голяма част от инструментите са с отворен код, което позволява допълнителна разработка и ползване за специални цели в средата и насочеността на съответната специална служба.

От описанието и анализа до тук, макар и в сравнително лаконичен формат (поради невъзможността да се направи пространно изложение, анализ и описание на изключително широкия кръг от проблеми и възможности на високите технологии), можем да се уверим в трайното участие и заинтересованост на специалните служби в изучаването, внедряването и употребата на високотехнологични решения. Нещо повече – може да се счита, че ускореното внедряване и развитие на съвременни технологии от високо ниво е от жизнено значение за сигурността – гражданска, корпоративна, национална.

В края на главата авторът прави кратък анализ на управленския цикъл в сигурността в светлината на високите технологии, като задължителен елемент от екосистемата на сигурността.

5. Глава пета. Престъпност и високи технологии

Тази глава е насочена към действията на противника, с което се завършва пълното изследване на Екосистемата на Сигурност 4.0.

Нарастващ брой проучвания заключават, че появата на Интернет преобразява организационния живот на престъпността. С много статии и доклади, описващи различни видове организационни структури, участващи в киберпрестъпленията, като „организирана престъпност“ става ясно, че се създава една нова престъпна екосфера. В рамките на последните пет години светът на киберпрестъпността достигна индустриални размери. Хакерите, програмистите, социалните инженери и паричните мулета поддържат работен бизнес режим и често прилагат

съвременни техники за насочване срещу компании и лица. През последните няколко години паралел между характеризирането на организираната престъпност като сериозна заплаха за националната сигурност и развиващата се характеристика на киберпрестъпността като тежко престъпление – следователно организирано „по подразбиране“, задейства секюритизацията на киберпрестъпността, с важни последици за правомощията и подходите на полицията и разпределението на ресурсите.

Авторът определя и класифицира противника в рамките на използваните подходи и организация на дейност – от организирани престъпни групи до индивидуалисти, от чужди специални служби до хакери наемници. Анализира съвременните престъпления в светлината на високотехнологичните направления, изучавани и разглеждани по-горе.

6. Заключение

Трябва да се отбележи, че липсата на визия в службите за сигурност води до дефицит на креативност, на лошо управление, на слаби резултати. Специалните служби не са самодостатъчни организации, а имат благородната цел да постигнат ефективно противодействие на престъпността и да обезпечат спокоен живот и дейност на гражданите.

Представеното изложение на работата в автореферата показва, че предварително поставените цели и задачи са постигнати и работата притежава голям личен заряд – научен и визионерски пробив в стика между науките за сигурност и науките, отнасящи се до всеки един от основните елементи на Промишленост 4.0 и Сигурност 4.0.

III. Научни публикации по темата

1. Радулов, Н., Сигурност 4.0. Сигурността и четвъртата промишлена революция, В: Сб. докл. от Годишна Университетска научна конференция, В. Търново, изд. НВУ, ISSN 2367-7465, 2018, 9-34

2. Радулов, Н., Виртуална реалност и сигурност. Сигурност 4.0, В: Сб. докл. от Годишна Университетска научна конференция, В. Търново, изд. НВУ, ISSN 1314-1937, 2019, т. 4, 86-93

3. Радулов, Н., Проследяване. Сигурност 4.0, В: Сб. научни трудове, НБУ, ISBN 978-619-7383-13-3, 2019, т. 1, 8-14
4. Радулов, Н., Съвременни корелации в сигурността, В: Technics, technology, education, safety, Изд. НТС, ISSN 1310-3946, бр. 10, т. 3, 2016, 28-30
5. Radulov, N., Security today. Current issues, In: CONFSEC, International scientific conference, Dec, 2017, Ed. STUME, ISSN 2603-2945, year 1, issue 1, 37-39
6. Radulov, N., Internet of the things. Security 4.0, In: CONFSEC, International scientific conference, Dec, 2017, Ed. STUME, ISSN 2603-2945, year 2, issue 1(3), 2018, 5-7
7. Radulov, N., Artificial Intelligence and security, In: Security & Future, Int. Sci. J., Ed. STUME, ISSN 2535-0668, 3, 2018, 3-5
8. Radulov, N., Security 4.0. Part one: Security and The Forth Industrial Revolution, In: Security 4.0, Int. Sci. J., Ed. STUME, ISSN 2543-8582, year 4, issue 5, 2019, 265-267
9. Radulov, N., Ecosystem of Security 4.0, In: Security & Future, Int. Sci. J., Ed. STUME, ISSN 2535-0668, year 3, ISSUE 3, 2019, 69-70
10. Radulov, N., Additive Technology and Security 4.0, In: INDUSTRY 4.0, Int. Sci. J., Ed. STUME, ISSN 2534-8582, year 4, ISSUE 6, 2019, 317-318
11. Радулов, Н., „Сигурност 4.0“ монография, Изд. НТС по машиностроене „Индустрия 4.0“, София, 2019, ISBN 978-619-7383-15-7, 325 с.

IV. Използвана литература за написване на автореферата

На кирилица

1. Йончев, Д. В търсене на сигурността. Сигурността в концепцията на присъствието, „Изток-Запад“, 2014, 411 с.
2. Радулов, Н., Разузнавателен Анализ, АСИ Принт, София, 2013, 430 с.

На латиница

4. Attali, J., A Brief History of the Future: A Brave and Controversial Look at the Twenty-First Century, Arcade Publishing, 2009, ISBN 1-55970-879-4
5. Burrows, M., The Future, Declassified Megatrends That Will Undo the World Unless We Take Action, 2014
6. Goldston, D., Big data: Data wrangling, In: Nature, 455 (7209), 2008
7. Goodman, M., Future Crimes. Inside the Digital Underground and the Battle for Our Connected World, Penguin Random House, 2016, 608 p.
8. Greengard, S., The Internet of Things, May, 2015, MIT press, Part 4., 181
9. Grossman, N., Drones and Terrorism. Asymmetrical Warfare and the Threat to Global Security, I. B. Tauris & Co. Ltd., 2018
10. Howe, D., M. Costanzo, P. Fey, T. Gojobori, L. Hannick, W. Hide, D. P. Hill, R. Kania, M. Schaeffer, S. St Pierre, S. Twigger, O. White, S. Yon Rhee, Big data: The future of biocuration, In: Nature, 455 (7209), 2008
11. Lowenthal, M. Intelligence: From Secrets to Policy, Publ. April 28th 2006 by CQ Press, 334 p.
12. Lynch, C., Big data: How do your data grow? In: Nature, 455 (7209), 2008
13. Nelson, S., Big data: The Harvard computers, In: Nature, 455 (7209), 2008
14. Platt, W., Strategic intelligence production: Basic principles, New York: Frederick A. Praeger, 1957
15. Reilly, B. C., Doing More with More: The Efficacy of Big Data in the Intelligence Community, In: American Intelligence Journal 32:1 (2015): 18-24.
16. Russell, S., P. Norvig, Artificial Intelligence: A Modern Approach, Prentice Hall, 2010, 1132 p.

17. Waldrop, M., Big data: Wikiomics, In: Nature, 455 (7209), 2008
18. Weigend, A., Big Data, Levine Greenberg Rostan Literary Agency and Synopsis Literary Agency, 2017,