КОМПЛЕКСЕН МОДЕЛ НА СИГУРНОСТТА В КИБЕРПРОСТРАНСТВОТО

Иван Илиев
Университет по библиотекознание и информационни технологии

Резюме: Съвременното общество е изградено въз основа на изключителен напредък на науката и технологиите. Все по-голяма е необходимостта от изследване на връзката между науката за обществената сигурност и проблемите на човешкото общество, свързани с съвременните технологии, за да се идентифицират предизвикателствата в съвременната среда за киберсигурност. Повечето заплахи за нашата технологична сигурност идват от киберпространството, което води до значителни трансформации в системата за национална сигурност.

Ключови думи: национална сигурност, киберсигурност, технологии, системи на управление, изкуствен интелект.

Въведение

В различните политически и социални системи съществуването на сектор и организации за национална сигурност може да се счита за универсално в почти всички държави. Въпреки че има много формулировки и тълкувания на понятието „национална сигурност“ и на проблема, който то обхваща, няма общоприето определение.

Във връзка с това нововъзникналият аспект на националната сигурност във връзка с информационната, комуникационната сигурност, киберсигурността и защитата на националната сигурност, в съвременната цифрова ера е от първостепенно значение за нациите по света.

Обществата и икономиките все повече разчитат на информационни технологии и взаимносвързани мрежи и потенциалните уязвимости и последствия от кибератаки нарастват експоненциално.

Дигиталната трансформация на света доведе до множество ползи, от подобрени обществени услуги до подобрени икономически възможности. Това обаче изложи страните и на широк спектър от киберзаплахи, включително пробиви на данни, атаки с искане на откуп и кибершпионаж. Тези заплахи не само компрометират поверителността, целостта и наличността на критична информация, но също така имат потенциала да нарушат основни услуги и да навредят на националната сигурност.

Методология на изследването

Методическият подход и основните инструменти, използвани при провеждането на изследването се състоят от анализиране на научни публикации и правнонормативни документи. Разглеждат се някои стратегии и теории относно връзката между технологичната еволюция и сферата на националната сигурност, които могат да се тълкуват общо, независимо от държавата или средата. Всички тези теории и фактори, както и примерите на международната сцена показват посоката на бъдещото развитие на сигурността. Целта на разглеждането им е да предоставят пълен преглед на технологичните тенденции и да обозначат техните взаимовръзки с аспектите на националната сигурност.

Резултати

Секторът на националната сигурност е свързан със света на информационните и комуникационните технологии от гледна точка на разузнаването, контраразузнаването и събирането на информация. В този случай можем да видим трансформацията на разузнавателните технологии и методи и трансграничните възможности за решения за събиране на информация и как те излизат на преден план. Примери могат да бъдат случаите на масово събиране на данни, метаданни и събирането на информация. Освен въздействието върху националната сигурност, правните и дипломатическите последици от събирането и управлението на тази информация показват и посоките на технологичното развитие, например възможностите за използване на нарастващата маса от данни за целите на сигурността. Много методи за събиране на информация са едни и същи в процеса на събиране и анализиране на данни за криминални области и за националната сигурност, така че те зависят от техните различни цели и техните специфики.

Европейският съюз актуализира правилата си в областта на киберсигурността през 2023 г. Целта е да се надгради изградената правна рамка, за тя да бъде полезна в съвременния дигитален свят, като е разширява обхвата на областите и секторите, които тя засяга.

С оглед на събитията от последните години: световната пандемия, сериозните военни конфликти в няколко ключови места по света и зачестилите атаки на всички свързани с тях инфраструктури и крайни устройства, трябва да се въведат мерки и да се предприемат действия за адекватно решаване на проблемите в киберпространството. Трябва да се защити инфраструктурата на киберпространството, така също и всички свързани системи и обекти, както и да се насочи вниманието върху сигурността на услугите и мрежите за крайно потребление.

В нашия свят разпространението на инфокомуникационни решения, които вече са незаменими в нашето ежедневие, е непрекъснато. Появиха се

нови технологии и решения (например 5G технология, изкуствен интелект и интернет на нещата), чиито последствия за нашето ежедневие все още не са напълно известни. Въпреки това може да се предвиди, че те ще преобразят до голяма степен ежедневието ни, но освен положителния си ефект могат да носят и много заплахи. Помислете само за защитата на критичните инфраструктури, които използват ИТ решения, за сигурността на нашите лични данни или дори за проблема с разграничаването на истинската от невярната информация, която ни засяга.

Ролята на киберпространството става все по-важна и количеството информация, генерирана в цифров вид, нараства, което е добра индикация за темповете на развитие. Разпространението на цифровизацията, нарастващото значение на тенденцията за мобилност и значението на изкуствения интелект са прогнозирани и планирани.

Значителното увеличение на броя на устройствата през последните десет години, достигащи понастоящем десетки милиарди бройки, много от които ще бъдат обект на кибератаки, ще доведе до извънредно излагане на сигурността и нежелано развитие на сектора, като в отговор на това правителствата ще трябва да отделят все повече ресурси за своите способности за киберотбрана и по-нататъшното развитие на ИКТ средата.

Докато 3G технологиите дадоха възможност за мобилен интернет, а с 4G се появиха мобилните широколентови услуги, се очаква 5G да се превърне в инфраструктурата за свързаност, която ще проправи пътя за нови продукти и услуги и ще засегне всички сектори на обществото [1].

Много от съществуващите днес услуги зависят от 5G мрежите, което би могло да е предпоставка за мащабни и целенасочени атакати. Свързаността на устройствата и мрежите в единна система въздействат върху защитата на националната сигурност на държавата. Това означава, че опазването на тези мрежи от атаки, грешки и неизправности е от стратегичеко значение както за отделните държави, така и за Европейският съюз.

Сложността на безжичните мрежови екосистеми и устройствата, свързани с интернет на нещата (IoT), се увеличава бързо с напредъка на технологиите и респективно се увеличават и киберзаплахите. Съществуващите методи не могат да вземат последователни решения в сложни мрежови среди, особено в случаи с частична наблюдаемост и нестационарност [2]. Мрежовата осведоменост наблюдава и разбира активностите на мрежата, уязвимостите и текущите дейности в реално време, след което са необходими усъвършенствани анализи, алгоритми за машинно обучение и изкуствен интелект, за да се подобри възприемането на риска посредством анализиране на огромни количества информация, идентифициране на тенденции и предвиждане на бъдещи пробиви в сигурността.

Развитието също така показва сериозността на проблемите на технологичното превъзходство и „дисбаланса“ в притежаването на съвременни технологии. Зависимостта от чужди технологии и по този начин уязвимостта към оборудването, системите и доставчиците от други страни също могат пряко и косвено да повлияят на сигурността на дадена общност, държава или елемент от системата за национална сигурност [3]. Причините за това могат да бъдат видени и във факта, че информационните и комуникационните технологии, както и свързаните с киберпространството индустрии станаха стратегически важни. Примери вече може да се видят на международната сцена, като най-значим пример е конфликтът между САЩ и Китай относно икономическото значение на 5G технологията и сигурността, която се видоизменя вследствие на тази технология.

Нововъзникващите технологии стават все по-достъпни в широк кръг от области, и то много по-бързо, отколкото в миналото. Този бърз темп на усвояване на технологиите изпреварва възможностите на гражданското общество, регулаторите и организациите да прилагат принципите за безопасност и сигурност. Необходимо е отговорно внедряване на новите технологии, като от решаващо значение е да се подсили основата: системи, необходими за поддържането на тези технологии в изправност. В противен случай организациите вероятно ще бъдат под риск да допуснат фундаментални уязвимости на сигурността, устойчивостта и доверието на работещите с тях. Констатациите на Global Cyber Outlook за 2024 г. показват, че организациите обръщат внимание и реагират бързо, за да смекчат рисковете от приемане на нововъзникващи технологии. В прогнозата за глобалната киберсигурност приблизително половината от лидерите казват, че автоматизацията и машинното обучение биха имали най-голямо влияние върху киберсигурността през следващите две години [4]. Към момента положението е същото – тази година приблизително половината от лидерите все още са съгласни, че генеративният изкуствен интелект ще има най-значително въздействие върху киберсигурността през следващите две години. Изкуственият интелект ще има най-голямо отражение върху индустрии като киберсигурност (65%), селско стопанство (63%), банкиране (56%) и застраховане (56%), като това са основно индустриите, които ще предприемат мерки по управлението и сигурността, свързани с тази нова технология. Мащабът на технологията е такъв, че взаимодейства с всички индустрии, предприятия и отделни субекти, които дори не знаят за участието си. През следващите години ще се тестват подходът на глобалните организации към управлението на риска и устойчивостта им, тъй като повечето големи организации се трансформират по-бързо и по-често в сравнение с държавните или малките организации. Големите компании използват ки-

берсигурността като диференциращ фактор за постигане на по-добри бизнес резултати и по-голяма конкурентоспособност спрямо съперниците си.

Изводи/Дискусия

Сигурното и надеждно участие в съвремения динамичен и технологично зависим свят трябва да цели укрепване и защитаване на позицията на всеки участник в киберпространството по адекватен и целесъобразен начин и това трябва да важи за всяка нововъзникваща технология, устройство или връзка. Много от векторите на атаките могат да изглеждат еднакви на пръв поглед, но те са склонни да се усилват и разклоняват в неочаквани посоки. Настъпващите промени засягат бъдещето на мисленето относно националната сигурност и развитието на принципите и методите, които да се изполват. Задачата на участниците в системите за национална сигурност, работещи при строго законодателство, е да реагират ефективно на различни заплахи в променящата се среда. Всичко това е възможно само чрез непрекъснато наблюдение и реагиране на промените в околната среда и дългосрочно стратегическо мислене.

Заключение

Необходимостта от цялостно и проактивно справяне с киберзаплахите никога не е била по-критична. Апаратът за национална сигурност трябва да се адаптира към развиващия се характер на кибервойната и да разработи стабилни стратегии, политики и способности за защита на интересите на страната. Естеството на проблема и необходимите промени пред управлението на киберпространството са как организациите да отговорят на технологичните разработки, как да се справят с настъпващите регулации, проблеми и промени, вследствие на което да се достигне до извода, че функционирането на националната сигурност е неразделна част от социалната среда заедно с нейните процеси и взаимодействието им с технологиите.

References/Литература

1. **Evropeyska** komisia, Generalna direktsia „Saobshtitelni mrezhi, sadarzhanie i tehnologii“. Instrumentarium na ES za sigurnostta v oblastta na 5G: nabor ot stabilni i vseobhvatni merki za koordiniran podhod na ES za garantirane na sigurnostta na 5G mrezhi. Sluzhba za publikatsii na Evropeyskia sayuz, 2021. https://data.europa.eu/doi/10.2759/07427.

   [**Европейска** комисия, Генерална дирекция „Съобщителни мрежи, съдържание и технологии“. Инструментариум на ЕС за сигурността в областта на 5G: набор от стабилни и всеобхватни мерки за координиран

подход на ЕС за гарантиране на сигурността на 5G мрежи. Служба за публикации на Европейския съюз, 2021. https://data.europa.eu/doi/10.2759/07427.]
2. **Xie**, Junwei, Application Study on the Reinforcement Learning Strategies in the Network Awareness Risk Perception and Prevention. – In: *International Journal of Computational Intelligence Systems*, Springer Science and Business Media B.V., 2024.
3. **Lewis**, J. A. Telecom and National Security (commentary). March 13, Center for Strategic and International Studies (CSIS), 2018. https://www.csis.org/analysis/.
4. **Lamba**, Tripti, Shivani **Kandwal**. Global Outlook of Cyber Security. 2022, pp. 269 – 276. 10.1007/978-981-19-2065-3_30.

За автора

Иван Илиев е докторант в Университета по библиотекознание и информационни технологии. Професионалните му интереси са в областта на защитата на националната сигурност и сигурността на информационните и комуникационните системи.

За контакт с автора: 9123490-1@unibit.bg

A COMPREHENSIVE MODEL OF SECURITY IN CYBERSPACE

Ivan Iliev
University of Library Studies and Information Technologies

Abstract: Modern society is based on exceptional progress in science and technology. It is increasingly the need to explore the connection between the science of public security and the problems of human society related to modern technology to identify the challenges in the modern environment for cybersecurity. Most threats to our technological security come from cyberspace, leading to significant transformations in the national security system.

Keywords: national security, cyber security, technologies, management systems, artificial intelligence.

About the Author

Ivan Iliev is a doctoral student at the University of Library Science and Information Technology. His professional interests are in the field of national security defence and the security of information and communication systems.

To contact the Author: 9123490-1@unibit.bg