Република Северна Македонија
Министерство за одбрана

СТРАТЕГИЈА ЗА САЈБЕР ОДБРАНА

Март 2026

Содржина

Предговор

Безбедноста на граѓаните, заштитата на суверенитетот и територијалниот интегритет, како и зачувувањето на демократските вредности и владеењето на правото, претставуваат основни функции на државата. Остварувањето на овие функции бара стабилен и интегриран систем за одбрана, заснован на долгорочна визија, јасна институционална одговорност и континуиран развој на способности.

Врз основа на Стратегијата за одбрана, Министерството за одбрана ја донесува Стратегијата за сајбер одбрана (2026–2030), со цел системско зајакнување на одбранбените способности во сајбер просторот како составен дел од интегрираната одбрана на Република Северна Македонија. Во современото безбедносно опкружување, сајбер просторот претставува оперативен домен во кој нарушувањето на комуникациско-информациските системи може директно да влијае врз способноста за командување, контрола и извршување на воените мисии. Оттука, сајбер одбраната се дефинира како постојана воена задача која се спроведува во мир, вонредна и воена состојба.

Оваа Стратегија ги преточува стратегиските определби во јасни насоки за управување, планирање и развој на способности. Таа воспоставува институционален став дека одбраната во сајбер просторот е предуслов за оперативна подготвеност на Армијата и дека нејзиниот развој мора да се третира со ист степен на приоритет како и останатите борбени и капацитетите за поддршка.

Како членка на НАТО, Република Северна Македонија има обврска да обезбеди интероперабилност, доверливост и отпорност на своите воени системи. Придонесот кон колективната одбрана не се мери само преку физичко распоредување на сили, туку и преку способноста за сигурно и непречено дејствување во дигитално и хибридно опкружување. Сајбер одбраната претставува составен дел од националните обврски во рамките на Алијансата и од способноста за учество во меѓународни мисии и операции.

Стратегијата ја препознава меѓузависноста помеѓу воените системи и останатите елементи на националната критична инфраструктура. Одбранбениот систем во значителна мера се потпира на цивилни комуникациски, енергетски и информатички капацитети, кои исто така можат да бидат цел на сајбер напади. Поради тоа, Стратегијата предвидува соработка со надлежните државни органи и со приватниот сектор, притоа строго зачувувајќи ја оперативната автономија и безбедносната контрола над воените системи.

Со оваа Стратегија се воспоставуваат јасни надлежности, механизми за координација и принципи на дејствување во кризни состојби, со цел зајакнување

на националната и сојузничката сајбер отпорност и обезбедување ефективна одбрана на државата во оперативниот сајбер простор.

Вовед

Изработката на Стратегијата за сајбер одбрана (2026–2030) го утврдува долгорочниот пристап на Министерството за одбрана за заштита и одржување на воените оперативни способности во сајбер просторот. Стратегијата го препознава сајбер просторот како оперативна средина во која воената ефикасност, командната структура и националните безбедносни интереси се постојано оспорувани и изложени на сложени хибридни влијанија.

Стратегијата е изградена врз принципот „отпорноста на прво место“. Таа поаѓа од реалната претпоставка дека непријателските активности се континуирани, дека стратегиската конкуренција се одвива под прагот на вооружен конфликт и дека нарушувањата во сајбер просторот имаат висока веројатност да коинцидираат со воено-политички кризи. Оттука, одбранбениот систем мора да биде дизајниран да функционира под притисок, да ги апсорбира нарушувањата и брзо да ја враќа функционалноста без загрозување на мисијата.

Ова подразбира обезбедување на континуитет на командувањето и контролата, сигурни и заштитени комуникации, дисциплинирано управување со идентитет и пристап, сегментација на критичните системи, постојан мониторинг, организиран и извежбан одговор на инциденти, како и системско и предвидливо закрепнување. Одвраќањето се заснова првенствено на принципот на негирање реализиран преку изградба на зајакнат, прилагодлив и обновлив одбранбен систем кој го ограничува влијанието и ја намалува можноста противникот да постигне значајни стратегиски ефекти.

Стратегијата е структурирана околу четири меѓусебно поврзани столба на имплементација за периодот 2026–2030 година, насочени кон постигнување четири стратегиски резултати до 2030 година: професионален и одржлив сајбер персонал, модернизирана и отпорна одбранбена дигитална инфраструктура, управувачка и оперативна рамка усогласена со НАТО стандардите и меѓународната соработка, како и целосно оперативна способност за одбранбени сајбер операции со елементи за брз одговор.

Си имплементацијата на Стратегијата, до 2030, одбранбениот систем треба да биде способен да ги одржува суштинските функции на мисијата во услови на напад врз дигиталната инфраструктура, ефикасно да координира дејствување при сериозни инциденти и со способност да придонесува во колективната одбрана, врз основа на отпорност, интероперабилност и дисциплинирана институционална одговорност.

Визија

Со имплементацијата на Стратегијата за сајбер одбрана, Министерството за одбрана и Армијата на Република Северна Македонија да поседуваат интегрирана, подготвена за оперативни дејства и интероперабилна способност за сајбер одбрана која обезбедува непрекинатост на командувањето и контролата, заштита на комуникациско-информациските системи и слобода на дејствување во сајбер просторот во мир, криза и вооружен конфликт.

Сајбер одбраната се третира како постојана воена мисија и составен дел од одбранбеното планирање, управувањето со ризик и развојот на силите. Системите на Министерството за одбрана и Армијата ќе бидат проектирани и управувани со вградена отпорност, способни да издржат, апсорбираат и брзо да се опоравуваат од софистицирани сајбер напади без нарушување на оперативната готовност и извршувањето на мисијата.

Визијата подразбира воспоставување на јасна командна одговорност, постојана ситуациона свест, адаптибилна одбрана и координиран одговор, во целосна усогласеност со стандардите и принципите за колективна одбрана во сајбер доменот на национално и меѓународно ниво.

Министерството за одбрана ќе развива сајбер способност која не само што штити, туку обезбедува оперативна предност и ја зајакнува националната и сојузничката отпорност во оперативниот сајбер простор.

Мисија

Мисијата на Министерството за одбрана и Армијата во сајбер доменот е да ја заштитат, обезбедат и одржат отпорноста на комуникациско-информациските системи, мрежите и податоците од значење за одбраната, со цел да се гарантира непречено командување и контрола, за сигурно донесување одлуки и ефективно извршување на националните и сојузничките мисии.

Оваа мисија се реализира преку:

- воспоставување на кохерентен систем за управување со сајбер одбраната со јасно дефинирани надлежности и одговорности;
- развој и одржување на технички и оперативни капацитети за превенција, детекција, одбрана, одговор и опоравување од сајбер инциденти;
- интеграција на сајбер одбраната во сите нивоа на воено планирање, подготовка и операции;
- развој и задржување на стручен персонал со способности усогласени со национални и меѓународни стандарди;
- обезбедување интероперабилност и размена на информации на национално ниво и со сојузниците во рамките на колективната одбрана.

Сајбер одбраната се спроведува како континуирана функција, заснована на проценка на ризик, принципот на отпорност и целосна усогласеност со националното законодавство и меѓународното право.

1. Стратегиска поставеност

Стратегија се донесува како рамка за имплементација на сајбер одбрана во Министерството за обрана и Армијата. Таа ја операционализира насоката утврдена во Стратегијата за одбрана дека остварувањето на одбранбените цели бара континуирано следење на безбедносната средина, координирано планирање и развој на соодветни способности.

Истовремено, Стратегијата е усогласена со Националната стратегија за сајбер безбедност 2025–2028, преку воведување на релевантните национални принципи како што се управување засновано на проценка на ризик, отпорност, безбедност вградена во системскиот дизајн и координирано управување со инциденти.

Во рамките на одбранбено планирање, оваа Стратегија претставува документ кои ги дава насоките за развој на одбранбени политики, министерски упатства, доктринарни измени, плански документи и програми за имплементација. Таа обезбедува основа за развој на способности, имплементација на иновативни пристапи, дефинирање на приоритети за обука и спроведување на активности за утврдување и проценка на подготвеноста во рамките на структурите на Министерството и Армијата.

Стратегија го опфаќа одбранбениот систем во целина: Министерството за одбрана, Генералштабот како носител на воената командна одговорност, подредените структури, различните системи за одбрана, како и сервисите неопходни за обезбедување на оперативна способност. Истата се однесува и на воените мрежи и комуникации, информациските системи што го поддржуваат командувањето и контролата, како и управувачките и контролни механизми неопходни за обезбедување на нивната доверливост, интегритет и достапност во услови на постојани закани во сајбер просторот.

Со Стратегијата свесно се избегнува дуплирање на националната цивилна рамка за сајбер безбедност. Наместо тоа, Министерството за одбрана ќе одржува сопствена одбранбено-оперативна способност, ќе соработува преку формални процеси за координација и ќе придонесува кон севкупната државна отпорност кога тоа е неопходно, но со целосно зачувување на оперативната автономија над воените системи и комуникации.

Стратегијата не пропишува конкретни технички решенија, производи или алатки. Техничките избори ќе се утврдуваат преку подредени планови, одлуките за имплементација на инфраструктурни решенија и предвидените оперативни процедури. Овој документ ја утврдува политичката насока и дисциплината на

уверување врз основа на кои тие избори ќе се оценуваат во однос на придонесот кон оперативната подготвеност и отпорноста на одбранбениот систем.

Во современите воени операции оперативна способност зависи од интегритетот, достапноста и доверливоста на информациските системи и комуникациските врски. Тука ефектите од сајбер нападите ретко се изолирани; тие можат да бидат синхронизирани со дезинформации, саботажи или поширок хибриден притисок со цел нарушување на процесот на донесување одлуки и ослабување на воениот одговор. Поради тоа, одбранбениот систем мора да поаѓа од претпоставката дека сајбер нарушувањата ќе бидат постојани во мирновремени услови и ќе се интензивираат во услови на криза, при што софистицираните актери ќе настојуваат да ги искористат зависностите и организациските слабости, наместо само да „прекинат“ поединечен систем. Оттука, оваа Стратегија ја третира сајбер одбраната како обезбедување на мисијата со цел заштита на способноста за командување, комуникација, координирање и одржување на силите, во услови на зависност од цивилна инфраструктура.

2. Правна и институционална рамка

Министерството за одбрана ја задржува политичката надлежност за одбранбената политика, распределбата на ресурсите и исполнувањето на националните и сојузничките обврски во сајбер доменот. Генералштабот ја задржува одговорноста за интеграција на сајбер одбраната во борбената готовност, оперативното планирање и извршувањето преку синџирот на командување. Оваа поделба ја одразува суштинската демократска поставеност на цивилна контрола и воена командна одговорност и претставува предуслов за дисциплинирана и ефективна сајбер одбрана.

Со цел обезбедување единство на напорите во рамките на одбранбениот систем, Министерството за одбрана и Армијата ќе воспостават централно координативно тело во доменот на сајбер одбраната, како носител на надлежност за усогласување на политиките, надзор над имплементацијата и консолидирано известување за состојбата на подготвеноста и клучните ризици. Ова тело ќе има јасно дефинирани овластувања и одговорности, со цел обезбедување на системска усогласеност. Со оваа Стратегија се утврдува дека назначеното централно координативно тело во доменот на сајбер одбраната ќе биде одговорно за обезбедување кохерентност на политиките во рамките на Министерството, стандардизација на процедурите, одржување на рамка за мерење на перформанси и институционална зрелост, како и интегрирање на извештаите со цел обезбедување подобро одлучување од страна на Министерството по прашања релевантни за сајбер одбраната.

Оперативното извршување останува во рамките на синџирот на командување на Армијата и определените оперативни елементи, вклучително и способноста за одговор на сајбер инциденти и капацитетите за постојан мониторинг и реакција. Улогата на централното координативно тело во доменот на сајбер одбраната не е

оперативно командување, туку обезбедување системска кохезија: единствени стандарди, спроведливи приоритети, јасно дефинирани одговорности и обезбедување верификација на подготвеноста за сајбер одбрана.

Сајбер одбраната мора да функционира континуирано, но истовремено да може да се прилагодува и засилува на контролиран и правно кохерентен начин во согласност со ескалацијата на безбедносната средина. Поради тоа, оваа Стратегија воспоставува четири нивоа на активирање, кои имаат за цел да ја насочуваат подготвеноста, донесувањето одлуки и координацијата, без создавање техничка или институционална нејасност.

1. Во услови на **Редовна одбранбена поставеност**, сајбер одбраната претставува трајна функција насочена кон превенција преку дисциплинирано управување, континуиран мониторинг, намалување на ранливостите и обезбедување на мерки за закрепнување. Целта на оваа поставеност е подготвеноста на системот за сајбер одбрана преку изградба на ниво на отпорност што овозможува управлива, а не хаотична ескалација. Во оваа фаза се обезбедува редовна валидација, интеграција на сајбер аспектите во обуката и постојано унапредување врз основа на научените лекции и проценетите ризици.
2. Во услови на **Зголемена будност**, активирана поради засилена геополитичка напнатост, веродостојни индикатори за закана или зголемени непријателски активности насочени кон националните институции, одбранбениот систем го засилува мониторингот, ја забрзува примената на безбедносни ажурирања и третманот на ризиците кај системите од суштинско значење за мисијата, ја зголемува подготвеноста на тимовите за брз одговор и воведува построга контрола врз конфигурациските промени. Значаен сегмент во оваа фаза е поставувањето на приоритети како што се насочување на вниманието и ресурсите кон функциите од суштинско значење за мисијата и обезбедување дека раководството има јасна слика за тековниот ризик и неговите оперативни импликации.
3. Во услови на **Одбранбена криза**, активирана поради значајни национални сајбер инциденти, хибриден притисок што влијае врз одбранбената подготвеност или непосредна закана по безбедноста на одбранбените операции, одбранбениот систем преминува во кризен режим на функционирање. Одлучувањето во сајбер доменот станува временски чувствително, процедурите за ескалација се скратуваат, а координацијата со националните структури за управување со кризи станува континуирана. Приоритет е обезбедување на континуитет на командувањето, сигурни комуникации и стабилизација на одбранбените сервиси. Системот мора да биде способен да функционира во режим на деградација, да ги одржува суштинските функции и брзо да ги обнови критичните сервиси, при истовремено зачувување на класифицираните информации и оперативната безбедност.

4. Во услови на **Конфликтна поставеност**, активирана во случај на вооружен конфликт или еквивалентни состојби, сајбер одбраната станува неразделна од оперативното опстојување. Одбранбениот систем мора да поаѓа од претпоставката за континуирана непријателска активност насочена кон неговата дигитална инфраструктура и да функционира со нарушувањето како очекувана состојба. Донесувањето одлуки се фокусира на одржување на мисијата, заштита на силите и зачувување на оперативната слобода на дејствување. Координацијата со сојузниците станува суштинска за обезбедување интероперабилност и поддршка, при што одбранбениот систем мора да ја одржува сопствената минимална функционална способност додека се интегрира во рамките на колективната одбрана.

Предвидените нивоа на активирање треба да бидат рефлектирани во подредените директиви, проверките на подготвеност, предвидените процедури и известувања, со цел ескалирањето да резултира со предвидливо институционално однесување, а не со импровизација.

Цивилната контрола се остварува преку насоки дефинирани од страна на Министерството со кои се врши одобрување на стратегиски планови, воспоставување на механизми на отчетност како и распределба на соодветни ресурси.

Воената командна одговорност се реализира преку обезбедување на подготвеност, дисциплина, интеграција на сајбер одбраната во оперативното планирање и нејзино извршување преку линијата на командување и контрола. Оперативната автономија во сајбер одбраната подразбира дека Армијата ја задржува целосната надлежност врз функционирањето, заштитата и обновувањето на воените мрежи, системи и комуникациска инфраструктура. Поради тоа, оваа Стратегија утврдува дека одлуките во доменот на сајбер одбраната кои влијаат врз функциите од суштинско значење за мисијата мора да останат во рамките на одбранбените командни аранжмани, со јасно дефинирани прагови на ескалација кон министерското раководство кога станува збор за одлуки од стратегиско значење.

Министерството за одбрана ќе учествува во националните структури за управување со кризи преку дефинирани врски за координација и усогласени процедури за размена на информации, усогласување на јавната комуникација и заемна поддршка. Во случај на големи национални сајбер инциденти што влијаат врз поширокатa општествена стабилност, одбранбениот систем ќе споделува информации релевантни за националната безбедност, со целосно почитување на законот за безбедност на класифицирани информации како и законските и подзаконските акти за безбедност на класифицирани информации.

Во ситуации кога националното управување со кризи, предводено од цивилните структури, бара увид во состојбата на одбранбениот систем, во услови кога нарушување на цивилна критична инфраструктура влијае врз одбранбената

подготвеност, Министерството за одбрана и Армијата ќе обезбедат ажурирани информации за состојбата, проценки на влијанието и точки за координација, задржувајќи ја целосната надлежност за техничките и оперативните мерки во рамките на сопствените мрежи и системи.

Стратегија наложува воспоставување на постојан механизам за цивилно-воена координација, кој ќе функционира редовно во мирновремени услови и ќе преминува во континуиран режим на ангажман во услови на криза. Што значи дека, согласно Стратегијата, учеството на Министерството и Армијата е интегрирано во националната рамка за управување со кризи, при што истовремено ја зачувува на јасноста на одбранбената командна структура.

3. Предизвици за сајбер одбрана

Одбранбениот систем функционира во средина во која непријателската сајбер активност е постојана, адаптивна и често интегрирана во поширок хибридни кампањи. Софистицираните актери настојуваат да обезбедат долгорочен пристап, разузнавачка предност и можност за нарушување на процесот на донесување одлуки во одлучувачки моменти. Притисокот ретко е јавно најавен; тој се акумулира преку извидување, компромитација на синџири на снабдување, злоупотреба на кориснички права и надлежности, и постепено еродирање на довербата во системите и информациите.

Во такви услови, традиционалната разлика помеѓу „мир“ и „конфликт“ станува нејасна. Одбранбениот систем мора да поаѓа од претпоставката дека функционирањето во услови на активна сајбер закана претставува основна состојба, а не исклучок.

Стратегиската подготвеноста не може да се мери исклучиво преку опрема и распоред на обука. Таа мора да ја вклучи способноста за одржување на функционално командување и контрола, зачувување на интегритетот на оперативните информации и продолжување на операциите во услови на нарушување. Поради тоа, сајбер одбраната во оваа Стратегија се третира како клучна компонента на оперативната способност и предуслов за подготвеност.

Државно спонзорираните актери претставуваат највисок ризик, бидејќи комбинираат техничка софистицираност, долгорочна упорност и стратегиска намера. Во одбранбен контекст, нивните цели најчесто вклучуваат прибирање оперативно релевантни информации, подготовка на деструктивни опции за време на криза и поткопување на довербата во колективната безбедност.

Криминалните актери претставуваат значаен секундарен ризик, бидејќи нивните методи како изнуда, откупнички софтвер и посредување во пристап, можат да предизвикаат високо ниво на нарушување, а нивната инфраструктура може да биде искористена од пософистицирани актери.

Идеолошки мотивираните актери можат да создадат репутациска штета и оперативна дистракција, особено во политички чувствителни периоди, но нивното стратегиско влијание обично е ограничено освен ако нивните активности не се синхронизирани со поширoки кампањи.

Одбранбениот систем мора да се штити од целокупниот спектар на закани, но приоритетот мора да се насочи кон заканите кои најзначајно влијаат врз мисијата. Системите што го поддржуваат командувањето и контролата, подготвеноста на силите, мобилизацијата, разузнавачката поддршка и оперативните комуникации бараат највисоко ниво на отпорност и уверување.

Современата одбранбена способност се потпира на меѓусебно поврзани информациски системи и на функционални врски што надминуваат директна контрола на Министерството и Армијата. Цивилната инфраструктура, особено енергетскиот систем и телекомуникациите, создаваат системски ризик, бидејќи нејзиното нарушување може да предизвика каскадни ефекти врз одбранбената подготвеност. Стратегија експлицитно го препознава зголемениот ризик произлезен од ваквите функционални врски и фактот дека отпорноста на тие субјекти станува составен дел од воената подготвеност.

Линиите на снабдување претставуваат дополнителен системски ризик. Одбранбените системи се развиваат и одржуваат преку добавувачи, интегратори и сервисни провајдери. Компромитација на добавувач може директно да се одрази врз одбранбените операции. Поради тоа, оваа Стратегија ја третира сигурноста на линиите на снабдување и принципот „безбедност по дизајн“ во процесот на набавка како императиви за обезбедување на мисијата, а не како административна формалност.

Комплексноста и наследените (застарените) системи, исто така, претставуваат двигатели на ризик. Одбранбената инфраструктура се развива со децении, често со акумулирани технички предизвици. Во услови на криза, кревка наследена средина ја зголемува веројатноста дека одбранбените мерки ќе предизвикаат несакани нарушувања. Поради тоа, модернизацијата и способноста за закрепнување не се третираат како „информатички надградби“, туку како инвестиции во отпорност неопходни за континуитет на операциите.

Новите технологии истовремено ги зголемуваат можностите за развој и употреба на комуникациско – информациските системи и на заканите. Автоматизацијата може да го забрза одбранбеното и напаѓачкото дејствување. Вештачката интелигенција овозможува побрзо извидување, адаптивни фишинг кампањи и манипулација со информации, вклучително и синтетички медиуми што можат да ја поткопаат довербата, преку содржини од типот „deepfake“. Додека развојот на квантното пресметување претставува идно потенцијално нарушување на постојните криптографски механизми.

Во ваков безбедносен опсег, превенцијата сама по себе е структурно недоволна. Одбранбениот систем мора да претпостави дека обидите за компромитација ќе бидат постојани и дека во одредени случаи ќе успеат. Отпорноста преку ограничување на опсегот на нарушување, одржување на суштинските функции и брзо закрепнување, претставува единствена стабилна основа за зачувување на оперативната подготвеност во услови на неизвесност.

4. Водечки принципи

Оваа Стратегија се реализира преку шест водечки принципи. Секој принцип претставува насока на градење на одбранбената способност во сајбер просторот. Следењето на принципите при реализација на стратегијата треба да придонесе сајбер одбраната да биде оперативно поставена, заснован на проценет ризик, прилагодена на современото оперативно опкружување, базирана на стандарди, со инкорпорирана структурирана соработка и институционална одговорност. Овие принципи имаат за цел да се спречи третирање на сајбер одбраната како изолирана техничка програма, туку како одбранбена способност што мора да биде планирана, финансирана, извежбана и оперативно функционална.

4.1 Оперативна поставеност

Принципот на оперативна поставеност на сајбер одбраната постои за да ги заштитат и обезбедат резултатите од одбранбените дејства.

Стратегиски цели со примена на овој принцип се:

- Целосна интеграција на сајбер одбраната во оперативното планирање и извршување во сите домени, така што сајбер аспектите ќе бидат вградени во стратегиското планирање, подготвеноста, вежбите и извршувањето на мисиите. Практичната импликација е дека барањата за сајбер одбрана ќе се третираат како составен дел од критериумите за оперативна подготвеност, а сајбер ризикот ќе се изразува во оперативни термини како влијание врз командувањето, темпото, логистиката и успехот на мисијата, а не исклучиво во технички категории.
- Обезбедување континуирана оперативна ефикасност на системите за командување и контрола и во услови на активна сајбер закана. Подразбирајќи дизајн на одбранбениот систем и обука персоналот за одржување на мисијата во услови на нарушување, деградација или непријателска сајбер активност. При што се одредува секоја функција од суштинско значење за мисијата, што зависи од дигитални сервиси, да има дефинирани процедури за функционирање во режим на деградирана инфраструктура, утврдени цели за закрепнување и редовно извежбани процедури за континуитет.

4.2 Планирање засновано на проценет ризик

Принцип за планирање на сајбер одбраната врз основа на проценетиот ризик, дефинира дека мора да се следат заканите кон мисијата и преземаат мерки за управување на истите.

Стратегиски цели со примена на овој принцип се:

- Интеграција на развој на способности водени од разузнавачки проценки за закани во структурата на организациите. Приоритетот на инвестирање се заснова врз валидни проценки на закани, анализа на важноста на мисијата и изложеност на ризик од стратегиски аспект. Ова бара воспоставување структуриран механизам за проценка на ризик и редовно ангажирање на раководството во справување со сајбер ризикот како значаен сегмент од одбранбеното планирање.
- Усогласување на распределбата на ресурси врз основа на важноста на мисијата и ризикот од сајбер напади. Ова значи дека средствата и преземените мерки и активности ќе бидат концентрирани таму каде што оперативното влијание е највисоко, во функциите од суштинско значење за мисијата, критичните комуникации и системите неопходни за исполнување на националните и обврските преземени во рамките на колективните структури за безбедност. Што подразбира дека и системите со помало значење ќе бидат заштитени, но не на сметка на критичната инфраструктура за одбрана.

4.3 Следење и интеграција на нови технологии

Принципот на следење и интеграција на нови технологии, претставува прилагодување кон современото оперативно опкружување. Сајбер одбраната мора да ја одразува реалноста на хибриден, мулти-доменски и информациски заситен конфликт.

Стратегиски цели со примена на овој принцип се:

- Развој на способности за ефективно функционирање во хибридни и мулти-доменски сценарија на закани. Сајбер одбраната да биде интегрирана во вежбите и оперативните претпоставки, каде што нарушувањето на информатичката инфраструктура, манипулацијата со информации и паралелните физички прекини се третираат како реални, а не исклучителни услови.
- Предвидување и одговор на новите технолошки и оперативни предизвици. Одржување на адаптивна поставеност, преку континуирана проценка на растечките методи на закана и технолошките промени, како што се автоматизирани напади и ризици поврзани со криптографија. Ова не подразбира шпекулативни технолошки програми, туку дисциплинирано

следење на трендовите поврзано со набавки, обука и имплементација на отпорност.

4.4 Стандардизирана оперативна дисциплина

Принципот на стандардизирана оперативна дисциплина е пристап заснован на строго дефинирани стандарди кои треба да ги дефинираат насоките на функционирање во национални и меѓународни рамки.

Стратегиски цели со примена на овој принцип се:

- Вградување на принципите „безбедност по дизајн“ и „zero-trust“ низ целиот животен циклус на одбранбените системи. Што значи дека безбедносните барања ќе бидат составен дел од набавките, одобрувањето на инфраструктурни решенија и управувањето со системите, со цел новите решенија да не создаваат слаби и ранливи структури.
- Усогласеност со побарувањата за соработка со националните институции и меѓународните партнери преку усвојување на релевантните меѓународни стандарди и рамки во областа на сајбер одбраната, а се со цел обезбедување оперативна интероперабилност и доверливост.

4.5 Структурирана соработка

Принципот на структурирана соработка за спроведување на сајбер обрана се однесува на соработката со цивилните органи, субјектите на критичната инфраструктура, индустријата, академската заедница и меѓународните партнери, но таа мора да се реализира преку формални процеси што ги штитат чувствителните информации и ја зачувуваат командната автономија.

Стратегиски цели со примена на овој принцип се:

- Интеграција на цивилно-воената соработка за спроведување на сајбер отпорност преку воспоставување на формални процедури за координација со националните цивилни органи и структурите за управување со кризи, обезбедувајќи навремена ескалација и усогласување во национални кризни состојби, во согласност со националната рамка за управување со сајбер кризи.
- Зајакнување на интеграцијата во колективната сајбер одбрана со меѓународните партнери. Оваа Стратегија наложува активно учество во сојузничките механизми за размена на информации и реализација на вежби, со цел валидација на интероперабилноста, одлучувањето и координираниот одговор во случај на реален сајбер напад.

4.6 Институционална одговорност

Принципот на институционална одговорност во обезбедува дека сајбер одбраната не смее да зависи од индивидуална експертиза или краткорочни проекти.

Стратегиски цели со примена на овој принцип се:

- Воспоставување јасно управување, авторитет и отчетност. Овој принцип налага во Стратегијата формално да ги дефинира улогите и одговорностите во рамките на одбранбениот систем, вклучително и централен носител на надлежност за сајбер одбрана одговорен за кохерентност, надзор и известување, како и јасно дефинирани оперативни одговорности преку синџирот на командување.
- Бидејќи сајбер одбраната фундаментално зависи од обучен и постојан персонал потребно е создавање на систем за кој ќе обезбеди одржлив развој и задржување на персоналот, и организациска зрелост за сајбер одбрана. Тоа значи развој на кариерни патеки, професионално образование и механизми за задржување, со цел експертизата да стане институционална способност, а не индивидуална предност.

5. Стратегиските области на развој

Имплементацијата на Стратегијата се реализира преку развој на стратегиски способности дефинирани со четири фундаментални столба. Овие столбови претставуваат структурирани области насочени кон постигнување мерливи резултати во подготвеноста на сајбер одбраната до 2030 година, и тоа преку зајакнување на оперативната сајбер подготвеност и обезбедување на мисијата, воспоставување управување засновано на ризик и ефективен стратегиски надзор, унапредување на интероперабилноста и усогласеноста со стандарди во рамки на колективната одбрана, како и развој на одржлив човечки капитал и организациска отпорност.

Секој столб е дефиниран преку неговата стратегиска перспектива, логика на имплементација, очекувано ниво на зрелост до 2030 година како и придонесот кон континуираната оперативна подготвеност.

5.1 Столб 1: Оперативна сајбер подготвеност и обезбедување на мисијата

Првиот столб има за цел трансформација за интеграција на сајбер одбраната во оперативна способност што директно ја поддржува воената ефикасност и континуитетот на командувањето. Овој столб се фокусира на вградување на сајбер одбраната во оперативната доктрина и планирањето, заштита на функциите од суштинско значење за мисијата, имплементација на сегментација и дисциплинирано управување со идентитет и пристап, како и структурна интеграција на процедури за функционирање при нарушен режим на работа.

Овој столб бара дисциплинирано уверување во способноста за закрепнување. Одбранбениот систем мора да може предвидливо и навремено да ги обновува критичните сервиси. Оперативната подготвеност ќе се мери не само преку детекција и одговор, туку и преку способноста за одржување на континуитет на мисијата и обновување на суштинските сервиси во рамки на дефинирани временски цели.

Со цел подобрување на оперативната свест за сајбер ситуациите и можностите за координиран одговор, Министерството за одбрана ќе обезбеди услови и ресурси за функционирање на СаОЦ, во Министерството за одбрана и Армијата, одговорен за континуирано следење на информатичките мрежи и инфраструктура, координација при одговор на сајбер инциденти и поддршка на одбранбените операции во сајбер просторот. За зајакнување на оперативната отпорност Армијата ќе развие распоредлив капацитет за сајбер одбрана способен да ги поддржи распоредливите единици на Армијата.

Министерството за одбрана и Армијата ќе воспостават стандардизирани процедури за известување и реакција при сајбер инциденти, кои што влијаат на одбранбените информатичките мрежи и инфраструктура, со кои ќе се дефинираат нивоата на ризик со цел донесување навремени одлуки и ефикасна координација помеѓу сите нивоа.

До 2030 година, се очекува функциите од суштинско значење за мисијата да имаат експлицитни барања за сајбер отпорност, мерките за континуитет да бидат дизајнирани и извежбани, а раководниот кадар на релевантните нивоа да ја разбираат врската помеѓу сајбер условите и нивниот простор за одлучување. Сајбер аспектите да бидат интегрирани во вежбите како оперативен фактор на притисок, а не како технички „додаток“.

5.2 Столб 2: Управување засновано на ризик и стратегиски надзор

Вториот столб структурно го интегрира планирањето водено согласно заканите, давањето на приоритети во справување со заканите и отчетноста. Управувањето мора во секој момент да одговори на три прашања: кои се ризици се критични при сајбер напад, кои мерки се преземаат и како се потврдува дека подготвеноста се подобрува.

Овој столб побарува воспоставување формална рамка за проценка на ризик од сајбер напад а поврзана со одбранбените мисии, јасни протоколи за ескалација и годишна стратегиска ревизија што ќе дава информација за развојот на способностите и буџетирањето. Ќе се применуваат мерливи индикатори на перформанси поврзани со исходите на мисијата, а не само со технички параметри.

Министерството за одбрана и Армијата ќе обезбедат одржливост на долгорочен план и оперативна способност на капацитетите за сајбер одбрана обезбедени преку национални инвестиции и придонеси од НАТО сојузниците и меѓународните партнери. Планирањето на одржливоста ќе ги опфати барањата за

менаџирање/управување со животниот циклус, вклучувајќи одржување, лиценцирање, техничка поддршка и обука на персоналот.

До 2030 година, сајбер ризикот ќе биде интегриран во циклусите на одбранбено планирање, набавките и известувањето за подготвеност. Централното координативно тело во доменот на сајбер одбраната ќе одржува рамка за зрелост и ќе обезбедува редовен надзор и отчетност.

5.3 Столб 3: Интероперабилност, стандарди и интеграција

Третиот столб ја усогласува поставеноста на сајбер одбраната во националните меѓународните рамки на соработка преку примена на релевантните меѓународни стандарди. Овој столб опфаќа усогласување со стандарди, механизми за безбедна размена на информации, учество во национални и сојузнички вежби и дисциплинирана цивилно-воена координација во согласност со националната рамка за управување со кризи.

До 2030 година, одбранбениот систем да биде способен сигурно и безбедно да разменува информации за закани со националните институции и меѓународните партнери и сојузници, да се интегрира во надворешни оперативни мрежи кога тоа е потребно и да учествува во заеднички активности за сајбер отпорност за валидација на сопствената цврстина и способност за закрепнување.

5.4 Столб 4: Човечки капитал и организациска отпорност

Четвртиот столб има за цел изградба на одржлива, професионална и адаптивна сајбер способност. Сајбер одбраната е пред сè човечки овозможена способност, поради тоа ќе се воспостават кариерни патеки, професионално образование усогласено со сојузнички програми, механизми за задржување на персоналот и структури за резервен капацитет. Развојот на сајбер резервен концепт ќе биде правно и оперативно уреден, со можност за редовно извежбање и предвидлива мобилизација.

Министерството за одбрана и Армијата ќе го поддржат развојот на сајбер персоналот преку јасно дефинирани улоги и одговорности, дефиниран професионален развој и континуирана обука на техничко ниво, усогласена со меѓународните и НАТО стандардите. Тоа вклучува напредни технички обуки од сајбер доменот, учество на сајбер вежби и обуки, и соработка со сојузниците со цел постигнување на оперативна интероперабилност.

До 2030 година, одбранбениот систем ќе одржува стабилен корпус на професионалци во управувачки, оперативни и валидни функции, со континуирана обука и капацитет за засилување во кризни услови.

6. Имплементација на стратегијата

Имплементацијата на оваа Стратегија ќе се спроведува преку дисциплиниран систем на управување, јасно дефинирани надлежности и мерлива одговорност. Подготвеноста за сајбер одбрана ќе се третира како составен дел од оперативната подготвеност на одбранбениот систем. Централното координативно тело во доменот на сајбер одбраната ќе обезбедува редовно и консолидирано известување до раководството за состојбата на подготвеноста, клучните ризици при имплементацијата и напредокот во развојот на способностите.

Доколку развојот на сајбер способностите ќе се реализира во услови на ограничени човечки и финансиски ресурси. Приоритет ќе имаат функциите од суштинско значење за мисијата и критичните зависности. Способноста ќе се гради преку професионализација, континуирана обука, задржување на кадарот и селективни партнерства, при што одговорноста за сајбер подготвеноста ќе биде вградена во целокупната структура на одбранбениот систем, а не ограничена на поединечна организациска единица.

Набавките и управувањето со ризик ќе претставуваат дел од клучните инструменти за обезбедување на отпорноста. Безбедносните барања ќе бидат интегрирани во спецификациите и животниот циклус на системите, а ризиците поврзани со наследени технологии, добавувачи и организациска поставеност ќе бидат предмет на континуиран надзор. Подготвеноста ќе се потврдува преку редовна евалуација и независни проценки, со можност за ревизија на Стратегијата доколку безбедносната средина или резултатите од имплементацијата тоа го наложат.

7. Заклучок

Стратегија за сајбер одбрана ја потврдува политичката намера и насоката за развој и имплементација на способности за сајбер одбрана во Министерството за одбрана и Армијата а се со цел обезбедување на оперативна способност во сајбер просторот во периодот 2026–2030 година. Истата се темели врз основа на неизбежната реалност а тоа е дека софистицираните непријателски активности ќе продолжат, а заканите во сајбер просторот сè почесто ќе се совпаѓаат со пошироки политичко-безбедносни кризи. Во такви услови, одвраќањето се остварува преку негирање, што подразбира обезбедување одбранбен систем што е отпорен, способен за закрепнување, интероперабилен и функционален дури и во услови на нарушување.

Стратегијата воспоставува три институционални обврски што го дефинираат успехот до 2030 година:

- Сајбер одбраната ќе се третира како услов за оперативна подготвеност, целосно интегриран во планирањето, вежбите и обезбедувањето на мисијата.
- Ќе се воспостави дисциплина во управувањето преку јасно дефинирана надлежност, мерлива подготвеност и континуирано известување, обезбедувајќи дека напредокот е видлив и предмет на отчетност.
- Изградба на отпорноста како системско својство, преку модернизирана и сегментирана инфраструктура, структурирана соработка со цивилните органи и доверливи партнери, како и професионален кадар структурно интегриран во кариерни патеки, а не во индивидуален ангажман.

Стратегијата за одбрана бара координација помеѓу воените и цивилните компоненти како предуслов за ефективна имплементација на одбраната. Оваа Стратегија за сајбер одбрана одговара на таа обврска во сајбер доменот преку јасно дефинирање на улогите, воспоставување координација без институционална нејасност и изградба на одбранбен систем способен да ја одржува подготвеноста во услови на активна сајбер закана.

Со имплементацијата на оваа Стратегија, Министерството за одбрана го зајакнува суверенитетот на Република Северна Македонија преку практичната способност да одлучува и дејствува под притисок, да ги исполнува националните одбранбени обврски и навремено и доверливо да придонесува во колективната одбрана преку обезбедување сигурност, интероперабилност и способност за закрепнување.

МИНИСТЕР ЗА ОДБРАНА

Владо Мисајловски