ИНФОРМАЦИОННАТА ВОЙНА МЕЖДУ УКРАЙНА И РУСИЯ

Петко Димов

THE INFORMATION WAR BETWEEN UKRAINE AND RUSSIA

Petko Dimov

Резюме: *Известно е, че информационната война се води за сърцата и умовете на три типа аудитория: собственото население, противниковото население и евентуалните съюзници. Затова в тази статия е направен опит да се разбере до колко двете страни са успели да направят това? За целта е направено изследване на нормативната дейност и предприетите законови действия в областта на информационната сфера и киберпространството, като са разгледани повече от 76693 нормативни документи издадени от правителствата на двете страни в периода 24.02.2022 г. до 13.08.2022 г. и публикувани в съответните държавни електронни бази данни. След което действията и на двете страни са анализирани от гледна точка на влиянието им над собствената, противниковата и съюзната аудитория и е направен сравнителен анализ на постигнатото до този момент.*

Ключови думи: *военна операция, война, Украйна.*

Abstract: *In an article, an attempt is made to understand to what extent the warring parties have been able to influence their own, opposing and allied audiences? For this purpose, a study of the normative activity and the legal actions taken in the field of the information sphere was carried out, and more than 76693 normative documents issued by the governments of the two countries in the period from 24.02.2022 to 13.08.2022 and published in the respective state electronic databases.*

Keywords: *operation , warfare, Ukraine.*

„Истината е първата жертва във войната“, тези думи са споменати за първи път на образователна конференция в защита на жените през август 1915 г. от Етел Анакин, съпруга на британския политик Филип Сноудън[1]. Днес те важат с пълна сила и в съвременната война между Русия и Украйна.

[1] **Annakin**, E. Woman and War by Mrs. Philip Snowden. Journal of Proceedings and Addresses of the Fifty-Third Annual Meeting and International Congress on Education, Held at Oakland, California, August 16-27, 1915

От началото на руско-украинския конфликт се наблюдават страхове, че това е началото на „Трета световна война“. Това, разбира се, е преувеличение, макар че в информационното пространство наистина може да се счита за „световна война“. Нейният обхват отиде далеч отвъд Русия и Украйна, като всъщност постепенно обхвана САЩ, НАТО, ЕС, Китай, редица корпорации, банки, международни институции, различни неправителствени организации и други отдалечени региони.

Известно е, че информационната война се води за „сърцата и умовете“ на три типа аудитория: *собственото население, противниковото население и евентуалните съюзници*. Затова в тази статия е направен опит да се разбере до колко двете страни са успели да обхванат трите типа аудитория?

За целта е направено изследване на нормативната дейност и предприетите законови действия в областта на информационната сфера и киберпространството, публикувани в съответните държавни електронни бази данни, като са разгледани повече от 76693 нормативни документи издадени от правителствата на двете страни в периода 24.02.2022 г. до 13.08.2022 г.

Методиката на изследването включва преглед на официалните правителствени бази данни с помощта на техните търсачки, след което намерените документи в областта на информационната сфера ръчно се преглеждат и анализират от гледана точка на влиянието им над собствената, противниковата и съюзната аудитории.

АНАЛИЗ НА ДЕЙСТВИЯТА НА УКРАЙНА В ИНФОРМАЦИОННАТА СФЕРА

Направено е изследване на нормативната дейност на Украйна след започване на бойните действия, като от портала на Държавната Рада (zakon.rada.gov.ua) са прегледани 2850 законови решения и постановления, подписани в периода от 24.02.22 г. до 13.08.2022 г., от който се констатира, че 49 имат връзка с практически действия в областта на информационната сфера.

Още преди войната са приети Стратегия за стратегическите комуникации, Стратегия за защита на информационната сигурност и Стратегия за киберсигурност[2], които своевременно се актуализират, точно преди войната с постановление № 447 от 14.05.2021 г.

Промените се управляват и със закони по време на войната, например „Закон за основните принципи на киберсигурността“ е влезнал в сила на 1.08.2022 г. С него се определят обектите от

https://books.google.bg/books?id=noEBAAAAYAAJ&q=%22first+casualty%22&redir_esc=y#v=snippet&

[2] Постановление на президента на Украйна от 15 март 2016 г. No 96/2016 за стратегията за киберсигурност на Украйна https://zakon.rada.gov.ua/laws/show/n0003525-16#Text

критичната информационна инфраструктура и изискванията към различните участници.

С други думи може да се каже, че украинците имат сравнително съвременна нормативна уредба в областта на киберсигурността, а в областта на информационната сигурност се налагат промени с влизане в сила на „Постановлението на президента за военно положение“, като например, предсрочното дипломиране на курсантите от Института за специална комуникация и информационна защита на Политехническия университет в Киев[3].

В опит да противодействат на масовите кибератаки в началото на войната от 08.03 с постановление 42 се заповядва на банките и държавните организации да съхраняват личните данни на своите потребители в облачни хранилища само в ЕС, Обединеното кралство, Съединените американски щати или Канада[4]. В тази връзка на 13.03 е приет Закон за гарантиране функционирането на информационните и комуникационните системи и публичните електронни регистри, който постановява да се създават резервни копия за съхранение, извън окупираните територии. На 15.03 е актуализиран и Наказателно-процесуалния кодекс за противодействие на кибератаките. Приет е Закона за електронните съобщения, като се променя „Процедурата за поддържане на регистър на доставчиците на електронни съобщителни мрежи и услуги“ и начините за тяхното сертифициране.

Едно от първите неща, с които се заема Министерството на цифровата трансформация на Украйна е да създаде електронен документ за самоличност през периода на военното положение (eDocument), който предоставя информация за лицето с помощта на мобилното приложение Diia, като това става автоматично, без присъствие на потребителя посредством „Единния държавен уеб портал за електронни услуги“.

На 19.03 е издадено Постановление 151 за неутрализирането на заплахите за информационната сигурност на държавата, като цифровите наземни радио и телевизионни съоръжения започват работа в денонощен режим от специално място в условия на война. Отчитайки пряката военна агресия от страна на Руската федерация, активното разпространение на дезинформацията от страна на агресивната държава, изкривяването на информацията, както и обосновката или отричането на въоръжената агресия на Руската федерация, бе издаден указ от 19 март 2022 г., № 152/2022 на президента на Украйна, относно прилагането на единна информационна политика съгласно военното право. Прилагането на единна информационна политика е приоритетен въпрос на националната сигурност, чието предоставяне се прилага чрез

[3] https://zakon.rada.gov.ua/laws/show/207-2022-%D1%80#Text
[4] https://zakon.rada.gov.ua/laws/show/v0042500-22#Text

комбиниране на всички национални телевизионни канали, чието програмно съдържание се състои главно от информация и аналитични програми на единна информационна платформа за стратегическа комуникация "United News #UAразом".

Всички дейности по отношение на събирането, обработката и разпространението на официални информационни продукти се предоставят на Украинската национална информационна агенция "Ukrinform", а по отношение на производството и излъчването на телевизионни и радиопрограми – на държавното предприятие "Мултимедийна платформа за международно радиоразпръскване на Украйна", като на последното се отпускат допълнително средства за създаване на телевизионен проект на руски език "Свобода". Създават се и две програми: "Развитие и модернизация на държавната система за специална комуникация и защита на информацията" и "Национална информационна програма" за осигуряване на защита и непрекъсната работа на Националната телекомуникационна мрежа и съоръжения от критична информационна инфраструктура – национални електронни информационни ресурси и държавни информационни и комуникационни системи.

Приет е закон за забрана на пропагандата на руския неонацистки тоталитарен режим, символите, използвани от въоръжените и други военни формации на Руската федерация във войната срещу Украйна.

От хронологията за приемане на нормативната уредба се вижда, че в началото на войната украинските власти са насочени предимно към подсигуряване на киберсигурността на електронното управление и защита на информационната сигурност на собствените граждани. В същото време са взети мерки за противодействие на дезинформацията и синхронизиране на съобщенията на медиите, както към собствената аудитория, така и към съюзниците.

Още в първите дни на конфликта, Украйна излъчи голям брой пропагандни продукти, които предизвикват силни емоции, с цел повишаване на патриотизма и морала на **собствената аудитория**. Съобщенията се излъчват по всички канали, като особено много се залага на интернет и социалните медии. Широко се използваха видеоклипове, плакати, анимирани изображения карикатури, вицове и вирусни съобщения в социалните мрежи, които залагат на героичния образ на украинските войници. Всички съобщения първоначално се одобряват и публикуват в официалните канали или на онлайн конференции, а в последствие се разпространяват в социални групи, Facebook, Twitter, Youtube и др. Не беше пропуснат и Телеграм, за който бяха създадени редица групи и приложения.

Онлайн пропагандата на Украйна до голяма степен се фокусира върху нейните герои и мъченици, които разказват за украинската

смелост или осмиващи анекдоти за руската глупост и агресия. Това е класически пример за съвременна пропаганда, която е от решаващо значение за наратива, че украинците се борят за справедлива кауза и ще спечелят тази война. Тези съобщения трябва да повлияят на сърцата и умовете на собствените им граждани. Това е особено важно в този конфликт, тъй като украинците се опитват да поддържат висок морал сред своите бойци и да съберат глобална подкрепа за своята кауза.

Пример за вирусно съобщение е случаят със Змийския остров. Според запис, публикуван от украинската медия „Правда“, настъпващите руски ВМС са дали ултиматум на 13 украински граничари да се предадат или да умрат, но украинците са ги напсували, преди да умрат. В последствие техните думи се превърнаха във вирусно съобщение в социалните мрежи, чрез аудио запис и видеоклип, който събра 3,5 милиона гледания в YouTube още на 24.02. Украинският президент Володимир Зеленски лично обяви смъртта им в друго видео, като каза, че всеки от тях ще бъде удостоен със званието Герой на Украйна. За съжаление, само няколко дни по-късно руснаците пуснаха клип, как същите тези войници са пленени, но живи, което беше потвърдено от украински официални лица във Facebook. Може да се каже, че това беше допустима пропагандна грешка, защото не трябва да се използва лъжа, но в случая със социалните мрежи беше по-важна бързината на разпространение на героичния образ.

В предишните войни противниковите сили се опитваха да нарушат вражеските комуникации, да ограничат разпространението на военновременна пропаганда и дори да прекъснат физическите комуникационни линии, като телеграфни кабели. В ерата на Интернет такива кабели са рядкост, затова целта на руснаците бяха комуникационните кули и прекъсването на достъпа до интернет. Съвременните средства включват кибератаки, вирусни съобщения и удавяне на противоположния разказ в море от съдържание на противника. Затова новите войни се развиват с главоломна скорост в социалните медии и официални уебсайтове, които се нуждаят от повече съдържание за разпространение на посланията от нашия разказ и удавяне на този на противника. Социалните медии се превърнаха в основен канал за прокарване на информация и технологичните компании могат да играят роля в информационната война, независимо дали са проверени или не.

Такъв пример от първите дни на войната беше разпространението на един специално изработен видеоклип в стил Холивуд с т.н. „Киевски призрак“, който разказва за оцелял от първите удари пилот, който сам е свалил няколко руски изтребителя. Първоначално Twitter го маркира „извън контекста“, тъй като имаше кадри взети от игра, но след като се появи в официален украински акаунт на Министерство на отбраната

стана вирусен и бързо се разпространи в Twitter, Facebook, Tik Tok и YouTube[5]. В последствие Snopes публикува статия, че това е фалшификат и въпреки, че има съобщения за няколко свалени руски самолети, няма такива, които да свързват това с киевския призрак. Има и редица други примери, в които украинската страна умело използваше изкуствен интелект за създаване на фалшиви клипове, вкарващи думи в устата на Путин, карикатури на руски танкове, носещи крадени тоалетни чинии или в бързината публикувани истории със съмнителна автентичност, които целяха объркване и осмиване на руснаците.

Украинските говорители с радост съобщаваха фактите, които посочват техни победи, но почти нищо не казват за украинските загуби или за движението на техните войски, което е класифицирано. Затова в нашите медии идва само информация от вторични източници, като сайта „Орикс“ и американския институт за изследване на войната, занимаващи се с анализ на сателитни снимки и от социалните медии.

От гледна точка на стратегията им за влияние над **съюзната аудитория** Украйна заложи на създаването на емоции предизвикващи тъга и съчувствие. С постоянно излъчвани клипове на Президента на Украйна беше създаден трагичен, мъченически образ на Володимир Зеленски, който се представяше като героична жертва, търсеща подкрепата на света. Тази емоция е твърде силна, а ефектът от нея е контрапродуктивен в дългосрочен план, но в началото те нямаше как да знаят, че войната ще се проточи.

Затова украинското правителство се обърна към западните социални медии, показвайки отлично разбиране на информационните технологии и съвременните маркетинг похвати. Например, в Twitter беше създадена инициативата "Hero Stickers", която да събира различни хакерски организации за извършване на кибератаки срещу Русия със забележителни резултати. Украйна многократно е публикувала онлайн обяви за набиране на цивилни хакери или доброволци и всички бяхме свидетели на публични искания за различни видове помощ от социалните платформи. В резултат на това много международни хакерски организации са отговорили и са участвали в руско-украинската информационна война. Най-голямата хакерска организация в света – „Анонимните“, осъществи редица атаки над руски правителствени сайтове, сред които беше и достъп до съхранявани лични данни в сайта на Министерство на отбраната на Руската федерация. Според китайски източници 27% от DDoS атаките над руските сайтове са стартирани в САЩ, което е малко вероятно да е

[5] **Shevtsov**, A., **Tzagkarakis**, C., **Antonakaki**, D., **Pratikakis**, P., **Ioannidis**, S. (2022). Twitter Dataset on the Russo-Ukrainian War. https://arxiv.org/abs/2204.08530

извършено от отделни хакери, а по-скоро е дело на организирана правителствена сила[6].

За да се опитат да прекъснат информационния поток в Украйна, руските сили бомбардираха комуникационните кули, прекъснаха украинските интернет услуги и се опитаха да блокират социалните медии. Затова още на 27 февруари, по искане на вицепремиера на Украйна, Илон Мъск обяви, откриването на StarLink за Украйна. StarLink предоставя 5G интернет услуги в недостъпни райони, чрез огромна мрежа от сателити, като към момента е извела около 3000 сателита, а в последствие те трябва да станат плътна мрежа от 12 000 сателита, разположени на много ниска орбита около Земята. Все още не е известно, какво е точната роля на тази система, но благодарение на нея се гарантира сигурната работа на Интернет в Украйна, защото руснаците все още не са намерили начин да я деактивират. Вероятно StarLink има и бойно използване от украинското разузнаване и военните щабове за комуникация в полеви условия. Все пак едно е сигурно, технологията 5G ще играе решаваща роля в следващите войни и със сигурност ще събуди интереса към космическите стратегии на различни страни.

В борбата за **противниковата аудитория** Въоръжените сили на Украйна започнаха да издирват контакти в социалните мрежи на близки на пленени и загинали руски войници и да се опитват да комуникират с тях, в опит да създадат масово недоволство срещу правителството. Един впечатляващ пример в тази област е сайтът "Проектът", който установява имената на руските командири на формирования, които взимат участие в специалната операция. "Проект" публикува база данни с информация за единиците на руската армия, участващи във войната, от коя област на страната идват, както и имената на командирите им. Специално подразделение хакери изследва биографиите на тези офицери и състоянието на военните части, които командват, издирва техни близки и прави опити да им влияе в социалните мрежи.

Публикуват се и разследвания, който подхранват стереотипите за руснаците. Според сайта „средният доход на командирите на дивизии през 2019 е бил 160 хиляди рубли (4599 лева по настоящият курс) и притежават един малък апартамент, 1/3 от офицерите имат ипотечни заеми, ¼ са имали пътни глоби, някои от които за употреба на алкохол“. Но трябва да имаме в предвид, че това е пропаганда, която има за цел да търси лоши примери на скандали за корупция в Интернет и други подобни простъпки, за да ги разгласява. Тактиката, която се използва е, че в официалните акаунти или новинарските издания се казва, че има

[6] https://zhuanlan.zhihu.com/p/486137021

такъв интересен сайт, което е истина, макар че в него има и манипулирано съдържание. Всичко това прави истината доста неуловима, с напредването на войната тези граници става още по-размити, както за Украйна, така и за Русия. Това е мъглата на войната.

С тези предварително създадени условия, украинският посланик в ООН Сергий Кислица сподели поредица от текстови съобщения, които според него са извлечени от мобилния телефон на мъртъв руски войник. „Мамо, аз съм в Украйна. Тук бушува истинска война. Ние бомбардираме всичко, независимо дали това са цивилни или военни“, пише руският войник, според разказа на г-н Кислица на руски език. Това съобщение се дава в подкрепа на твърдение, направено от официални лица и широко повтаряно в социалните медии, че руските войници са недостатъчно обучени и твърде млади. В крайна сметка това е специално създадена история предназначена за руската аудитория – особено за родители, които се тревожат за съдбата на своите деца. Това е вековна тактика, с която украинците се опитват да предизвикат масово недоволство и да отклонят противника от по-големи военни цели. Също с тази цел медиите показва десетки репортажи с руски военнопленници, някои с окървавени превръзки, увити около ръцете или лицата им. Във видеото се чува как пленените осъждат инвазията. Видеоклиповете може да повдигнат въпроси дали Украйна е нарушила Женевската конвенция, която регулира споделянето на изображения на военнопленници.

Не на последно място украинците се опитаха да приложат външен натиск върху всички възможни доставчици на интернет, облачни услуги, информационни и комуникационни технологии, с които работят руските правителствени сайтове.

Украйна отправи многократни искания в тази посока. Например, украинският министър на дигиталната трансформация в опити да ограничи руското влияние е молил „Internet Corporation for Assigned Names“ – ICANN за отмяна на SSL сертификатите за руски домейни. В последствие стана известно писмото, с което му отговарят, че тези сертификати се произвеждат от оператори на трети страни и ICANN не участва в издаването им. Въпреки това е явно, че с други големи компании са имали успех и успяха да създадат големи трудности на руските служби за информационна сигурност.

ИЗСЛЕДВАНЕ И АНАЛИЗ НА ДЕЙСТВИЯТА НА РУСКАТА ФЕДЕРАЦИЯ В ИНФОРМАЦИОННАТА СФЕРА

В търсачката на правителствения сайт publication.pravo.gov.ru при търсене на нормативни документи, подписани в периода 24.02.2022 г. до 13.08.2022 г. са намерени 73843 резултата на Руската дума, правителството и укази на Президента на Руската Федерация, от които

почти 70 касаещи сигурността в информационното и киберпространството.

От документите се вижда, че в опит да защити **собствената аудитория** Русия също засилва усилията за блокиране, ограничаване и контролиране на различните чуждестранни социални платформи и доставчици, опериращи на нейна територия. С указа на Президента се забранява ползването на чуждестранно осигуряване в обекти на критичната информационната инфраструктура[7].

Още със започване на войната вицепремиерът Дмитрий Чернишенко възлага на Министерството на цифровото развитие, комуникациите и масовите медии на Руската Федерация да подготви приоритетни мерки за защита на информационната инфраструктура на страната. В резултат предприетите мерки включват: отпускане на средства за подкрепа на IT индустрията, повишаване на заплатите на служителите в IT сектора, безвъзмездна подкрепа за обещаващи местни IT решения, преференциални заеми на IT компании за текуща дейност и изпълнение на нови проекти, 0% ставка на данъка върху общия доход в сектора, отсрочка от армията за IT специалисти, подкрепа за закупуване на критични местни IT разработки за държавни и общински нужди и други данъчни стимули и преференции за интернет компании и интегратори.

„Яндекс“, „Ростелеком“ и VK веднага обявиха, че предоставят своите публични „облаци“ за постигане на максимална скорост на държавните сайтове. Според изтекла правителствена телеграма, публикувана в Nexta, вицепремиерът е наредил на всички държавни уебсайтове и уеб услуги да преминат към руската система за имена на домейни .ru в срок до 11 март и да се премине към използването на DNS сървъри, намиращи се на територията на Русия, както и да се „усложни политиката при използването на пароли“[8]. Освен спиране на употребата на чуждестранния хостинг, беше издаден и указ с допълнителни мерки, които спират използването на броячи за посещаемост, инструменти за анализ и рекламни банери, предоставени от чуждестранни компании, като „Google Analytics“[9].

Още на деветия ден от войната „Държавната дума“ прие закон за наказание при разпространение на фалшиви новини, свързани с действията на руските въоръжени сили, в който се налага глоба от 700 хиляди до 1,5 милиона рубли или до 3 години затвор, а ако това е довело до сериозни последици - от 10 до 15 години затвор[10]. Също така,

[7] http://publication.pravo.gov.ru/Document/View/0001202203300001?index=0&rangeSize=1
[8] https://twitter.com/nexta_tv/status/1500553480548892679/photo/1
[9] Указ http://publication.pravo.gov.ru/Document/View/0001202205010023?index=3&rangeSize=1
[10] Уголовный кодекс Российской Федерации от 25.03.2022 http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891&ysclid=l6s7e4gnxa970611260

депутатите приеха изменения в Кодекса за административните престъпления относно отговорността за публичните действия, насочени към дискредитиране на използването на Въоръжените сили на Руската федерация, с цел защита на интересите на Руската федерация и нейните граждани, поддържане на международния мир и сигурност[11]. С други думи, не може всеки да разпространява, каквато си иска информация за събитията в Украйна, а само такава, която произлиза от официалните руски институции. Затова голяма част от уебсайтовете и блоговете просто мълчат по този въпрос, за да не сбъркат някъде и да бъдат глобени или вкарани в затвора.

На 06.03 е прието изменение в кодекса за административни нарушения, касаещо правилата за използване на спътникови мрежи за комуникация на чуждестранни организации от руски потребители. Нещо повече, в началото на третата седмица от войната, Главната прокуратура на Руската федерация поиска от съда да признае технологичната компания Meta за екстремистка организация и да забрани дейността им в Русия на основание член 280 и член 205.1 от Наказателния кодекс на Руската федерация за „публични призиви за извършване на екстремистки дейности и насърчаване на терористични дейности във Facebook и Instagram, както и заради това, че е дискриминирала държавни медии от 2020 г. насам. С това решение правителството блокира Facebook и Instagram, след което предложи на правителствените агенции да създават акаунти във вътрешните социални мрежи като RuTube (за видео), VK (клонинг на Facebook), Fiesta (като Instagram) и Telegram. Газпром Медия, също създаде един вид TikTok, наречен Yappy.

Google и YouTube преустановиха напълно продажбата на онлайн реклами в Русия, TikTok спря стриймовете на живо и публикуването на ново съдържание в страната[12]. Twitter обяви, че част от потребителите в Русия нямат достъп до социалната мрежа. Microsoft забрани продажбите към руски граждани, следвайки подобен ход на Apple. Блокирани бяха BBC, „Voice of America“, „Deutsche Welle“, Радио „Свободна Европа“. Независимото радио „Ехото на Москва“ беше свалено от ефир заради това, че продължаваше да нарича случващото се в Украйна „война“. Същата бе и съдбата на опозиционната телевизия „Дождь“ и украинската „Свобода“.

Всички тези действия вероятно ще затруднят по-голямата част от руските граждани да виждат противниковата гледна точка, но според скорошно проучване на Център „Левада“, почти една четвърт от

[11] https://realnoevremya.ru/articles/245500-hronologiya-voennoy-specoperacii-30-glavnyh-sobytiy-za-mesyac?

[12] https://boulevardbulgaria.bg/articles/rusiya-zapochna-aktivna-podgotovka-za-izklyuchvane-ot-globalniya-internet

анкетираните руски граждани използват VPN услуги за достъп до блокирани уебсайтове, като посочват точки за връзка извън Русия[13]. Този подход за постигане на „суверенен интернет“ е модернизиран опит от други страни, които имаха подобни действия преди време. През 2019 г. Иран се „изключи“ от глобалния Интернет за една седмица, докато правителството се бореше с вътрешни размирици. Китай от години държи гражданите си в капана на „Великата защитна стена“, която се характеризира с агресивно наблюдение и цензура.

Наложените ограничаване на достъпа до чуждестранни технологии и комуникационни платформи принуждава потребителите да разчитат на алтернативни и налични услуги от руски компании. Тези услуги са строго контролирани от руските власти, чрез агресивна цензура и наблюдение.

От началото на войната в Украйна руските потребители имаха значителни проблеми с достъпа до правителствени уебсайтове и онлайн банкови клиенти, защото браузърите започнаха да ги отбелязват като опасни. Причината е отмяната на сертификатите за цифрова сигурност от чуждестранните органи по сертифициране във връзка с горенаписаните молби на Украйна и наложените санкции на Русия. Освен това в условията на санкции има ограничения в ползваните платежните системи и руските сайтове могат просто да загубят способността да плащат за такива услуги.

Има няколко десетки организации в света, които имат цифрови главни сертификати, но 75% от тях се издават само от пет от най-големите компании, които се намират в САЩ[14]. По правило цифровите сертификати имат дървовидна структура: собственикът на главния сертификат може да даде правото и на други да издават дъщерни сертификати, но те трябва да са подписани от неговия главен сертификат. Именно този факт може да се използва за измама. Съвременните браузъри, не отварят сайтове, които не са защитени от сертификат и предоставят предупреждение за „опасна връзка“. За да не се случи това, сайтът трябва да има HTTPS, който осигурява комуникация между браузърите и уебсайтовете, като криптира комуникацията, за да не я четат или модифицират интернет доставчиците. Това е още по-необходимо, когато става въпрос за електронна поща, социални мрежи, онлайн банкиране и услуги на т.н. „електронно правителство“.

Именно поради тази причина Министерството на цифровото развитие, комуникациите и масовите медии на Руската федерация предлага собствен главен сертификат, от който се издават дъщерните

[13] https://www.levada.ru/en/2022/04/22/internet-social-networks-and-vpn/

[14] **Bougias**, A., **Episcopos**, A., **Leledakis**, G. Valuation of European firms during the Russia–Ukraine war, Economics Letters, Volume 218, 2022, ISSN 0165-1765, https://doi.org/10.1016/j.econlet.2022.110750

сертификати на обществените услуги. Тук проблемът е, че браузъри като Google Chrome, Apple Safari, Microsoft Edge и Mozilla не разпознават този сертификат. Затова руските потребителите или трябва ръчно да добавят руския сертификат към надеждния списък, или да преминат към руските браузърите на Yandex и Атом. Тъй като сертификатът е държавна собственост, инсталирането му е въпрос на доверие в органите. Обикновено, интернет доставчика или всяка друга страна нямат достъп до данните, които потребителят обменя със уеб страницата, но в този случай инсталираните държавни сертификати ще позволят на руското правителство при нужда да получи достъп до информация в нешифрована форма, от който и да е сайт. Например, при прихващане на HTTPS (атака „човек в средата“), противник в мрежата може да се представя за уеб сайт (напр. facebook.com) и представя собствен фалшив сертификат с публичния ключ на нападателя. Обикновено нападателят не може да получи никакъв легитимен сертификат за домейн, който нападателят не контролира, и така браузърите ще откриват и осуетят този вид атака. Ако обаче нападателят може да убеди потребителите да инсталират друг главен сертификат в браузърите си, те ще се доверят на фалшивия сертификат на нападателя. С тези фалшиви сертификати (или държавно издадени такива), нападателят (държавата) може да се представя за всеки уеб сайт и да записва това, което потребителите правят или публикуват на сайта. С оглед на горенаписаното бих препоръчал на руските граждани да ползват два браузъра един за интернет и един руски за достъп до електронното правителство, но това едва ли ще го направи по-голямата маса от хора. Средният руски гражданин буквално живее в друг свят и вижда това, което му позволи правителството в т.н. прозорец на Овертон.

Относно **противниковата аудитория,** стратегията на руснаците е комбинация от физическо въздействие, кибератаки, информационни и психологически операции, провеждани от предварително подготвени мощни формирования.

Сред първите цели във военната операция бяха основните елементи от медийната и комуникационната инфраструктура на Украйна. Доказателство за това е първият разрушен чрез диверсия обект – главния телевизионен ретранслатор в Източна Украйна. Впоследствие базовите станции на мобилните оператори бяха подложени на въздействия, както на диверсии и огневи удари, така и на хакерски атаки за кражби на данни, DDoS на важни портали и официални уебсайтове с ботнет мрежи от типа „Марай“ и заглушаване на сигнала от формированията за радиоелектронна борба (РЕБ)[15].

[15] https://postvai.com/analizi/hibridni-deistwia.html

Поради това на териториите на Крим и Източна Украйна почти не функционират украински мобилни оператори и не се приемат украински радиа и телевизии.

В киберпространството първоначално се събира информация, чрез фишинг, закупуване на компрометирани данни от хакерските форуми, атаки за достъп до адресни книги на пощенски сървъри. За проникване се използват типични техники на социалния инженеринг или директно проникване чрез софтуерни уязвимости в системите за управление. Следва вътрешно разпространяване на злонамерения код от типа „НотПетя“ и кражба на данни и тяхното предаване, чрез криптиран комуникационен софтуер от рода на Telegram Group API интерфейс или кражба на файлове с помощта на Robocopy, който ги копира в допълнителен облачен диск.

В информационното пространство на противника Кремъл, чрез пряко или непряко финансиране, създава дезинформационно съдържание, поддържа „фабрики от тролове“ и разпространява това съдържание координирано в социалните мрежи. Тези „тролове“ са най-често работещи от вкъщи хора, които създават и поддържат фалшиви (а напоследък и истински) профили, с които по команда споделят „новините“ в групи и страници, както и писане на коментари под новинарски статии[16]. Това, от своя страна, води до алгоритмично усилване на тези публикации (защото явно много хора се интересуват), като Фейсбук (и други социални мрежи) го показват на повече и повече хора. Същите тези тролове докладват популярни личности, които в случая пишат в подкрепа на Украйна, и неефективната система на модерация на Фейсбук, води до блокиране не на фалшивите новини, оправдаващи войната, а на легитимни гласове.

С цел провеждане на емпиричен експеримент за разпространение на фалшивите новини във Facebook бе създадена групата „Военни анализи“ чрез която се доказа, че технологичните компании не определят правилата за цялостна дезинформация, а само за конкретно поведение, конкретни участници и конкретно съдържание, докато модераторите на групи имат известна свобода да определят кое е непроверено или невярно съдържание. Макар тази свобода да е свързана с възможно лично наказание на администратора за дейността на цялата група, при това при условие, че алгоритъмът на Facebook по-често счита проруското съдържание за фалшиво.

Относно стратегията за влияние на **съюзната аудитория**, това което често не успява да бъде разбрано, е, че руската пропаганда, въпреки общоприетото убеждение, не е особено фокусирана върху западния свят. Русия е наясно, че в по-голямата си част хората тук са

[16] https://blog.bozho.net/blog/3907

враждебни към Русия и нищо няма да промени това. Но набирането на популярност в Африка и Азия, е постижима цел и това със сигурност е във фокуса на руските информационни и психологически операции. Например, ние може да видим новина за разлика в държанието към украинските и чернокожите бежанци, която да не ни въздейства, но тя да има значително въздействие в Индия или Африка[17]. Макар тази новина да няма отражение в Европа, страни като Нигерия може да имат различен поглед и да се възприемат като по-малко достойни от белите хора, които се опитват да избягат от Украйна[18].

Руската пропаганда обръща специално място на Китай, дори всички събития от бойните действия са придружени от репортажи на живо в екипите, на които са включени китайски журналисти и то на фона, че китайците не подкрепят разширяването на НАТО[19]. Carter Center China Focus предостави първото проучване проведено през април на китайското обществено мнение по отношение на нахлуването на Русия в Украйна. Резултатите показват, че 75% от анкетираните са съгласни, че подкрепата за Русия в Украйна е в националният интерес на Китай[20]. Но повече от 60% от респондентите подкрепят неутрална политика, чрез морална подкрепа, без доставяне на оръжие на Русия. По-специално само 16% от анкетираните подкрепят предоставянето на оръжия на Русия, само 3% повече от тези, които вярват, че Китай трябва да промени сегашния си курс и да осъди Руската инвазия. Нещо повече, говорителят на китайското външно министерство също многократно обвинява НАТО за това, че се е доближила твърде близо до границите на Русия.

Руснаците използват отношението на китайците, като обявяват конспирацията за американските био лаборатории в Украйна, като едно от основните оправдания за войната, като обвързват това със случилото се покрай Covid-19, което е в интерес на Китай.

В информационната война широко се използват телевизионни екипи с предварително подготвени репортажи или с цел провокация на позиционирани камери за заснемане на противника. С тази цел формированията се разполагат и водят огън от детски градини, училища и жилищни или обществени сгради. В рамките на 1 – 2 часа след събитието се излъчват репортажи, в които играят актьори. В този процес в Украйна масово участват руски телевизионни и

[17] https://www.axios.com/africans-in-ukraine-racism-81bf8ebd-2d03-4373-bdeb-b5de9db7ec91.html
[18] **Talabi**, F., **Aiyesimoju**, A., **Lamidi**, I., **Bello**, S., **Okunade**, J., **CUgwuoke**, C., **Gever**, V. The use of social media storytelling for help-seeking and help-receiving among Nigerian refugees of the Ukraine–Russia war, Telematics and Informatics, Volume 71, 2022, https://doi.org/10.1016/j.tele.2022.101836
[19] https://uscnpm.org/2022/04/28/oriana-skylar-mastro-russia-ukraine-china-interview/
[20] https://uscnpm.org/2022/04/19/chinese-public-opinion-war-in-ukraine/#:~:text=To%20our%20knowledge%2C%20this%20is%20the%20first%20representative,support%20China%20mediating%20an%20end%20to%20the%20conflict.

информационни агенции (НТВ, „Първи канал“, “Life News”, „24-и канал“, „Звезда“, РИА „Новости“, “Russia Today”, „Россия сегодня“, ИТАР-ТАСС и „Комсомольская правда“), а също Интернет издания и агенции (“Anna News” и “Life News”), за които се твърди, че са на ГРУ и ФСБ.

Една от основните цели на дезинформацията на Кремъл е да прехвърли вината за предполагаеми военни престъпления, извършени в Украйна. Например, когато на 8 април ракетен удар на руските въоръжени сили удари ЖП гарата в Краматорск, убивайки десетки невинни хора, бягащи от ужасите на войната, Русия обвини Украйна в атаката. Естествено това се използва и от другата страна.

Един от основните принципи в дезинформацията е отричане, обвинение, прехвърляне на вина и разсейване (отхвърляне – разколебаване – прехвърляне на вина). Пример за това са зверствата в Буча, първо се отхвърлят, след това започват да казват, че това са провокации, впоследствие прехвърлят вина и обвиняват Украйна, накрая за разсейване се пускат подобни садистични клипове, показващи украински мъчители на пленени руски войници.

Често използват операции чрез координиран имейл тролинг в Telegram Cyber Front Z, за който се твърди, че е свързан с „фермата за тролове“ която наводнява информационното пространство с фалшиви обвинения за военни престъпления, за които се твърди, че са извършени от украинските „неонацисти“, за да се удавят проукраинските гласове в морето от лъжи.

Основният наратив на руската пропаганда е, че те не се бият с украинският народ, а се опитват да го освободят от група неонацисти. Естествено Русия също има своя собствена форма на създаване на митове, но тя е далеч по-малко ефективна, тъй като руските държавни медии по закон трябва да наричат конфликта „специална военна операция“, а не война. Това и страха от импровизации им дава по-малко свобода за действие.

В крайна сметка руснаците на тяхна територия успяха да спрат прозападните медии и да защитят собствената си аудитория от чуждестранно влияние и кибератаки, печелят разбиране в Китай, но губят информационното пространство в западния свят и Украйна, въпреки че имат някои отделни успехи в киберпространството.

КИБЕРАТАКИ В ДРУГИ СТРАНИ И ВЛИЯНИЕТО ИМ В БЪЛГАРИЯ

След започване на войната зачестиха кибератаките над редица държавни портали в ЕС и САЩ, банки и оръжейни компании, като Локхийд Мартин (която доставя HIMARS на Украйна). Още на 28 февруари беше проведена атака срещу Google Chrome, а в Румъния беше хакнат сайта на Министерство на отбраната и други

правителствени сайтове. Атаката беше организирана от група проруски хакери, които са извършили атаки и срещу сайтове на институции в Естония, Полша, Чехия, както и срещу сайтове на НАТО. Във Швеция беше хакнат сайта на най-голямата банка в страната. Криптовирус атакува голям европейски газопровод, мрежа на енергийната компания „Creos“ беше атакувана от рансъмуера BlackCat/ALPHV. Отново беше пуснат вирус подобен на "NotPetya", който през 2017 г. засегна части от инфраструктурата на Украйна и повреди компютри в държави по целия свят. Със започване на войната, той отново се разпространи в редица европейски страни, в това число и в България.

На 4 април сървър на “Български пощи” е бил компрометиран и са инсталирани няколко инструмента за разгръщане на кибератака отвътре. Атаката, обаче, не е била активирана веднага, а просто чрез инсталираните инструменти е бил разпространен криптовирус върху избрани сървъри в информационния център на пощите и върху отделни компютри в много пощенски станции[21]. Използвани са специфични техники, за да се заобиколи и деактивира анти-вирусния софтуер. Криптовирусът е настроен така, че може да засяга всички държави без Русия и някои нейни съюзници. Той може да се активира при определена команда, която е подадена чак на 16 април при започване на изплащането на великденските надбавки, при което всички системи на “Български пощи” са поразени. Не може да се изпращат и получават пратки. Не може да се плащат сметки. Не може да се изплащат пенсии и великденски надбавки. Налага се помощ от външни експерти по киберсигурност, които почистват над 6600 засегнати компютъра и над 100 сървъра, системи и възстановяват бази данни от инфраструктурата на Държавния облак. След анализа констатират, че основния проблем е в липсата на дигитална грамотност на служителите и в морално остарялата материална база. Около 44% от компютрите са на възраст над 15 г. и работят със софтуер, извън всякаква възможност за поддръжка, който не може да бъде защитен със съвременни антивирусни решения. Инвестициите в информационна сигурност и защита на данните, са били системно неглижирани. По-късно на 20.04 хакери атакуваха сайта на Комисията по енергийни и водно регулиране (КЕВР), който временно е излязъл от строя.

Освен това България е обект на целенасочена пропаганда и мащабна дезинформация, особено в социалните мрежи. Това се дължи на липсата на държавен орган у нас, който да е натоварен официално с политиката за защита от хибридни заплахи или стратегическите комуникации, в т.ч. за борба с насочената дезинформация. От

[21] Официална страница на вицепремиера по ефективно управление Калина Константинова https://www.facebook.com/kalina.konstantinova.politician/posts/pfbid0kC4oF6t3WMGEbQFCmEqRevSubrCV3495gqubSxKz1ktW3C4goYtCjkbq6SszyYBQl

предишното правителство у нас беше създадено Министерство на електронното управление, което частично припознава някои от тези дейности[22]. Необходимо е да бъде създадено аналитично звено, което да следи за дезинформационни наративи и кампании и да информира своевременно заинтересованите страни, да координира обмен на информация между министерствата и да изучава добрите практики на други страни. Необходимо е да се провеждат повече курсове по медийна грамотност във всички звена на Държавна администрация и да се повиши дигиталната компетентност на нашето общество.

Изводи

На стратегическо ниво, борбата за общественото мнение в информационното пространство и защитата на критичната инфраструктура са от изключителна важност и имат потенциал за постигане на победа или загуба. Тази информационна война доказва безспорно на хората по цял свят, че социални медийни платформи могат успешно да бъдат използвани като много ефективно оръжия за масово поразяване. Именно затова критичната информационна инфраструктурата, заедно с държавните сайтове и социалните платформи следва да бъдат стратегически актив, също като дипломацията.

От хронологията за приемане на нормативната уредба в двете държави след започване на войната се вижда, че в началото те са насочени към подсигуряване на киберсигурността, но едно от първите неща за решаване е била защитата на електронното управление и удостоверяване на гражданите. На следващо място са взети мерки за противодействие на дезинформацията и синхронизиране на собствените медии, които са от изключителна важност за успеха на операцията.

5G сателитните технологии ще имат решаваща роля в бъдещите войни, особено ако се действа срещу по-силен противник с превъзходство във въздушно пространство. При малки и мобилни сухопътни формирования, тяхната роля е много по-важна от тази на дроновете и следва Българските въоръжени сили да инвестират в тази технология.

Войната показва, че обхватът на информационните операции отиде далеч отвъд Русия и Украйна. Той засегна целия свят. Всъщност, в тях участват също САЩ, НАТО, Китай, редица корпорации, големи

22 https://euractiv.bg/section/%d0%bf%d0%be%d0%bb%d0%b8%d1%82%d0%b8%d0%ba%d0%b0/news/%d0%b1%d1%8a%d0%bb%d0%b3%d0%b0%d1%80%d0%b8%d1%8f-%d0%bf%d1%80%d0%b0%d0%b2%d0%b8-%d0%be%d1%80%d0%b3%d0%b0%d0%bd-%d0%b7%d0%b0-%d0%b1%d0%be%d1%80%d0%b1%d0%b0-%d1%81-%d1%82%d1%80%d0%be%d0%bb%d0%be%d0%b2/

банки, неправителствени организации, международни институции и различни професионални и браншови организации и други несвързани страни и региони.

В крайна сметка, от настоящия анализ се вижда, че към настоящия момент Русия губи информационната война в западния свят и Украйна, но има пълен успех в самата Русия и печели разбирането на китайските граждани и други изолирани страни като Иран и Северна Корея. Има някои частични успехи в Азия и Африка, но това бързо може да се промени, защото западните сили имат много по-добър обхват на социалните платформи, като Facebook, Twitter, Instagram, YouTube, Google.

В крайна сметка този конфликт вече не е просто война между две страни и две армии. Това е формата на бъдеща война. Война зад войната.

ЛИТЕРАТУРА:

1. Блог на Божидар Божанов – Министър на Електронното управление https://blog.bozho.net/blog/3907

2. Официална страница на вицепремиера по ефективно управление Калина Константинова https://www.facebook.com/kalina.konstantinova.politician/posts/pfbid0kC4oF6t3WMGEbQFCmEqRevSubrCV3495gqubSxKz1ktW3C4goYtCjkbq6SszyYBQl

3. Постановление на президента на Украйна от 15 март 2016 г. No 96/2016 за стратегията за киберсигурност на Украйна https://zakon.rada.gov.ua/laws/show/n0003525-16#Text

4. Уголовный кодекс Российской Федерации от 25.03.2022 http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891&ysclid=l6s7e4gnxa970611260

5. Указ президента росийской федерации http://publication.pravo.gov.ru/Document/View/0001202205010023?index=3&rangeSize=1

6. **Annakin**, E. Woman and War by Mrs. Philip Snowden. Journal of Proceedings and Addresses of the Fifty-Third Annual Meeting and International Congress on Education, Held at Oakland, California, August 16-27, 1915 https://books.google.bg/books?id=noEBAAAAYAAJ&q=%22first+casualty%22&redir_esc=y#v=snippet&

7. **Bougias**, A., **Episcopos**, A., **Leledakis**, G. Valuation of European firms during the Russia–Ukraine war, Economics Letters, Volume 218, 2022, ISSN 0165-1765, https://doi.org/10.1016/j.econlet.2022.110750

8. **Shevtsov**, A., **Tzagkarakis**, C., **Antonakaki**, D., **Pratikakis**, P., **Ioannidis**, S. (2022). Twitter Dataset on the Russo-Ukrainian War. https://arxiv.org/abs/2204.08530

9. **Talabi**, F., **Aiyesimoju**, A., **Lamidi**, I., **Bello**, S., **Okunade**, J., **CUgwuoke**, C., **Gever**, V. The use of social media storytelling for help-seeking and help-receiving among Nigerian refugees of the Ukraine–Russia war, Telematics and Informatics, Volume 71, 2022, https://doi.org/10.1016/j.tele.2022.101836

10.http://publication.pravo.gov.ru/Document/View/0001202203300001?index=0&rangeSize=1

11. https://boulevardbulgaria.bg/articles/rusiya-zapochna-aktivna-podgotovka-za-izklyuchvane-ot-globalniya-internet

12. https://euractiv.bg/section/%d0%bf%d0%be%d0%bb%d0%b8%d1%82%d0%b8%d0%ba%d0%b0/news/%d0%b1%d1%8a%d0%bb%d0%b3%d0%b0%d1%80%d0%b8%d1%8f-%d0%bf%d1%80%d0%b0%d0%b2%d0%b8-%d0%be%d1%80%d0%b3%d0%b0%d0%bd-%d0%b7%d0%b0-%d0%b1%d0%be%d1%80%d0%b1%d0%b0-%d1%81-%d1%82%d1%80%d0%be%d0%bb%d0%be%d0%b2/

13. https://postvai.com/analizi/hibridni-deistwia.html

14. https://realnoevremya.ru/articles/245500-hronologiya-voennoy-specoperacii-30-glavnyh-sobytiy-za-mesyac

15. https://twitter.com/nexta_tv/status/1500553480548892679/photo/1

16. https://uscnpm.org/2022/04/19/chinese-public-opinion-war-in-ukraine/#:~:text=To%20our%20knowledge%2C%20this%20is%20the%20first%20representative,support%20China%20mediating%20an%20end%20to%20the%20conflict

17. https://uscnpm.org/2022/04/28/oriana-skylar-mastro-russia-ukraine-china-interview/

18. https://www.axios.com/africans-in-ukraine-racism-81bf8ebd-2d03-4373-bdeb-b5de9db7ec91.html

19. https://www.levada.ru/en/2022/04/22/internet-social-networks-and-vpn/

20. https://zakon.rada.gov.ua/laws/show/207-2022-%D1%80#Text

21. https://zakon.rada.gov.ua/laws/show/v0042500-22#Text
22. https://zhuanlan.zhihu.com/p/486137021