Գ Լ Ո Բ Ո Ւ Ս
Վերլուծական տեղեկագիր
ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ

Г Л О Б У С
Аналитический бюллетень
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

№ 2
Հունիս, 2008թ.

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

ՏԵՂԵԿԱՏՎԱԿԱՆ ՊԱՏԵՐԱԶՄՆԵՐԸ ԵՎ ԼՂՀ-Ն

Ակնհայտ է, որ ԼՂՀ տեղեկատվական անվտանգության *(ՏԱ)* հարցերն ունեն իրենց առանձնահատկությունը. օբյեկտիվ շատ ցուցանիշների առումով հայկական այս երկրորդ հանրապետությունը գտնվում է տեղեկատվական պատերազմի ճակատի առաջին գծում: Միևնույն ժամանակ, հարկ է ընդգծել, որ ԼՂՀ *ՏԱ* հիմնախնդիրները անհրաժեշտ է դիտարկել Հայաստանի (ՀՀ-ի, ԼՂՀ-ի և, տեղեկատվական տեսանկյունից՝ Ջավախքի) ու Հայության *ՏԱ* համակարգի համատեքստում: *ՏԱ* թվարկված սուբյեկտների առանձին, դիսկրետ ընկալումը մեթոդաբանորեն ճիշտ չէ և անարդյունավետ է:

Նշենք նաև, որ սույն աշխատանքում չեն քննարկվում կիբերտարածության (հաքերների գործողություններ և այլն) անվտանգության հետ կապված հարցերը: Սակայն հարկ է փաստել այն մեծ ակտիվությունը, որ ցուցաբերում են այսօր ադրբեջանական հատուկ կառույցներն այս ուղղությամբ: Համակարգչային խափանարարների նպատակը հաճախ պետական կառույցների պաշտոնյաների էլեկտրոնային գրագրությանը հետևելն է, որը Հայաստանում, ի տարբերություն շատ երկրների, չի գաղտնագրվում և փոխանցվում է բաց տեքստով[1]:

Առաջին սերնդի տեղեկատվական պատերազմները և ԼՂՀ-ն. Ընդունված է կարծել, թե տեղեկատվական հոսքերը լինում են երկու տեսակ.

1. Տեղեկատվության հոսքեր, որոնք ներկայացնում, լուսաբանում են մարդկության կենսագործունեության այս կամ այն ոլորտները և ձևավորում են գլոբալ տեղեկատվական դաշտը:
2. Նպատակաուղղված տեղեկատվական հոսքեր, որոնք նպատակ ունեն ազդել կոնկրետ հասցեատիրոջ ռազմաքաղաքական, սոցիալ-տնտեսական և հոգևոր-հոգեբանական վիճակի վրա:

Առաջին տեսակի տեղեկատվական հոսքերը, որպես կանոն, ընկալվում են որպես բնականոն երևույթ և առանձնապես չեն վերահսկվում հասարակության և պետության կողմից: Այնինչ, դրանք կարող են հայտնի սպառնալիք ներկայացնել, օրինակ, հասարակության (հատկապես ավանդական հասարակության) հոգեբանական և բարոյական վիճակի համար: Դրա հետ մեկտեղ, նման հոսքերը կարող են ստեղծել որոշակի տեղեկատվական-հոգեբանական ֆոն, որը կարող է օգտագործվել երկրորդ տեսակի՝ նպատակաուղղված տեղեկատվական հոսքերի հեղինակների կողմից: Այս համատեքստում ցանկացած հասարակության, մանավանդ այն հասարակության, որը գտնվում է ռազմաքաղաքական դիմակայության մեջ (իսկ նման կարգավիճակում է գտնվում ԼՂՀ-ն), տեղեկատվական դաշտը կարիք ունի փորձագիտական մոնիթորինգի և անհրաժեշտության դեպքում՝ կոռեկցիայի պետության և հասարակության կողմից տեղեկատվության «բովանդակային բալանսը» պահպանելու տեսանկյունից:

Երկրորդ տեսակի տեղեկատվական հոսքերը, որպես կանոն, համապատասխանում են դասական տեղեկատվական գործողությունների և տեղեկատվական պատերազմների սահմանմանը: Հայության և Հայաստանի ներգրավվածությունը մասշտաբային, որոշակի իմաստով՝ գլոբալ քաղաքական գործընթացներին, Ցեղասպանության և ԼՂՀ ճանաչման համատեքստում, ավտոմատ կերպով նրանց վերածում է նման պատերազմների սուբյեկտի: ԼՂՀ-ի պարագայում առավել ակնհայտ և հիմնական տեղեկատվական ագրեսոր պետք է համարել, իհարկե, Ադրբեջանի Հանրապետությունը և նրա դաշնակիցներին: Միևնույն ժամանակ, տեղեկատվական հոսքերի վերլուծությունից այնպիսի տպավորություն է ստեղծվում, թե տեղեկատվական պատերազմ ծավալած ադրբեջանական կառույցները որոշակի, մասնավորապես՝ մեթոդաբանական աջակցություն են ստանում թուրքական և Ադրբեջանի հետ դաշնակից այլ պետությունների մասնագետների կողմից: ԼՂՀ-ի դեմ տեղեկատվական գործողություններում չի բացառվում նաև այդ երկրում տեղակայված խոշոր էներգետիկական ընկերու-

[1] Տե՛ս սույն տեղեկագրի «Вопросы кибербезопасности Армении» հոդվածը:

թյունների փորձագետների մասնակցությունը: Այս հանգամանքը խիստ կարևոր է Ադրբեջանի տեղեկատվական ռեսուրսների ճիշտ գնահատման համար և առավել հանգամանալի ուսումնասիրության կարիք ունի:

ԼՂՀ-ի դեմ ուղղված տեղեկատվական հայտնի գործողությունների համախումբը կարելի է բնութագրել որպես առաջին սերնդի դասական տեղեկատվական պատերազմ, որը կոչված է լրացնելու այն գործողությունները, որոնք իրականացվում են Ադրբեջանի կողմից ռազմական, քաղաքական և տնտեսական ոլորտներում: Այս համատեքստում ադրբեջանական կողմի տեղեկատվական հոսքերը պայմանականորեն կարելի է բնութագրել երեք վեկտորներով, որոնցից մեկը ներքին է, մյուս երկուսը՝ արտաքին.

- Ներքին վեկտորն ուղղված է ադրբեջանական լսարանին և նպատակ է հետապնդում *հասարակության մեջ պահել Լեռնային Ղարաբաղի մասին հիշողությունը որպես Ադրբեջանի անքակտելի մաս և երիտասարդ սերնդին դաստիարակել ռազմատենչության, ռևանշի և հայատյացության ոգով:*
- Առաջին արտաքին վեկտորն ուղղված է ***հայ հանրության դեմ և հիմնականում իրագործվում է հոգեբանական պատերազմների ժանրով:*** Օրինակ, մատուցվում են էներգետիկական կամ էլ ֆինանսական ոլորտների ձեռքբերումները, դրանք հարաբերակցվում են սեփական ՋՈւ հզորացման և, համապատասխանաբար, ոչ միայն ԼՂՀ-ի, այլ նաև ՀՀ-ի նկատմամբ տարածքային հավակնությունների հետ:
- Երկրորդ արտաքին տեղեկատվական վեկտորն ուղղված է համաշխարհային հանրության տարբեր հատվածներին և նպատակ ունի ձևավորել «հայկական ագրեսիայից տուժած» Ադրբեջանի դրական իմիջը, և «սևացնել» այն ամենը, ինչ կապված է Հայաստանի ու Հայության հետ:

Բնականաբար, տեղեկատվական հոսքերի ներկայացված ուղղությունները հստակ սահմանազատում չունեն. դրանք հաճախ սինթեզվում և փոխլրացնում են միմյանց: Հարկ է ընդունել, որ իրենց տեղեկատվական գործողություններում ադրբեջանցիները հասել են որոշ հաջողությունների. ներկայումս նրանք օգտագործում են մի շարք քրեստոմատիական մեթոդիկաներ և տեխնոլոգիաներ[1]: Այնինչ, հայկական կողմը միշտ չէ, որ համարժեք է պատասխանում այդ մարտահրավերներին, իսկ ***պոստֆակտում*** ռեժիմով հերքումներն արդյունավետ չեն.այստեղ անհրաժեշտ է համակարգային մոտեցում:

Երկրորդ սերնդի տեղեկատվական պատերազմներ և ԼՂՀ. Միևնույն ժամանակ, մեր կարծիքով, ԼՂՀ-ի համար առավել վտանգավոր են այն տեղեկատվական գործողությունները, որոնք իրականացվում են *RAND* կորպորացիայի մասնագետների մշակած «երկրորդ սերնդի տեղեկատվական պատերազմների» հայեցակարգի հիման վրա: Նշենք, որ եթե առաջին սերնդի տեղեկատվական ագրեսիան դիտարկվում է որպես ավանդական պատերազմի ընդհանուր համատեքստում կիրառվող ինչ-որ կարևոր բաղադրիչ, ապա տեղեկատվական երկրորդ սերնդի պատերազմներն ինքնուրույն նշանակություն ունեն և սահմանվում են այն ստեղծողների կողմից՝ որպես ռազմավարական հակամարտության սկզբունքորեն նոր տեսակ, որ «կյանքի են կոչվում տեղեկատվական հեղափոխությամբ, որը հակամարտության հնարավոր ոլորտների շրջանակ է մտցնում տեղեկատվական տարածությունը և մի շարք այլ բնագավառներ (առաջին հերթին՝ տնտեսությունը) և ժամանակի մեջ ամիսներ ու տարիներ է տևում...»:

Այն խնդիրների շարքում, որոնք լուծվում են երկրորդ սերնդի տեղեկատվական պատերազմների օգնությամբ, մասնավորապես առանձնացնենք հետևյալները.

1. Հասարակական գիտակցության և երկրի բնակչության սոցիալական խմբերի քաղաքական կողմնորոշման մանիպուլյացիա՝ քաղաքական լարվածություն և քաոս ստեղծելու նպատակով:
2. Քաղաքական հարաբերությունների ապակայունացում կուսակցությունների, միավորումների և շարժումների միջև՝ կոնֆլիկտներ հրահրելու, անվստահություն, կասկածամտություն բորբոքելու, քաղաքական պայքարը սրելու նպատակով, ընդդիմության հանդեպ ճնշումների, փոխոչնչացման սադրանքներ:

[1] Տե՛ս սույն տեղեկագրի «Ադրբեջանական ՋԼՄ-ի կողմից կիրառվող տեղեկատվական գործողությունների տեխնոլոգիաները» հոդվածը:

3. Իշխանական մարմինների տեղեկատվական ապահովման մակարդակի նվազում, սխալ վարչական որոշումների մղող սադրանք, դժվարություններ կառավարման մարմինների կողմից կարևոր որոշումներ ընդունելիս։
4. Բնակչությանը ապատեղեկատվության տրամադրում պետական մարմինների աշխատանքի մասին, նրանց հեղինակազրկում, կառավարման մարմինների վարկաբեկում։
5. Պետության միջազգային հեղինակազրկում, այլ երկրների հետ համագործակցության խափանում։

Վերը թվարկվածից հետևում է, որ որոշակի իմաստով ՀՀ-ն և ԼՂՀ-ն արդեն ենթարկվում են «երկրորդ կարգի» տեղեկատվական հարձակման։ Նման պատերազմների առավել բնորոշ դրսևորումներ են այսպես կոչված «գունավոր հեղափոխությունները»։ Այդ հեղափոխության օրինակ են, մասնավորապես, այն գործընթացները, որոնք տեղի ունեցան վերջերս, ՀՀ-ում նախագահական ընտրությունների ընթացքում, և որոնք անմիջական առնչություն ունեն ԼՂՀ անվտանգության հետ։ Որոշ քաղաքական ուժեր, մասնավորապես, լայնորեն օգտագործեցին հետևյալ կարգախոսները.

- «Կորչի՛ ղարաբաղյան կլանը». սրանով իսկ որոշակի կենցաղային պատկերացումներ բարձրացվեցին քաղաքական մակարդակի, և փորձ արվեց այդ պատկերացումները տարածել «ղարաբաղցի» հասկացության վրա ընդհանրապես։ Այսպիսով, փաստորեն, ձգտում էին իրականացնել վերը նշված առաջին կետը՝ հասարակական գիտակցության և երկրի բնակչության սոցիալական խմբերի քաղաքական կողմնորոշման մանիպուլյացիան՝ քաղաքական լարվածություն և քաոս ստեղծելու նպատակով։
- «Չկարգավորված Ղարաբաղյան հակամարտությունը մեր բոլոր դժբախտությունների աղբյուրն է». սրանով, մասնավորապես, արմատավորվում էր առանց որևէ նախապայմանի՝ ազատագրված տարածքների հանձնման գաղափարը։

ՀՀ և ԼՂՀ տեղեկատվական ինտեգրման խնդիրները. Հարկ է ընդգծել, որ վերը բերված «գունավոր կարգախոսները» հասարակության մեջ որոշակի ռեզոնանս ստացան, և այս փաստը, մասնավորապես, ՀՀ և ԼՂՀ տեղեկատվական քաղաքականության ոլորտում թույլ տրված կոպիտ սխալների հետևանք էր։ Չնայած ռազմաքաղաքական և տնտեսական բնագավառներում երկու հանրապետությունների հաջող ինտեգրմանը, տեղեկատվական ինտեգրման մասին խոսելը դեռ վաղ է։ «Ղարաբաղյան շարժման» տարիներին ՀՀ հանրությունն ամենևին էլ վատ տեղեկացված չէր (նկատի ունենալով տեղեկատվության հաղորդման հանրահավաքային և մասնավոր աղբյուրները) ԼՂՀ իրավիճակի մասին։ Մինչդեռ այսօր տպավորություն է ստեղծվում, թե ԼՂՀ-ն գտնվում է «ռադիոլռության» գոտում, միայն միջազգային դիտորդների այցելությունների ժամանակ են հեռուստաալիքները, Ստեփանակերտի նախագահական նստավայրի ֆոնին, տրաֆարետ ռեպորտաժներ հաղորդում։ Այս կապակցությամբ նշենք, որ հիմնախնդիրն ընդհանուր է ամբողջ Հայաստանի համար. «սեփական թղթակիցների» խորհրդային համակարգը վերացավ, իսկ գլոբալացման դարաշրջանում գրեթե բոլոր տարածաշրջանները տեղեկատվական իմաստով հայտնվեցին միմյանցից մեկուսացված վիճակում։

Որոշ հետևություններ. Խիստ հրատապացել է ԼՂՀ *ՏՄ* հիմնախնդիրներով զբաղվող մասնագիտացված փորձագիտական կառույցի ստեղծումը։ Այն պետք է ՀՀ մասնագետների հետ համատեղ, աշխատանքներ իրականացնի հետևյալ ուղղություններով.

1. Ինֆոգեն սպառնալիքների դասակարգում, այն կենտրոնների բացահայտում, որոնք ԼՂՀ-ի դեմ տեղեկատվական գործողությունների մշակողներն են հանդիսանում, ինչպես նաև դրանց չեզոքացմանն ուղղված արդյունավետ և ասիմետրիկ մեթոդների մշակում։
2. Կանխարգելիչ և հարձակողական տեղեկատվական գործողությունների վարման մեթոդների մշակում։
3. ՀՀ – ԼՂՀ միասնական տեղեկատվական տարածության ձևավորմանն ուղղված ջանքերի գործադրում։

Գագիկ Հարությունյան
«Նորավանք» հիմնադրամ

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ АРМЕНИИ

С каждым годом Азербайджан все более укрепляет свои позиции на информационном фронте. Это связано с тем, что официальный Баку стал уделять этому вопросу большое внимание, а также финансы. В свою очередь Турция традиционно демонстрирует государственный подход к данному вопросу.

Безопасность армянского сегмента интернета

Азербайджанская сторона уже четыре года ведет активную войну против армянского сегмента интернета. Периодически к азербайджанцам присоединяются и турецкие хакеры. Так, в феврале 2007г. были взломаны сайты омбудсмена, агентства «Де Факто», тестируемый сайт Национальной статистической службы. Предупреждения, посланные владельцам сайтов, показали, что даже через много часов после случившегося там не заметили факта взлома. Прошлым летом азербайджанцы воспользовались отсутствием бдительности у армянского провайдера *«Web»* и взяли под контроль десятки сайтов из Армении, включая интернет-проекты агентства «Медиамакс», которые были размещены на сервере компании. В течение нескольких недель компания не исправляла своей оплошности, сваливая всю вину на владельцев сайтов. Фактически оказалось, что государственные структуры, ответственные за безопасность, никак не вмешались в ситуацию, и только постоянные жалобы в конечном итоге вынудили компанию через длительное время исправить пробелы в системе безопасности серверов. Пока что азербайджанцы довольствуются разрушением сайтов либо размещением антиармянской информации. Однако, если учитывать, что владельцы столь значимых сайтов не замечают фактов взлома, то это может позволить азербайджанцам в нужное время распространять заранее подготовленную дезинформацию непосредственно через армянские сайты.

Подобные случаи массированных атак на армянские сайты происходят по несколько раз в год. При этом нападения становятся все более профессиональными, с азербайджанской стороны вовлекается все больше человеческих и, разумеется, финансовых ресурсов, а объектами атак становятся все более значимые армянские сайты. Соответственно становится насущной проблемой защита не только государственных, но и вообще важных для Армении сайтов. Создается впечатление, частично подкрепленное фактами, что спецслужбы Азербайджана контролируют ряд хакерских групп, а нападения на армянские сайты осуществляются для выявления их слабых сторон, а уже не для простого вредительства. Таким образом, в Баку, вероятнее всего, готовят базу для того, чтобы в нужный момент постараться полностью обрушить армянский сегмент интернета. Для противостояния подобной угрозе, а также возможности массированной контратаки Армении должна обладать необходимыми подготовленными кадрами, а также разработанной стратегией действий.

Безопасность внутренних сетей

Взлом внутренней сети МИД Армении в декабре прошлого года стал логическим продолжением безалаберности армянской стороны и планомерной деятельности азербайджанской. Даже из открытых сообщений в прессе можно было бы сделать выводы о том, что в Азербайджане спецслужбы контролируют ряд хакерских групп, которые используются для атак против Армении.

Не менее серьезно стоит задача защиты электронной корреспонденции. Судя по всему, этому вопросу в нашей стране пока не уделяется должного внимания. Так, пресс-секретарь

Министерства обороны Армении уже долгие годы использует для рассылки пресс-релизов почту на российском бесплатном сервере mail.ru, взлом которого даже открыто рекламируется в интернете и стоит порядка $50. Нет никаких гарантий, что и в данный момент этот почтовый ящик не находится под негласным контролем азербайджанцев и не будет использован в удачное время в своих целях.

Совершенно очевидно, насколько серьезный урон может быть нанесен взломами электронной переписки высокопоставленных чиновников. В январе одному из армянских «интернет-бойцов» удалось полностью взять под свой контроль азербайджанский новостной сайт *Xronika.com*. Этот сайт азербайджанские спецслужбы удачно позиционировали как якобы армянский, готовя плацдарм для провокаций. После чего с этого сайта армянским пользователям рассылался вирус, предназначенный для воровства паролей с компьютеров. После взлом данного сайта оказалось, что его успешно использовали против Армении. Взлом почтового ящика *Xronika.com* выявил, что азербайджанцы получили доступ к электронной переписке нескольких сотен армянских пользователей, включая внутреннюю переписку между армянскими посольствами (в частности, Казахстана), высокопоставленными чиновниками, аналитического центра «Митк». Кроме того, у азербайджанцев в руках оказалось множество писем с отсканированными армянскими паспортами, переписка армянского офицера-гея со своим «другом» и т.д., что, естественно, давало азербайджанским спецслужбам поле для маневра. Надо учитывать, что *Xronika.com* является лишь одним из плацдармов информационной войны против Армении и неизвестно, сколько еще подобных сайтов контролируется Азербайджаном[1].

В целом, должна существовать единая стратегия защиты государственных внутренних сетей, систем электронного документооборота. Особенно с учетом того, что в стране все больше внедряются системы электронного правительства, опасность несанкционированного доступа к системам усиливается. Не менее важной является защита негосударственных коммерческих сетей стратегического значения, например, связанных с энергосистемами, уязвимость которых может привести к катастрофическим последствиям.

Пропаганда

Практически никаких действий, направленных против азербайджанской и турецкой пропаганды, с армянской стороны не предпринимается. Основные действия в этом направлении предпринимаются со стороны армян из Армении и диаспоры, которые действуют из личного патриотизма и энтузиазма. Например, действия против дезинформации азербайджанских СМИ о том, что армяне Львова требуют переименовать город в «Арьюц», были предприняты исключительно со стороны армянского интернет-сообщества, которому удалось вынудить большинство украинских СМИ убрать этот материал с интернет-сайтов. В то время как в Азербайджане и Турции такими вопросами масштабно занимаются государственные структуры. При этом с армянской стороны небольшой штат специалистов мог бы проводить мониторинг азербайджанской агитации и дезинформации, проводя ответные мероприятия. С учетом наличия большого количества армян, вовлеченных в информационную войну на частном уровне, подобная структура могла бы, вовлекая их, эффективно и с минимальными затратами добиться успеха на этом фронте.

В армянской прессе постоянно идет рекламирование азербайджанских и турецких СМИ, в особенности, представленных в интернете. В целом можно сказать, что по статистике армянское телевидение и газеты больше рекламируют азербайджанские сетевые ресурсы, нежели отечественные. Более того, армянские СМИ без проверки перепечатывают турецкую и азербайджанскую дезинформацию, тем самым тиражируя ее среди армянской аудитории. Не говоря о

[1] Полученные сведения были переданы сотруднику Службы нацбезопасности. Однако абсолютно никакого отголоска это не получило – из СНБ даже не поинтересовались, каким образом был взломан сайт и т.д.

том, что зачастую азербайджанские новости просто копируются, сохраняя такие термины, как «карабахские сепаратисты», в кавычках используются слова «геноцид», «НКР» и т.д.

Кроме того, нет даже общего похода работы с государственной символикой. В армянских СМИ постоянно идет пропаганда государственной символики Азербайджана и Турции в самом выгодном свете. В то же время, в армянской прессе даже нет единого подхода к изображению карты НКР. Чаще всего армянский зритель видит на телеэкране бывший НКАО, не связанный с Арменией. То, что в стране не обращают внимания на такие «мелочи», является симптомом отсутствия понимания важности государственного подхода как к внутренней, так и к внешней пропаганде.

На внутреннем рынке, в свою очередь, полностью отсутствует государственный подход – местные СМИ практически не освещают жизнь в Нагорном Карабахе, регионах Армении, хотя при осознании важности задачи любое издание должно было бы иметь свои корпункты в Степанакерте, а также в региональных центрах. Фактически, в интернете существует только одно карабахское агентство *Karabakh-Open.com*, которое информирует о событиях в НКР оперативно. При этом другие армянские СМИ практически не обращают внимание на этот ресурс, продолжая черпать информацию из азербайджанских источников.

Создалась парадоксальная ситуация, когда для большинства армян основным источником информации в интернете является азербайджанский информационный портал *Day.az*, который по параметрам посещаемости и цитируемости превосходит все аналогичные армянские ресурсы вместе взятые. Стоит отметить, что в период «чрезвычайного положения» *Day.az* пользовался особой популярностью среди армян, так как умело агрегировал новости из Армении из всех источников, как официальных, так и оппозиционных, чего не смогло сделать ни одно армянское издание.

Заключение

При сохранении нынешней тенденции в ближайшее время Армения полностью потеряет инициативу в информационной войне против Азербайджана и Турции. Становится жизненно необходимым создание межведомственного органа, координирующим информационную деятельность СНБ, МИД, МО и других ведомств для противодействия и, главное, инициативных действий в этом направлении.

Самвел Мартиросян

ԱԴՐԲԵՋԱՆԱԿԱՆ ԶԼՄ-Ի ԿՈՂՄԻՑ ԿԻՐԱՌՎՈՂ ՏԵՂԵԿԱՏՎԱԿԱՆ ԳՈՐԾՈՂՈՒԹՅՈՒՆՆԵՐԻ ՏԵԽՆՈԼՈԳԻԱՆԵՐԸ

Հոդվածում ներկայացնում ենք ադրբեջանական լրատվամիջոցներում առկա տեղեկատվական գործողությունները, որոնք դասակարգվել են ըստ հիմնական ուղղությունների, և որոնց տրվել են պայմանական անվանումներ: Հիմնական շեշտադրումն այն է, որ Հայաստանի դեմ տարվում է լրջորեն նախապատրաստված, հեռանկարային տեղեկատվական պատերազմ, որը չի զիջում և նույնիսկ ավելի վտանգավոր է բաց ռազմական գործողություններից:

1. «Առաջնայնության գործոն». Այս սկզբունքի նախահայր կարելի է համարել նացիստական Գերմանիայի ակնառու դեմքերից մեկին՝ դոկտոր Գեբելսին: «Այն մարդը, ով կասի աշխարհին առաջին բառը, միշտ ճիշտ է», ասում էր նա[1]: Նույն եզրակացության են եկել մի շարք գիտնականներ, այդ թվում նաև Կ.Հովլանդը, Ն.Ջանիսը, Լ.Դոուբը և այլք: Քարոզչի հաջողությունն ապահովված է, եթե իր տեղեկատվությունն ավելի շուտ է հասել հասարակությանը, քան նրա հակառակորդինը,- համոզված են նրանք: Դա հիմնավորվում է նրանով, որ մարդիկ գերադասում են հավատալ սկզբնական տեղեկատվությանը, և փոխել արդեն ստեղծված կարծիքն այս կամ այլ հարցի վերաբերյալ՝ շատ դժվար է[2]: Հիտլերը պնդում էր, որ հասարակությունը հակված է հավատալու նույնիսկ 90% չապացուցված մեղադրանքին, քան դրա հերքմանը, եթե դա նույնիսկ հիմնավորված է 100%-ով[3]: Ադրբեջանական մամուլը, կիրառելով այս սկզբունքը, փորձում է ակնհայտորեն օգտագործել իր, Հայաստանի ինչպես նաև համաշխարհային հասարակության կարծիքը փոխելու նպատակով: Ուշագրավ են ադրբեջանական մամուլում զինադադարի խախտման դեպքերի մասին հայտարարությունները, որոնք սկսել են կրել ամենօրյա բնույթ: Եթե հետևենք այդ հաղորդագրություններին, ապա անցյալ տարի գրեթե ամեն օր հայկական կողմը խախտում էր զինադադարը մեկ կամ երկու ուղղություններով: Անցյալ տարվա վերջից խախտումների մասշտաբն աստիճանաբար մեծացավ. այսօր հայկական կողմը խախտում է զինադադարն ամեն օր արդեն 4–5 ուղղություններով: Այս կեղծ հաղորդագրություններն համաշխարհային հասարակության կողմից ընդունվում են որպես իրական, ինչի ապացույցն է Եվրախորհրդի, ԵԱՀԿ, Եվրամիության, ԱՄՆ բարձրաստիճան ղեկավարության մտահոգությունը զինադադարի խախտման հաճախականության առիթով: Այսինքն՝ կեղծ քարոզչությունը միանշանակ օգուտ է բերում է հարևան երկրին՝ հավաստելով նրա «խաղաղասեր էությունը» և հավատարմությունը խաղաղության պահպանման պարտավորությանը: Մինչդեռ հայկական կողմը, եռամսյակը մեկ հայտարարելով «հարևանների» կողմից զինադադարի խախտման վերաբերյալ, ինչպես նաև հազվադեպ արձագանքելով կեղծ զինադադարի խախտման հայտարարություններին, ձեռք է բերում «զինադադարը խախտողի» կարգավիճակ, ինչն իր հերթին բացասաբար է անդրադառնում Հայաստանի միջազգային վարկանիշի և Ղարաբաղի հիմնախնդրի վրա: Եթե դրան գումարենք տարբեր միջազգային կազմակերպություններում ադրբեջանական կողմի ակտիվությունը, որի արդյունքն է նաև վերջերս ընդունված ՄԱԿ Գլխավոր ասամբլեայի A/62/L.42[4] որոշումը, որտեղ պետությունները (37 կողմ, 7 դեմ և 150 ձեռնպահ) ցույց տվեցին իրենց վերաբերմունքը Լեռնային Ղարաբաղի հիմնահարցին, ապա ակնհայտորեն տեսնում ենք նման քարոզչության արդյունքները:

---

[1] *Суровов В.,* Ледокол-**2**, Мн., 2004, стр. 167.

[2] *Грачев Г., Мельник И.,* Манипулирование личностью, М., 2003, стр. 200.

[3] Live Journal, 27 Novemer, 2007 http://realtymen.livejournal.com/638520.html

[4] http://www.un.org/ga/62/agenda/ps.shtml

2. «Փոխհրումային և անանուն հրումային համակարգ». Ընդունված է, որ տեղեկատվության վերաբերյալ որևէ հեղինակությանը կատարված հրումը մեծ ազդեցություն է թողնում հասարակության վրա: Այդ հեղինակությունը կարող է լինել կրոնական, քաղաքական գործիչ, գիտության կամ այլ ոլորտի մասնագետ: Միաժամանակ, ավելի համոզիչ լինելու համար կարող են օգտագործվել փաստաթղթերի մեկնաբանություններ, մասնագետների գնահատականներ կամ այլ հաշվետվություններ: Օրինակ, 2008թ. մարտի 28-ին *Day.az* տեղեկատվական գործակալությունը հայտնեց, որ մի խումբ հայեր, որոնց ինքնությունը չի հաջողվել պարզել, ավազակային հարձակում են գործել Բենիլյուքսի՝ Ռոտերդամում գտնվող Ադրբեջանական կոնգրեսի գրասենյակի վրա: Ոստիկանությունը և վկաները հաստատել են, որ այդ հարձակումը կատարվել է հայերի կողմից: Այս գործակալությունը հիմք է ընդունել մեկ այլ ադրբեջանական գործակալության (*ANS* գործակալությունը) հաղորդագրությունը, որտեղ, արդեն առանց որևէ հղման, ներկայացվել էր կատարվածը: Ի՞նչ ոստիկաններ, ի՞նչ վկաներ, ի՞նչ հայերից կազմված խումբ: Միևնույն ժամանակ, տեղեկատվության աղբյուրը չի պարզվել, իսկ լրագրողները ոչ մի պատասխանատվություն չեն կրել կեղծ տեղեկատվություն տարածելու համար: Հարկ է նաև նշել, որ նման տեղեկատվությունը հիմնականում կեղծ է: Իսկ հրումները գոյություն չունեցող հեղինակություններին այդ տեղեկատվությունն էլ ավելի հիմնավորված և համոզիչ են դարձնում հասարակության աչքում: 2008թ. հունվարի 28-ին Day.az գործակալությունը հայտարարել էր, թե իբր Ուկրաինայի Լվով քաղաքի հայկական համայնքն առաջարկել է անվանափոխել քաղաքն «Առյուծ»-ով՝ ի հիշատակ Լվով քաղաքի հայ հիմնադիրների[1]: Գործակալությունը հիմք էր ընդունել մեկ այլ ադրբեջանական գործակալության *(APA)* հայտարարությունը, որն ընդհանրապես չէր հիմնավորել այդ տեղեկությունը:

3. «Միջնորդներ» կամ «հայտնի մասնագետներ». Հայտնի է, որ արդյունավետ տեղեկատվական ազդեցությունն իրականացվում է հասարակության կողմից ճանաչված և հեղինակավոր մարդկանց միջոցով: Ոչ պաշտոնական տեղեկությունները՝ լուրերը, տարբեր ոլորտների մասնագետների գնահատականները, կրոնական առաջնորդների կարծիքները, ավելի նշանակալի են, քան այս կամ այն պետական կառույցի պաշտոնական տեղեկությունները: Այսպիսով, ցանկացած պետական դիրքորոշում հնարավոր է հասցնել հասարակությանը՝ ցանկալի արդյունքի հասնելու նպատակով: Ադրբեջանական մամուլը, ունենալով մի քանի նման մասնագետներ և առաջնորդներ, հաջողությամբ օգտագործում է այս գործոնը: Ներկայացնենք մի քանի օրինակներ: Ադրբեջանական մամուլում, հատկապես Day.az գործակալության ներկայացրած հարցազրույցները, վերցվում են միայն «հայտնի» մասնագետներից: Այս սկզբունքը մեծ դեր է խաղում հասարակական կարծիք ստեղծելու գործում: Այսպիսով, 2006թ. մարտի 14-ին մի անհայտ ադրբեջանցի «քաղաքագետ»՝ Վուգար Սեիդով, հայտնվեց ադրբեջանական մամուլում իր «պատմաքաղաքական վերլուծական» հոդվածով[2]: Մի քանի ամիս անց նույն անձը արդեն ներկայացվում է որպես «հայտնի քաղաքագետ Հունգարիայից»[3]: Մասնագետների շարքում է նաև հանրաճանաչ Վաֆա Գուլուզադեն, որը ժամանակ առ ժամանակ հայտնվում է մամուլում ինչ-որ կարևոր մեկնաբանություններով: Ադրբեջանցի «հայտնի» քաղաքագետների շարքը կարելի է շարունակել անվերջ, քանի որ ներկայացված գործոնը մեծ նշանակություն ունի տեղեկատվական պատերազմ վարելու ոլորտում:

4. «Հասկացությունների աղավաղում և դասակարգում». Ըստ հոգեբան Գ.Օլպորտի, յուրաքանչյուր լեզվի էությունն այն անվերջ տեղեկատվական հոսքի դասակարգման և բաշխման մեջ է, որին մենք ամեն վայրկյան հանդիպում ենք: Երբ ինչ-որ առարկա ենք նկարագրում, մենք ընդգծում ենք դրա յուրահատկությունը՝ ուշադրություն չդարձնելով այլ առանձնահատկություններին, ինչպես է այն նկարագրվում կամ դասակարգվում, դրա ներկայացման

[1] Day.az, http://www.day.az/news/armenia/105833.html

[2] Day.az, http://www.day.az/news/politics/73454.html

[3] http://www.day.az/news/politics/90865.html

ոճին, որոնք ուղղորդում են մեր մտքերը և զգացմունքային ընկալումը[1]: Նման դասակարգման արդյունքում ներկայացվող առարկաները կամ դեպքերը այնպես են ձևավորվում, որ քաղաքացին ընդունում է այդ քարոզչական իրավիճակի պարտադրված նկարագրումը: Այդ դասակարգումն իր էությամբ ընդգրկում է հատուկ փոխկապակցված բառեր յուրաքանչյուր տեղեկատվական հաղորդման համար: Դրանք բառեր և բառակապակցություններ են սեփական, «դրական» և կառուցողական դիրքորոշումը ներկայացնելու համար: Դրանք նաև տարբերակող բառեր են՝ թշնամուն բացասական ներկայացնելու համար: Գնահատենք այս գործոնն ադրբեջանական ՋԼՄ համատեքստում:

Ադրբեջանական *Day.az, ANS, Trend* և «*Зеркало*» գործակալությունները, ցանկանալով բարձրացնել իրենց զինված ուժերի ոգին, Հայաստանի զինված ուժերը ներկայացնում են որպես «Հայկական զինված ուժեր» կամ նույնիսկ «Հայկական զինված ստորաբաժանումներ»՝ իրենց ստորաբաժանումներն անվանելով «Ադրբեջանի ազգային բանակ»[2]: Միջադեպերը շփման եզրում ներկայացվում են այնպիսի ձևաչափով, որ նույնիսկ երեխայի համար դրա քարոզչական բնույթն ակնհայտ է[3]: Մեկ այլ օրինակ, որը ցույց է տալիս հարևան երկրի «կողմ» լինելը Ղարաբաղյան հիմնահարցի խաղաղ կարգավորմանը. «Հայաստանի ոչ կառուցողական դիրքորոշումը խոչընդոտում է հակամարտության խաղաղ կարգավորմանը»[4]: Բազմաթիվ են տնտեսական «աննախադեպ աճի» կամ այլ հաջողությունների (տնտեսական, քաղաքական, մարզական) վերաբերյալ համեմատությունները Հայաստանի նվաճումների հետ, որոնցում յուրաքանչյուր հնարավորություն օգտագործվում է՝ ցուցադրելու համար իրենց «առավելությունը»:

5. «Փաստերի շարադրանք». Մարդկանց մեծ մասը մտածում է կարծրատիպերով: Խոսքը «Ծուխն առանց կրակի չի լինում» կամ «Եթե այդ բանի մասին խոսում են, ուրեմն ինչ-որ բան կա» ասացվածքների մասին է: Արդյունքում՝ այլ կերպ մտածող մարդկանց մեջ փոքրամասնություն լինելու արհեստական տպավորություն է ստեղծվում: Նման քարոզչությունը հիմնականում կատարվում է սոցիոլոգիական հետազոտությունների կամ հեղինակավոր անձանց օժանդակությամբ, ինչը նվազեցնում է ընկալման քննադատությունը, քանի որ մարդիկ դժվար են ըմբռնում իրենց երկրում և աշխարհում տեղի ունեցածի մասին հայտարարությունների հետևում եղած կեղծ տեղեկատվությունը: Օրինակ, 2006թ. մարտի 25-ին *Day.az* գործակալությունը տարածեց տեղեկատվություն հասարակական հարցման արդյունքների մասին, ըստ որի՝ ընտրողների 72.2%-ը սատարում է ներկա նախագահին: Հետաքրքիրն այն է, որ տեղեկատվության մեջ ներկայացված են հետազոտությունը կատարող հասարակական կենտրոնի անվանումը և մի քանի թվեր՝ առանց որևէ հղման և մեթոդաբանական բացատրության[5]: 2007թ. հուլիսի 17-ին մեկ ուրիշ կազմակերպության հետազոտության արդյունքները հայտնվեցին նույն կայքում: Նույն ձեռագրով ներկայացված տեղեկատվությունը ոչնչով չէր տարբերվում մեկ տարի առաջվա հետազոտությունից: Հատկանշական է, որ նույնիսկ արդյունքների տոկոսային փոփոխություն տեղի չէր ունեցել, իսկ ներկայացված տեղեկատվության ողջ իմաստը ներկա նախագահին փառաբանելն ու մեծարելն էր առաջիկա նախագահական ընտրությունների շեմին[6]: Ինչ վերաբերում է այս գործոնի հակահայկական թեմատիկային, ապա վառ օրինակ է 2005թ. նոյեմբերի 3-ի տեղեկատվությունը Day.az կայքում[7], որտեղ ադրբեջանական այսպես կոչված «Ղարաբաղի ազատագրման կազմակերպությունը» կատարել

---

[1] *Арансон Э., Пратканис Э. Р.,* Эпоха пропаганды: механизмы убеждения, повседневное использование и злоупотребление, 2003. стр. 91.

[2] Армянские вооруженные формирования нарушили режим прекращения огня в Товузском, Физулинском и Агдамском районах, http://www.day.az/news/politics/103120.html , Вооруженные силы Армении обстреляли позиции Национальной армии Азербайджана, http://www.day.az/news/politics/102942.html

[3] ANS, ANS Специальный Репортаж / 13.03.2008 01:06 «Жизнь под пулями» http://www.ans.az/nid63762.html

[4] Day.az, http://www.day.az/news/politics/107744.html

[5] Day.az, http://www.day.az/news/politics/44744.html

[6] Day.az ,http://www.day.az/news/politics/86100.html

[7] Day.az, http://www.day.az/news/politics/34414.html

էր հասարակական հետազոտություն: Կարելի է պատկերացնել, թե ինչ ուղղվածություն ունի այդ հետազոտությունը: Նշենք միայն, որ այս «հետազոտության» իմաստը հասարակությանը Ղարաբաղի հիմնահարցի կարգավորման իրենց ցանկացած ձևաչափը ներկայացնելն է:

6. «Հետադարձ կապ». Այս գործոնին վերաբերող միջոցառումների առանձնահատկություններից են բարձրաստիճան անձանց մտերմիկ զրույցները փողոցներում, այցերը շրջաններ, ուղիղ կապի միջոցով հասարակության և ԶԼՄ-ի հետ հաղորդակցվելը: Հաճախ նման շփումները կազմակերպված թատրոնի բնույթ են կրում: Հայտնի է, օրինակ, որ Ֆրանսիայի նախագահ դը Գոլը երբևէ հարց չի ստացել, որին նախօրոք պատրաստված չի եղել: Ընդհանրապես, յուրաքանչյուր առաջնորդի աշխատակազմը պատրաստում է իր ղեկավարին հնարավոր հարցերին: Իսկ ի՞նչ է կատարվում Ադրբեջանում: Ադրբեջանական մամուլը լուսաբանում է իր առաջնորդի բազմաթիվ այցերը շրջաններ, որտեղ հիմնական հարցերը և պատասխանները կենտրոնացած են ադրբեջանական ռազմական հաջողությունների և ռազմական ուղիով տարածքների «ազատագրման» վրա: Նույն ոգով են աշխատում խորհրդարանի ներկայացուցիչները՝ տարբեր երկրներում հակահայկական քարոզչություն տանելով: Այսպիսով, խաղարկվում է տեղեկատվական պատերազմի այս գործոնը, ցույց է տրվում նախագահի և այլ բարձրաստիճան այրերի մտահոգությունը հասարակության, հատկապես հեռավոր շրջանների բնակիչների նկատմամբ, պատրաստակամությունը՝ տարածքներն ամեն գնով վերադարձնելու գործում: Դրա վառ օրինակ է հարևան երկրի նախագահի վերջերս կատարած այցը հարավարևմտյան շրջաններ: ANS գործակալության ներկայացրած տեղեկատվության համաձայն՝ նախագահին այցելել էր այդ շրջան բժշկական կենտրոնի և ՋԷԿ-ի բացման արարողությանը մասնակցելու նպատակով: Սակայն ներկայացվածն ամբողջությամբ վերաբերում է Հայաստանի կողմից «գրավված տարածքներին», դրանց ազատագրման առաջնայնությանը, ինչպես նաև դրա արդյունքում հազարավոր փախստականների առկայության հարցերին[1]: Միջազգային կազմակերպություններում ադրբեջանական ներկայացուցիչների, ինչպես նաև այլ երկրներ պետական այրերի այցելություններին վերաբերող հայտարարությունները և դրանց լուսաբանումը տեղական մամուլում չեն տարբերվում նրանց տարած աշխատանքից երկրի ներսում: *Trend News* գործակալությունը հարցազրույց էր վերցրել Ադրբեջանի արտաքին գործերի նախարար Է.Մամեդյարովից՝ Լատվիա կատարած այցի ժամանակ: Սակայն այդ այցի վերաբերյալ մանրամասներին տեղեկացնելու փոխարեն՝ լրագրողն անդրադառնում է Հայաստանի ԱԳ նախարարի հետ հնարավոր հանդիպմանը և իր ակնկալիքներին: Արդյունքում՝ հոդվածում, ինչպես միշտ, նշվում է Հայաստանի «ոչ կառուցողական» դիրքի, միջազգային հանրության դիրքորոշման և Ղարաբաղի հիմնահարցի վերաբերյալ Ադրբեջանի անհանդուրժողականության մասին: Այսպիսով, կարող ենք եզրակացնել, որ հարևան երկրի բարձրաստիճան այրերի այցը և, ընդհանրապես, նրանց հետադարձ կապը հասարակության հետ նպատակ են հետապնդում զգոն պահել հասարակությանը և հիշեցնել «Հայաստանի կողմից տարված» ռազմական գործողությունների վերաբերյալ՝ դրանով իսկ ապահովելով իրենց ազգանվեր աշխատանքի դիմաց ընտրություններին ակնկալվող ձայների առկայությունը:

7. «Պատմության վերագրառում». Այս գործոնն օգտագործվում է ապագա սերնդի ձևավորման և ցանկալի գաղափարախոսության սերմանման նպատակով: Արհեստականորեն ձևավորված պատմական իրականությունը փոխանցվում է գրքերի, դասախոսությունների, ռադիո և հեռուստատեսության, ԶԼՄ-ի, թատերական ներկայացումների, գեղարվեստական ֆիլմերի օգնությամբ: Օգտագործելով այս ամբողջ ռեսուրսը՝ կառուցվում է վիրտուալ աշխարհ, որն ընկալվում է որպես իրական: Արդյունքում՝ մարդն իր իրական կյանքը կարող է ընդունել որպես տհաճ երազ, իսկ այն ամենը, ինչը քարոզվում է, որպես իրականություն: Անգլիացի կինոռեժիսոր Քեն Լոխը նշել է. «Կարևոր է, որ պատմությունը մենք գրենք, որով-

[1] ANS, http://www.ans.az/index.php?nid=69311

հետև նա, ով գրում է պատմությունը, կառավարում է ներկան»[1]: Պատմության վերափոխմամբ հնարավորություն է ընձեռվում ներազդել լայն զանգվածների հիշողության վրա: Այս առումով ադրբեջանական քարոզչությունը հասել է աննախադեպ արդյունքների: Պատմական կեղծիքներն անհամեմատ շատ են, հնչում են անհեթեթ հայտարարություններ: Երկրի ողջ տարածքում կատարվում են պատմամշակութային հետազոտություններ, հայտնագործությունները վերագրվում են ադրբեջանական «հնագույն պատմությանը»: Ոտնձգությունների են ենթարկվում ոչ միայն հայկական հարուստ մշակույթը և հայոց պատմությունը, այլև պարսկական ու վրացական մշակույթները նույնպես: Այս ամենը կատարվում է պետության օժանդակությամբ և ադրբեջանցի «գիտնականների» մասնակցությամբ:

Այսպիսով, տեղեկատվական պատերազմի գործոնների առկայությունն ադրբեջանական մամուլում հաստատում է այն փաստը, որ Ադրբեջանում տարվում է լուրջ, լայնածավալ և երկարաժամկետ տեղեկատվական պատերազմ ընդդեմ Հայաստանի: Մեր երկրի մամուլը գրեթե չի անդրադառնում այս խնդրին՝ դրանք կասեցնելու կամ հակահարված տալու նպատակով: Ժամանակ առ ժամանակ հայտնվում են ադրբեջանական մամուլի այս կամ այն տեղեկատվության հերքումներ: Սակայն, հաշվի առնելով տեղեկատվության տարածման ծավալները և ինտենսիվությունը, Հայաստանն ակնհայտորեն պարտություն է կրում: Դա ազդում է նաև Հայաստանի միջազգային վարկանիշի վրա, ինչը լուրջ հետևանքների կհանգեցնի ապագայում: Տարանջատելով ադրբեջանական և թուրքական հակահայկական տեղեկատվական գործողությունները՝ կարող ենք նշել, որ առաջինի ռազմավարությունը հասցեագրված է ադրբեջանական հասարակությանը՝ ընդդեմ Հայաստանի: Թուրքիայի վարած տեղեկատվական պատերազմն ընդամենը տարբերվում է նրանով, որ հասցեագրված է Հայաստանի և Ադրբեջանի հասարակություններին՝ ընդդեմ Հայաստանի: Սակայն վերջինի ռազմավարությունը և օգտագործվող գործոնները մեկ այլ հետազոտության առարկա են:

Սուրեն Մովսիսյան
«Նորավանք» հիմնադրամ

[1] *Кара-Мурза С.Г.,* “Манипуляция сознанием”, М., 2006, стр. 201.

О НЕКОТОРЫХ АСПЕКТАХ ИНФОРМАЦИОННОЙ УЯЗВИМОСТИ АЗЕРБАЙДЖАНА

5 мая в интернете появился материал «Азербайджанцы помогут Грузии?», согласно которому авиарейс Баку-Кабул открывается для того, чтобы обеспечить доставку афганских моджахедов, которые должны будут воевать на грузинской стороне против Абхазии в случае, если начнется война. Кроме того, в материале шла речь о том, что среди азербайджанских общин идет рекрутирование наемников для абхазской войны, а также могут быть задействованы заключенные из азербайджанских тюрем, которых отпустят по амнистии.

Материал (полностью приведен в приложении) был размещен на сайте по адресу http://realazer.at.ua, который был озаглавлен «Реальный Азербайджан». Несмотря на то, что материал содержал определенные известные факты, однако для внимательного взгляда было ясно, что это откровенная дезинформация. Кроме того, сайт http://realazer.at.ua размещен на бесплатном хостинге, что сразу должно было навести на подозрения о том, что за этим не стоит сколько-нибудь серьезная организация, а тем более сетевое издание, так как в мировой практике это вообще не принято. Однако статья была запущена в сеть в удачный момент – когда ситуация вокруг Абхазии максимально накалилась и интерес к теме был на пике.

После этого статья была максимально популяризирована через армянские форумы и интернет-дневники. За этим последовала перепечатка на сайте армянского агентства *Panarmenian.net*. В результате массированного размещения материала на армянских ресурсах за день сайт «Реальный Азербайджан» посетило более тысячи человек, около 80% из которых были из России, на втором месте по посещаемости шел Азербайджан. Одновременно неармянская аудитория интернет-дневников, на которых был размещен материал, также превысил несколько тысяч посетителей.

Столь агрессивное распространение в сети дезинформационного материала скандального содержания привело к тому, что не выдержали нервы у основного азербайджанского интернет-издания *Day.az*, на котором была размещена не менее скандальная статья с опровержением информации, которая попала с ложного «Реального Азербайджана» на *Panarmenian.net*. Заголовок статьи «О вреде высасывания из пальца и иных частей тела, или очередной бред сивой кобылы от агентства “ПанАрмениан”« Акпера Гасанова чрезмерно привлекал внимание. При этом в статье был полностью процитирован дезинформационный материал. После этого последовали друг за другом опровержения пресс-секретаря МИД Азербайджана, бывшего работника настоящего издания «Реальный Азербайджан» и т.д.

В результате азербайджанская сторона сама забила новостные потоки опровержениями дезинформации, чрезмерно привлекая к ней внимание. Это в свою очередь вызвало обратную реакцию – в российских новостных агентствах незамедлительно последовали отголоски. За этим последовала вторая волна – новость о возможном участии азербайджанцев в войне против Абхазии и, соответственно, русских начала распространяться в неармянских интернет-дневниках (русских, украинских, северокавказских), причем с большим количеством посетителей.

Третья волна последовала через несколько дней – дезинформация стала появляться уже в аналитических материалах в российских изданиях. Так, газета «Сегодня» уже 13 мая напечатала материал с заголовком «В России готова активизироваться пятая колонна. Кто грозит началом борьбы в России и переброской афганских душманов в Грузию», которая практически полностью основана на материале «Азербайджанцы помогут Грузии?». Также в «Московском комсомольце» появилась статья «Грузия нашла, чем ответить России» и т.д.

Мониторинг азербайджанских форумов показал, что большинство пользователей интернета не знало о том, что сайт настоящей газеты «Реальный Азербайджан» уже год как не су-

ществует. Что само по себе показывает уязвимость азербайджанского общества перед возможными махинациями с ложными сайтами.

Таким образом, на данный момент азербайджанская пропаганда проявляет чрезмерную чувствительность к дезинформации, тем самым работая против себя. Одной из проблем азербайджанского информационного фронта является чрезмерное увлечение дезинформацией – агентства практически ежедневно вбрасывают материалы ложного содержания. Столь большой поток, с одной стороны, имеет для Азербайджана положительный аспект – с большой долей вероятности какие-то материалы все же попадают в цель. С другой стороны, плотность столь высока, что азербайджанцы сами забивают потоки. И, кроме того, увлечение дезинформацией приводит к чрезмерной настороженности и рефлективной реакции на любую проармянскую публикацию. В случае с ложным «Реальным Азербайджаном» наиболее эффективным стало раскручивание темы именно с азербайджанской стороны. Несмотря на то, что небольшое внимание к деталям и тактически верный подход должны были бы заставить азербайджанскую сторону проигнорировать вброс дезинформации, и в этом случае эффект был бы минимальным. В случае более продуманной и растянутой во времени акции с армянской стороны информационный ущерб для Азербайджана мог бы быть намного сильнее.

Самвел Мартиросян

Приложение

Азербайджанцы помогут Грузии?

По оценкам политологов последние заявления президента Грузии Михаила Саакашвили о том, что «в планы Грузии входит не война, а создание достойной и благополучной жизни для всех жителей страны», выглядят скорее как последнее предупреждение руководителям сепаратистских режимов Абхазии и Южной Осетии, нежели о реальных планах президента.

«Большая агрессивная сила» пошла ва-банк и практически не оставила шансов на мирное урегулирование конфликтов на территории Грузии. Судя по всему, ее руководство не очень надеется на пользу международного давления на Россию и пытается найти «понимание» у своего восточного соседа, с которым у Грузии тесные политические и экономические связи.

По поступающей информации именно Азербайджан намерен оказать Грузии «посильную» помощь в решении ее территориальных проблем. В частности, скоро намечается возобновление авиарейсов Баку-Кабул, прерванных в конце марта этого года. Ожидается переброска в Азербайджан, а далее в Грузию, больших партий оружия и групп афганских моджахедов, прошедших подготовку под руководством английских инструкторов в секретных лагерях на территории Афганистана.

Информация о наличии таких лагерей стала известна после того, как разразился скандал из-за попавших в руки афганских спецслужб материалов о деятельности британских спецслужб в стране. В этих лагерях предполагалось «взрастить» 1800 солдат и 200 представителей младшего командного звена бывших моджахедов. Британцы говорят, что обращенные талибы должны помочь бороться с боевиками, а затем вернуться к мирной жизни. Афганцы же предполагают, что Великобритания создает военно-тренировочные лагеря довольно неясного назначения.

По предварительным оценкам специалистов, в Грузию может быть переброшено около 500 афганских «командос», обученных в британских лагерях.

Ожидается, что в операции против Абхазии, а в дальнейшем и против Южной Осетии, будет использовано оружие, полученное афганцами от своих английских спонсоров, что одновременно позволит не «засветиться» властям Азербайджана.

Также из достоверных источников стало известно, что уже около месяца идет активная вербовка среди азербайджанцев России, Киргизии, Узбекистана, Украины и ряда других стран, имеющих многочисленную азербайджанскую диаспору.

В процессе вербовки принимают самое активное участие руководители азербайджанских диаспор, а именно Председатель *Azerbaycan Diasporasi* Фикрет Велиев, председатель мурманского отделения Всероссийского азербайджанского конгресса Рафик Бадиров, президент Федеральной национально-культурной автономии азербайджанцев в России Саюн Садыков. Сообщается, что вербовка проходит не только среди рядовых членов азербайджанской диаспоры, но и среди студентов ряда московских и киевских вузов.

Координация работы азербайджанских диаспор поручена заведующему сектором политических исследований Администрации Президента Азербайджана Фуаду Ахундову и начальнику управления планирования внешней политики и стратегических исследований МИД Азербайджана Тофику Мусаеву.

О поддержке Грузии в своем недавнем интервью *Day.az* заявил также известный политолог и дипломат Фикрет Садыхов: «Скажем откровенно, Азербайджан самим фактом необходимости выбора в данном вопросе, поставлен в довольно сложное положение. Но какие бы у Азербайджана ни были добрососедские отношения с Россией, в данном конфликте наша страна должна встать на сторону Грузии.

Ибо Грузия является нашим стратегическим партнером и страной, через территорию которой проходят газопровод и трубопровод, доставляющие азербайджанские углеводороды на европейский рынок. Кроме того, Грузия всегда с пониманием относилась к проблемам Азербайджана, к борьбе с армянским сепаратизмом. Стало быть, у Азербайджана просто нет выбора, и он обязан будет поддержать Грузию в момент серьезного напряжения грузино-российских отношений».

Примечателен еще один факт. На днях уполномоченная по правам человека в Азербайджане, омбудсман Эльмира Сулейманова обратилась в Милли Меджлис с просьбой принять решение об

амнистии. Однако есть информация, что право на амнистию получат еще и те заключенные, не подпадающие по закону под помилование, которые согласятся на отправку в регион грузино-абхазского противостояния. Официально же амнистию предлагается приурочить к 85-летию со дня рождения общенационального лидера Гейдара Алиева, 15-летию со Дня национального спасения и 90-летию формирования Азербайджанской Демократической Республики и первого парламента.

Предполагается, что на свободу выйдет от полутора до двух тысяч заключённых, совершивших тяжкие преступления, половину из которых, а именно около одной тысячи человек, предполагается перебросить в Грузию.

Процесс формирования азербайджанских отрядов особенно активизировался после того, как грузинскую государственную границу пересекли российская бронетехника, тяжелая артиллерия и дополнительные воинские подразделения, численность которых в Абхазии только по официальным данным составила около 3000 человек.

ԱԴՐԲԵՋԱՆԱԿԱՆ «ՍՓՅՈՒՌՔԻ» ՔԱՐՈԶՉԱԿԱՆ ՁԵՌՆԱՐԿՆԵՐԸ

Արտասահմանյան պետություններում աստիճանաբար «արմատակալող» ադրբեջանական համայնքային կազմակերպությունները չեն թաքցնում, որ իրենց հիմնական խնդիրներից է նաև Հայաստանի դեմ քարոզչական ակտիվ աշխատանք իրականացնելը և, ադրբեջանական կողմի բնութագրմամբ, «աշխարհին Ադրբեջանի վերաբերյալ ճշմարտությունը» հասցնելը: 2006թ. մարտի 16-ին Բաքվում, Աշխարհի ադրբեջանցիների 2-րդ համաժողովին, Իլհամ Ալիևը նշեց. «Չնայած Ադրբեջանը հակամարտության մեջ տուժած կողմ է հանդիսանում, աշխարհում Ադրբեջանի հակամարտության վերաբերյալ թյուրըմբռնում կա, որը հայկական սփյուռքի քարոզչության արդյունքն է»: Ավելի ուշ Ի.Ալիևը հայտարարեց «Հայաստանի վրա բոլոր ուղղություններով, այդ թվում նաև տեղեկատվական դաշտում, գրոհելու ծրագրի մասին» (տե՛ս www.day.az, 22.06.2007):

Ադրբեջանական տեղեկատվական ագրեսիայի գործին կցվել է նաև «սփյուռքը»: Արտասահմանում հիմնադրվում են ադրբեջանական զանգվածային լրատվամիջոցներ՝ թերթեր, կայքեր, ամսագրեր, հրատարակվում, տարածվում է գրականություն: Առանցքում Ղարաբաղյան հիմնախնդիրն է, Ադրբեջանը, համայնքը ներկայացվում են դրական լույսի ներքո, կան պատմական, մշակութային բնույթի հոդվածներ, հարցազրույցներ համայնքային գործիչների հետ: Հայկական թեմատիկային չվերաբերող հրատարակությունները ևս առնչություն ունեն հայկական կողմի շահեր հետ, քանի որ նման քարոզչությամբ Ադրբեջանը լուծում է արտասահմանում բնակվող հայրենակիցներին Ադրբեջանի հետ կապելու, ազգային համախմբվածություն ապահովելու հիմնախնդիրներ:

Արտերկրի ադրբեջանական ԶԼՄ-ից, թերևս, առաջնահերթ պետք է նշել ադրբեջանական «Եվրոխաբար» («Euroxeber») թերթի մասին, որի առաջին համարը լույս է տեսել 2004թ. հուլիսի 11-ին: Շնորհանդեսը տեղի է ունեցել Բաքվի մամուլի ակումբում: Պաշտոնապես նշվում է, որ թերթն ունի մոտ 4 հազար տպաքանակ, ինչը, հնարավոր է, որոշ չափով չափազանցված ցուցանիշ է: Թերթը տարածվում է ԵՄ պետությունների ադրբեջանական համայնքներին, ուղարկվում է ԵՄ, Եվրախորհրդի, ԵԱՀԿ պաշտոնյաներին, ԵՄ պետությունների օրենսդիրներին: «Եվրոխաբարն» ունի նաև կայք՝ www.euroxeber.com:

Թերթը հրատարակում է 2000թ. Բրյուսելում հիմնադրված «Ադրբեջանական տուն» կազմակերպությունը, որի հիմնադիրն է Գյուրջամ Բյուլենթ Ֆերմանօղլուն: Նա կարող է բնութագրվել որպես ԵՄ-ում ադրբեջանական «սփյուռքի» ամենաակտիվ գործիչներից մեկը: Ծնվել է 1962թ. Իգդիրում: Ի դեպ, Ֆերմանօղլուները սերում են Հայաստանի Արմավիրի մարզի Ջանֆիդա գյուղից: Գյուրջամ Բյուլենթ Ֆերմանօղլուի ծնողները 1930-ականներին Հայաստանից փոխադրվել են Թուրքիա: 1980թ. Ֆերմանօղլուն հաստատվել է Բրյուսելում, աշխատել որպես թուրքական «Հյուրիեթ» և «Թերջյուման» թերթերի թղթակից: 1987թ. հիմնադրել է թյուրքալեզու «Գյուրբեթ» թերթը, որը Բելգիայում առաջին թյուրքալեզու տպագիր օրգանն էր: 1995թ. Բրյուսելում Ադրբեջանի դեսպանատան հիմնադրումից հետո 5 տարի աշխատել է դեսպանատանը, ապա, 2000թ., բացել «Ադրբեջանական տունը», ինչից կարելի է հետևություն անել, որ աշխատանքն արվել է Բաքվի «պետպատվերի» շրջանակում:

Ջանֆիդայից սերող լոբբիստը 2003-ից Խոջալիի դեպքերի տարելիցի օրերին հրապարակում է «Ջենոսայդ» հատորյակը:

Այս գործիչը ներկա է եղել նաև Բուդապեշտում Ռամիլ Սաֆարովի դատավարության նիստերին, այս թեմայով ադրբեջանական ԶԼՄ-ին տեղեկատվություն փոխանցող հիմնական լրագրողն է եղել:

Մոսկվայում լույս են տեսնում 2 ռուսալեզու ծավալուն թերթեր՝ «Ազեռռոս» և «Ազերբայջանսկի կոնգրես»: Հրատարակիչներն են ՌԴ-ում 2 խոշորագույն՝ «Ազեռռոս» (Ռուսաստանի ադրբեջանցիների դաշնային ազգային մշակութային ինքնավարություն) և «Համառուսաստա-

նյան ադրբեջանական կոնգրես» (Всеройссийский азербайджанский конгресс - ВАК) ադրբեջանական լոբբիստական կազմակերպությունները:

«Ազեռռոսը», չնայած Բաքվի բոլոր ջանքերին, չի ենթարկվում Ադրբեջանի իշխանություններին: Թերթը ղեկավարվում է տեղի ադրբեջանցի գործարարների, մասնավորապես՝ Սոյուն Սաղիխովի կողմից, որի հարաբերությունները Բաքվի հետ բավական լարված են: «Ազեռռոսի» խմբագրակազմում աշխատում են ռուսներ, գլխավոր խմբագիրն է ազգությամբ ռուս Ալեքսանդր Բաբյակինը: Հայկական թեմային անդրադառնալիս թերթի ռուս լրագրողներին երբեմն որոշակի ազատական մոտեցումներ են «թույլ տալիս»: Այստեղ, թերևս, պետք է նշել նաև այն փաստը, որ թերթը մասամբ ֆինանսավորվում է ՌԴ պետբյուջեից: Մասնավորապես, հայտնի է, որ 2001-2004թթ. հատկացվել է 150 հազար ռուբլի:

Հոդվածներից մեկում «Սուխոյ» ավիաշինարարական ընկերության փոխղեկավար Վլադիմիր Իլյուշինը դրվատանքով է արտահայտվում տնօրեն Միքայել Պողոսյանի մասին: Սակայն Ղարաբաղյան հարցում «Ազեռռոսը» կոշտ մոտեցումներ ունի, որոնք պաշտոնական Բաքվի դիրքորոշումներից չեն տարբերվում:

«Ազերբայջանսկի կոնգրես» թերթի մոտեցումներն առավել ներդաշնակ են ադրբեջանական պաշտոնական քարոզչությանը: Թերթի կայքում առանձին բաժնով ներկայացված է հայերի կողմից իբր թե ադրբեջանական հուշարձանների ոչնչացման թեման, «Ռուսաստանի հասարակությանը, գիտնականներին, մշակութային գործիչներին և պարզապես բարի կամքի տեր անձանց հայկական վանդալիզմի դեմ ձայն բարձրացնելու» կոչ է արվում: Այնուհետև ներկայացված է 3 տասնյակի չափ ադրբեջանական հուշարձանների ցանկ Շուշիում և շրջակայքում, «որոնց ճակատագիրը վտանգված է»:

Նիդեռլանդներում գործող ադրբեջանցի կանանց «Անա Վաթան» միության նախագահ Գյուլշեն Քյազիմովայի և Նիդեռլանդներում ադրբեջանական դեսպանատան կողմից Հաագայի Խաղաղության պալատի գրադարանին է նվիրվել 16 հատոր գիրք «Խոջալիի ցեղասպանության» թեմայով, ինչպես նաև հոլանդերենով հրատարակված ադրբեջանցի գրող Գուրբան Սահիդի «Ալի և Նինո» գեղարվեստական պատումը: Վերջինս հոլանդերենով հրատարակվել էր խորհրդային շրջանում: Ըստ ադրբեջանական աղբյուրների՝ գրադարանի տնօրեն Ջերուն Ֆերֆիլթը բարձր է գնահատել ադրբեջանական կողմի նվիրատվությունը:

Արտասահմանում ադրբեջանական կողմի քարոզչական հնարքների շրջանակներում նշենք 2008թ. փետրվարի 26-ին Դյուսելդորֆ քաղաքի «Chanel Europe» հեռուստաալիքով Խոջալիի դեպքերին նվիրված ֆիլմի ցուցադրությունը: Փետրվարի 27-ին թեմային անդրադարձավ նաև Ֆրանկֆուրտի «Chanel 7-ը»: Ըստ Արտասահմանում բնակվող ադրբեջանցիների հետ աշխատանքային պետկոմիտեի հաղորդագրության, այս նախաձեռնությունները հնարավոր դարձան «գերմանաբնակ ադրբեջանական համայնքային հաստատությունների» շնորհիվ:

Փարիզում ադրբեջանա-ֆրանսիական երիտասարդական ասոցիացիան սկսել է «Լե Պոն-Մոստ» հանդեսի հրատարակությունը, որը ադրբեջաներեն և ֆրանսերեն հոդվածներ է հրապարակում:

«Լոնդոնի ադրբեջանական համայնք» կազմակերպության նախաձեռնությամբ «Խոջալիի ողբերգությունը. միջազգային տեսակետ» և «Միջազգային տեսակետներ. Ղարաբաղի շուրջ հայ-ադրբեջանական հակամարտությունը» անգլիալեզու ադրբեջանամետ հրատարակությունների օրինակներ են ուղարկվել Միացյալ Թագավորության ԱԳ նախարար Դևիդ Միլիբանդին, համայնքների պալատի 646 անդամներին, ԵՄ խորհրդարանում Բրիտանիան ներկայացնող 78 պատգամավորների, միջազգային լրատվամիջոցների՝ «Վաշինգթոն Փոստին», «Սանդի թայմսին», «Նյու Յորք թայմսին», «Նյուզուիքին», «Բոսթոն գլոբին» և այլն: Ըստ ադրբեջանական աղբյուրի՝ գրքից օրինակներ են ուղարկվել աշխարհի 60 գրադարանների:

Ստրասբուրգում բավական ակտիվացել է «Եվրոպայի ադրբեջանցիների ֆորում» կազմակերպությունը: Վերջինիս ղեկավար անդամ Էմին Միլիի խոսքերով՝ կառույցը նախատեսում է Եվրոպայում հիմնել ադրբեջանական լրատվական գործակալություն: Այս մասին հայտարարվել է նախորդ տարեվերջին, սակայն ներկա դրությամբ կոնկրետ քայլերի մասին տեղեկատվություն չկա:

Հայկարամ Նահապետյան

МОРАЛЬНО-ПСИХОЛОГИЧЕСКАЯ ПОДГОТОВКА ВОЕННОСЛУЖАЩИХ

Морально-психологической подготовке личного состава вооруженных сил уделяется все возрастающее внимание в армиях зарубежных стран. Технологизация ведения военных действий, связанная с постоянным совершенствованием вооружений и военной техники (ВВТ), внедрение новейших информационно-коммуникативных и сетецентричных разработок в военном деле не снимают вопроса морально-психологического тренинга личного состава, а придают ему более прикладной и диверсифицированный характер. Асимметричность, инсургентность и локальность современных вооруженных конфликтов предъявляют специфические требования к морально-психологической подготовленности военнослужащих, осуществляющих функциональную нагрузку в конфликтах подобного характера.

Будучи преимущественно связанным с понятием «человеческий фактор», морально-психологическое состояние (МПС) личного состава вооруженных сил выступает емким феноменом, включающим в себя такие составляющие, от которых зависит поддержание его на должном уровне, как интенсификация морально-психологической подготовки (МПП) всех категорий личного состава с приоритетной отработкой соответствующих вопросов в ходе мероприятий оперативной и боевой подготовки; усиление социальной защиты военнослужащих и прежде всего повышение материальной заинтересованности личного состава; проведение мероприятий, направленных на повышение уровня профессиональной компетенции органов военного управления.

Военно-научные разработки в сфере изучения психологии военнослужащих выявили следующие факторы, положительно и негативно влияющие на МПС личного состава. К положительным факторам относят: высокий уровень личной профессиональной подготовки и постоянное стремление к его повышению; убежденность в исключительности государственного строя своей страны; гордость за принадлежность к своей стране и ее вооруженным силам; приверженность традициям воинской части и вооруженным силам в целом; уверенность в качестве своего оружия; высокая психологическая готовность к началу военных действий.

Очевидно, что указанные положительные факторы могут иметь место в армиях, имеющих богатую и долгую традицию военного дела, участия в войнах и боевых действиях, развитую государственно-правовую идеологию и социальное благополучие населения. Возникает вопрос: где можно найти точки опоры для построения здорового морально-психологического климата в своих вооруженных силах тем странам, которые не имеют таких военных традиций, годами выверенной идеологии и высокого социального уровня жизни населения? Особенно актуален данный вопрос для малых по своим размерам государств, находящихся в фазе создания или развития собственной государственности после значительного перерыва в обладании государственной самостоятельностью. Можно предположить, что такие основы применительно к этим государствам могут быть найдены в благоприятно сложившихся для них военных действиях, в особенности если они имели место не в отдаленном прошлом и стали определяющими факторами для уверования национальных государств в своей жизнеспособности и занятия достойного места в международном сообществе признанных государств.

К негативным факторам, оказывающим влияние «со знаком минус» на МПС военнослужащих, военные психологи относят повышенный интерес к материальному стимулированию военнослужащих в ущерб морально-нравственному воспитанию; пренебрежение к противнику, переоценка своих сил, повышенное комфортолюбие; потеря инициативы в ходе боевых действий, что может привести к существенному снижению МПС военнослужащих; наличие расовых предрассудков, проявление крайних форм индивидуализма, карьеризм, отчужденность, напряженность во взаимоотношениях; злоупотребление алкоголем, наркотиками[1].

[1] *М. Зеленков*, Морально-психологическая подготовка войск в армиях зарубежных стран // Зарубежное военное обозрение, М., 2000, № 11.

МПП военнослужащих в армиях наиболее продвинутых в военном деле стран строится на принципах высокой специализированности и диверсификации методик тренинга личного состава в зависимости от его функциональной нагрузки, поставленными перед ним задачами. МПП в связи с этим может носить общий (предназначенный для всего личного состава вооруженных сил) и специальный (для отдельных боевых единиц, подразделений и частей вооруженных сил) характер.

МПП предопределяется, кроме прочего, «матрицей» противостояния между актуальными и потенциальными противниками, включающей многие факторы, тесно связанные в свою очередь с психологическим настроем военнослужащих на выполнение поставленных перед ними боевых задач.

Случаем такого противостояния выступает соприкосновение армянских и азербайджанских военнослужащих на линии прекращения огня в нагорно-карабахском конфликте. Психологический контекст такого противостояния определяется в терминах морально-психологической способности военнослужащих сторон конфликта выполнить боевые задачи в случае интенсивного «размораживания» прекращения огня: налицо два разнонаправленных вектора, которые в самом общем выражение можно обозначить через «наступление» и «оборона».

МПП военнослужащих для эффективного осуществления задач оборонительного свойства основывается на большом опыте, накопленном при осуществлении оборонных мероприятий, и решении связанных с ними задач в войнах и боевых действиях, начиная с того периода, когда человечество вошло в фазу широкого вовлечения техники и технологий в военное дело. Разработки в этой сфере лежат на междисциплинарном стыке знаний, опыта и навыков психологического, социального, этнического, культурного, религиозного характера, теории и практики игрового моделирования[1].

При оборонных мероприятиях особенно важна сплоченность военнослужащих и их уверенность в том, что боевой товарищ не покинет свою позицию, ослабив тем самым позицию своего товарища. Отсюда, основной уклон в МПП военнослужащих, призванных осуществлять боевые задачи оборонного характера (как минимум, в краткосрочной, непосредственной перспективе, до момента возможного проведения контрнаступательных действий), должен проводиться в сторону психологической консолидации и солидаризации военнослужащих, привития им на ментальном уровне навыков «чувствования локтя» боевого товарища и преодоления естественного страха в боевых условиях[2].

---

[1] Два исторических примера на эту тему, приведенных известным исследователем Томасом Шеллингом: «Примеры из военной истории всегда хороши, потому что, если взять историю начиная с Древней Персии и Древней Греции, это история войн… У Ксенофона, греческого полководца, было 10 тысяч человек в войске. Он отступал под напором персов, и у его войска было невыгодное положение. Греческое войско было окружено персами численностью от 40 до 50 тысяч человек: отчасти это были всадники, отчасти пехота, вооруженная копьями. Греки заняли позицию для обороны. Один из военачальников Ксенофона сказал: посмотри, мы сейчас стоим спиной к крутому склону, как мы будем отступать, если понадобится? Нам назад никак нельзя. И Ксенофон сказал: что ж, и слава богу, персы знают, что мы не можем отступать, они знают, что мы будем бороться до последнего солдата, потому что у нас нет другого выхода. И более того, сказал он, каждый из нас, десяти тысяч, это знает, что если он будет думать о противнике, а не смотреть по сторонам и назад, что делают его товарищи, он будет знать, что товарищи рядом, потому что бежать им просто некуда, даже если бы они хотели. Таким образом, мы сосредоточимся на персах и никогда не отступим. И, конечно, они тогда не смогут наступать, если они не готовы бороться с греками, которые готовы бороться до последнего. И все 10 тысяч или 9999 понимали эту ситуацию. Можно взять более свежий пример: Первую мировую войну. Было сообщение, что немцы приковывают пулеметчиков к станку пулемета. Идея была в том, что они хотели, чтобы французы, британцы и потом американцы знали, что ни один пулеметчик не покинет огневую точку и не отступит, он привязан намертво, как говорится, к своему оружию и будет стрелять до тех пор, пока не кончатся патроны, и его уже ничем не напугаешь и не заставишь отступить. И это было важно даже для самих пулеметчиков, которые знали, что отступление невозможно. Точно так же как в случае с войском Ксенофона, которое стояло спиной к обрыву, пулеметчику ничего другого не оставалось, как стрелять». (*Презентация книги лауреата Нобелевской премии Т. Шеллинга «Стратегия конфликта»*, http://www.kreml.org/other/135727638?mode=print, 4.12.2006).

[2] Социальным фактором, в значительной мере определяющим поведение воина в бою, является *сплоченность воинского подразделения*. Она выступает своеобразным основанием для поддержания высокой психологической устойчивости и активности отдельных военнослужащих. Анализ боевых действий советских войск в Афганистане, войн Израиля на Ближнем Востоке, англо-аргентинского военного

Военная наука выработала и продолжает развивать методику проведения МПП военнослужащих, на которых возложена, помимо прочего, и «оборонная» функциональная нагрузка.

На первоначальном этапе такой подготовки обычно осуществляют своеобразную *психотерапию.* Это значит, что в процессе обучения специально создают такие условия, которые вызывают у военнослужащих негативные психические состояния. Оказавшись в обстановке, близкой к боевой, молодой солдат нередко теряет уверенность в своих силах, впадает в апатию или депрессию, у него возникает чувство страха. Часто при этом он испытывает болезненные синдромы типа головокружения, тошноты, онемения конечностей и т.д. В результате он может отказаться от пищи, потерять сон, забыть о своих служебных обязанностях, совершить дисциплинарный проступок, и даже дезертировать.

Однако в период обучения все это не представляет большой опасности. Солдат учат подавлять свой страх, преодолевать апатию, другие негативные эмоции и чувства, вырабатывают у них простейшие навыки самоконтроля и т.д. Это и есть *психотерапия*. Посредством ее вырабатывают умение сдерживать внешнее проявление негативных психических состояний, но от них самих избавиться еще не удается. На это, как правило, и делают упор специалисты психологической войны, осуществляя свое воздействие на личный состав войск противника.

Второй этап морально-психологической подготовки включает в себя мероприятия по так называемому *психологическому стимулированию*. Суть его состоит в приучении военнослужащих надежно выполнять свои профессиональные обязанности в условиях боевой деятельности. С этой целью в процессе боевой подготовки инструкторы обрушивают на солдат серию физических, психологических и нравственных раздражителей, совокупное воздействие которых приводит к запредельному торможению. Воля солдат оказывается практически сломленной, они в точном смысле слова теряют способность вообще что-то делать. Инструкторы в этих условиях должны приходить на помощь личному составу, приводить его психику в нормальное состояние. Их основная задача сводится к тому, чтобы научить подчиненных ясно осознавать приказы вышестоящего командования и выполнять их несмотря ни на что.

Психотерапию и психостимулирование раньше не считали важными элементами МПП военнослужащих, гораздо больше внимания уделяли идейно-политическому воспитанию. В последние годы ситуация изменилась коренным образом. Военные специалисты, анализируя боевые действия вооруженных сил Великобритании на Фолклендских островах, советских войск в Афганистане, США во Вьетнаме и в Персидском заливе, твердо убедились в необходимости целенаправленной закалки психики солдат и офицеров в обстановке, максимально приближенной к боевой. Сегодня они придерживаются следующей концепции:

а) то, что солдат успешно выдерживает в ходе учебы, он спокойно выдержит и в условиях настоящей войны,

б) в первую очередь из всех психологических качеств надо формировать чувство уверенности,

в) методы и приемы психотерапии и психостимулирования должны быть разнообразными[1].

Михаил Агаджанян

конфликта из-за Фолклендских островов показал, что отделения, экипажи, расчеты, состоящие из хорошо знавших друг друга военнослужащих (родственников, земляков и др.), проявляли большую активность, инициативу, стойкость. Изучая эту закономерность, немецкий военный психолог Е.Динтер подчеркивает, что страх потерять доверие группы, оказаться в моральной изоляции из-за трусости действует сильнее всего, позволяет совершать смелые поступки. В последнее время в армиях ведущих государств мира большое внимание уделяется созданию в воинских подразделениях «системы товарищеской поддержки», когда члены экипажей (расчетов, групп) наблюдают за появлением у сослуживцев симптомов нервного напряжения и оказывают друг другу неотложную психологическую помощь. Считается, что уверенность в сослуживцах, в том, что они придут на помощь в нужный момент, является важным условием решительных и самоотверженных боевых действий каждого солдата. (См. *А. Караяни*, *И. Сыромятников*, Прикладная военная психология, СПб, «Питер», 2006).

[1] *В. Крысько*, Секреты психологической войны (цели, задачи, методы, формы, опыт), Морально-психологическое состояние военнослужащих противника, http://dere.com.ua/library/krisko/013.shtml.

21-ՐԴ ԴԱՐԻ ՆՈՐ ՏԵՂԵԿԱՏՎԱԿԱՆ ՍՊԱՌԱԶԻՆՈՒԹՅՈՒՆԸ ԵՎ *DARPA*[1] ԿԵՆՏՐՈՆԸ

Ս.թ. փետրվարի սկզբին ԱՄՆ նախագահ Ջ.Բուշը հանձնարարեց կարճ ժամանակում ստեղծել մարտունակ ստորաբաժանում՝ ԱՄՆ-ի դեմ հաքերային և տեղեկատվական պատերազմ վարող խմբերի հետ պայքարելու համար: Հատկանշական է, որ այդ հանձնարարականը կյանքի կոչելու արդյունքում հիմնական թիրախներ են հանդիսացել պաշտպանական ենթակառուցվածքների տարրերը՝ կառավարման և հրթիռային կետերը, օդանավակայանները և նավահանգիստները, պետական և մասնավոր կապի համակարգերը: Այս հանձնարարականը հիմք հանդիսացավ սպառազինության նոր տեսակների և տեխնոլոգիական նոր մոտեցումների մշակման համար: Հոդվածում ներկայացված են սպառազինության ոլորտին վերաբերող նորամուծությունները, այդ գործընթացում ընդգրկված կազմակերպությունները և կենտրոնները: Հիմնական նպատակն է պատկերացում կազմել տեխնոլոգիական նոր մոտեցումների և վտանգների վերաբերյալ, որը սկզբունքորեն տարբերվում է մեր ունեցած մոտեցումներից 21-րդ դարում հնարավոր պատերազմների ժամանակ:

Ակնհայտ է, որ հանձնարարականը, որն այլ վտանգների շարքում առաջնային դարձրեց ԱՄՆ անվտանգության սպառնալիք հանդիսացող տեղեկատվական պատերազմը, միանգամայն հիմնավորված է: ԱՄՆ Կոնգրեսի ռազմական գործերով կոմիտեի նախագահ Կուրտ Վելդոնը նշում է, որ եթե 1998թ. գրանցվել էր տեղական համակարգչային ցանցերը[2] կոտրելու և խափանելու 547 դեպք, 2005թ. դրանց թիվը հասել էր 1824-ի, իսկ անցյալ տարի այն հատել է 3000-ի սահմանագիծը: Նման գրոհների բազմաթիվ դեպքեր են գրանցվել նաև Հնդկաստանի, Մեծ Բրիտանիայի և Իսրայելի ուժային գերատեսչությունների դեմ՝ «ջարդելով» միջուկային կենտրոնների և անվտանգության ծառայությունների տեղեկատվական ցանցերը, ոչնչացնելով մի շարք տվյալների բազաներ[3]:

Ստեղծված իրավիճակում ԱՄՆ ռազմաքաղաքական գերատեսչությունն արդեն իսկ 90-ականներին վերսկսեց տեղեկատվական պատերազմների հետ կապված խնդիրների ուսումնասիրությունները, որի արդյունքում մշակվեցին տեղեկատվական հակամարտության հիմնական հայեցակարգը և սկզբունքները: Դրա հիման վրա գործում է տեղեկատվական պատերազմի նախապատրաստման միջոցառումների երկարաժամկետ ծրագիրը, որը ներառում է կարևոր համակարգչային կառույցների պաշտպանության միջոցների և բազմափուլ համակարգերի, ինչպես նաև վիրտուալ հարձակողական սպառազինությունների ստեղծումը: Այդ ծրագրի իրականացման համար ներգրավվել են այնպիսի կազմակերպություններ և համալսարաններ, ինչպիսիք են Կալիֆորնիայի համալսարանը, Մասաչուսեթսի տեխնոլոգիական ինստիտուտը, «Բոինգ»-ը, *DARPA*-ն, որոնցից յուրաքանչյուրի հետ կնքվել են ավելի քան 50 միլիոն դոլար արժողության պայմանագրեր: Արդյունքում՝ արդեն 2008թ. սկզբին կատարվել են 25 պայմանագրերով նախատեսված պատվերներ, իսկ նորաստեղծ համակարգերը, փորձաքննություն անցնելուց հետո, ընդգրկվել են ԱՄՆ զինուժի մասնագիտացված ստորաբաժանումներում: Նման համակարգերի շարքին է դասվում հակառակորդի տեղեկատվության հավաքման կենտրոնների արգելափակման, կապի միջոցների, համակարգչային ցանցերի և ռադիոլոկացիոն կայանների խափանման համար նախատեսված էլեկտրամագնիսական զենքը: Վերջին տարիներին ամերիկյան սպառազինության տեսականե-

---

[1] *DARPA* (Defense Advanced Research Projects Agency) – պաշտպանության ոլորտի գիտական հետազոտությունների հեռանկարային պլանավորման կենտրոն:

[2] Խոսքը ԱՄՆ տեղական, ներքին ցանցերի մասին է:

[3] *Юлия Левашова,* “В Вооруженных силах США появился новый вид оружия – кибервирусы”, 01.05. 2008, Центр Исследования Компьютерной Преступности/ http://www.crime-research.ru/news/01.05.2008/4464/

րը համալրվեցին թշնամու տեղեկատվական ենթակառուցվածքների վրա ազդեցության նոր միջոցներով: Դրանց թվին են դասվում էլեկտրամագնիսական իմպուլսի շարժական գեներատորները, որոնք կարող են շարքից հանել ոչ միայն կապի համակարգերը, այլև ոչնչացնել այն սպասարկող անձնակազմը: Հենց այդպիսի սպառազինությունն է այսօր համալրում «Ցանցային ռազմական գործողությունների միավորված հրամանատարությունը»[1], որը ստեղծվել է ի կատարումն ԱՄՆ նախագահի վերոհիշյալ հանձնարարականի:

Ըստ ամերիկյան ռազմական վերլուծաբանների, այս հրամանատարությունը ԱՄՆ ռազմական ուժերի ամենագաղտնի զորամիավորումն է, որի գործունեության վերաբերյալ դժվար թե հնարավոր լինի տեղեկություններ հայթայթել: Սակայն այդ զորամիավորման վիրտուալ սպառազինության վերաբերյալ, այնուամենայնիվ, որոշ տեղեկություններ գոյություն ունեն: Կիբեռնետիկ զենքին անրադարձել է քվանտային ֆիզիկայի տեսաբան և այդ զենքի հեղինակ Լոուրենս Վուդը: Ըստ մասնագետի, այդ զինատեսակը ներառում է յուրաքանչյուր համակարգչի համար կործանարար էլեկտրոնային վիրուս: Նա նկարագրում է այդ զինատեսակը որպես քվանտային ֆիզիկայի և քաոսի տեսության վրա հիմնված ալգորիթմների հավաքածու, որը ներխուժելով նույնիսկ անջատված համակարգիչ՝ ամբողջովին խափանում է այն[2]:

Վիրտուալ զինատեսակներից է նաև այսպես կոչված «Նոուբոթ»-ը[3], որը տեղեկատվական ցանցում մեկ համակարգչից մյուսը տեղափոխվելու և բազմանալու հնարավորություն ունի: Այն հնարավոր չէ հայտնաբերել, քանի որ նախատեսված է նաև ինքնատեղափոխման կամ ինքնավերացման գործառույթը[4]:

Այնուամենայնիվ, անրադառնանք նաև մեկ այլ կազմակերպության, որը հայտնի է ռազմական, վերլուծական, տեխնոլոգիական նորամուծություններով: Խոսքը *DARPA* պաշտպանության ոլորտի գիտական հետազոտությունների հեռանկարային պլանավորման կենտրոնի մասին է: Այս կենտրոնը ստեղծվել է 1958թ. փետրվարին, Խորհրդային Միության կողմից «Սպուտնիկ» արհեստական արբանյակի արձակումից անմիջապես հետո, երբ ԱՄՆ նախագահ Էյզենհաուերը հրավիրեց հատուկ նիստ Խորհրդային Միության արբանյակային առաջընթացը վերլուծելու և ամերիկյան ձախողումը բացատրելու նպատակով: ԱՄՆ-ը, ունենալով տեխնիկական բոլոր հնարավորությունները, այնուամենայնիվ, պետք է հետևողական լիներ այդ ծրագրի իրականացման գործում[5]:

Կենտրոնի հիմնական խնդիրներից են ռազմական նոր տեխնոլոգիաների մշակումը, հեռանկարային ծրագրերում ֆինանսական հոսքերի բաշխումը և ղեկավարումը: Ստեղծման օրվանից կենտրոնի նորամուծությունների շարքում են ինտերնետը, համակարգչի աշխատանքի համար նախատեսված մկնիկը և այլն, ինչպես նաև հակաօդային պաշտպանության մի շարք ռադարներ: Նման նորամուծությունների և աշխատանքների արդյունավետության արդյունքն են կենտրոնի 2 մլրդ-անոց բյուջեն[6], տարբեր ոլորտների լավագույն մասնագետների ընդգրկվածությունը: *DARPA*-ի հիմնական առաքելությունն է՝ աջակցել ԱՄՆ զինված ուժերի տեխնոլոգիական բարձր որակի ապահովմանը և կանխել այն տեխնոլոգիական հետևանքները, որոնք կարող են վնաս հասցնել ԱՄՆ ազգային անվտանգությանը:

Ըստ փորձագիտական աղբյուրների, 2009թ. փետրվարից կգործի կենտրոնի զարգացման նորացված ռազմավարությունը, որը ներառում է տեղեկատվական տեխնոլոգիաների ոլորտին վերաբերող ռազմական և հետախուզական հետևյալ ուղղությունները.

1. տիեզերական և միջտիեզերական համակարգերի ընդլայնում, փոքր արբանյակների օգտագործում (1 – 100 կգ),

---

[1] Անգլերեն անվանումը՝ Joint Functional Compromen for Network Warfare, JFCCNW.

[2] Technology Industry, http://findarticles.com/p/articles/mi_qa5438/is_199805/ai_n21426272

[3] Անգլերեն անվանումը՝ Knowbot - Knowledge Robot.

[4] Информационное оружие, как средство ведения информационного противоборства, http://www.vrazvedka.ru/main/analytical/lekt-03.shtml

[5] Paul Chappel, "DARPA and the Future of Army Air and Missile Defence", Air Defence Artillery, http://www.airdefenseartillery.com/online/Extracts/DARPA.pdf

[6] Пентагон увеличил финансирование агенства DARPA, http://science.compulenta.ru/347527/

2. կապի ցանցերը 100 Գբիտ/վրկ հնարավորությամբ, նոր սերնդի թվային համակարգերը, ռադարների հիբրիդային համակարգերը,
3. տեղեկատվական առավելությունը (կիբեռգրոհների դեմ ավտոմատ պաշտպանվածություն, հաշվարկների պաշտպանության ապարատային միջոցներ, միջցանցային էկրաններ),
4. աջակցություն փոքր զորամիավորումների գործողություններին, *GPS* համակարգից դուրս նավիգացիոն միջոցներ քաղաքներում և շենքերում, էժան *GPS* ընդունիչներ և այլ:

2008թ. մարտին *DARPA* տնօրեն Թոնի Թեզերն իր հաշվետվությունը ներկայացրեց ԱՄՆ Կոնգրեսի ռազմական գործերով կոմիտեին՝ մանրամասն քննարկելով իր կազմակերպության տեխնոլոգիական հեռանկարային ծրագրերը: Ըստ Թեզերի, հիմնարար գործունեության ուղություններից են ցանցերի (առաջին հերթին ոչ լարային) ստեղծման աշխատանքները, որոնք կմիավորեն մարտավարական և ռազմավարական համակարգերը՝ միաժամանակ հնարավորություն ունենալով ավտոմատ կերպով ձևավորել սեփական համակարգը, ինքնուրույն ապահովելով անվտանգությունն արտաքին և ներքին ներխուժումներից:

DARPA կենտրոնը մտադիր է մշակել մոդուլային արբանյակների նոր տիեզերական հայեցակարգ, որն արդեն ստացել է «Ֆ6»[1] պայմանական անվանումը: Ծրագիրը նախատեսում է ուղեծրում «ֆրակցիոն մոդուլների» նոր խմբավորումներ ծավալել, որոնք սկզբունքորեն կտարբերվեն «ամբողջը մեկի մեջ» սկզբունքով պատրաստված առկա արբանյակներից: Այլ խոսքով՝ կենտրոնը մշակում է վիրտուալ արբանյակների կոնցեպցիա: Ըստ կենտրոնի տեղեկագրության, Ֆ6-ն ընդգրկելու է լավագույն տեխնոլոգիական նորամուծությունները[2]:

DARPA կենտրոնի հետ սերտորեն համագործակցում է նաև Պենտագոնը, որը հանձնարարական է ստացել տեղեկատվական ցանցերում հարձակողական և պաշտպանողական գործողություններ վարելու նոր միջոցների և ձևերի մշակման վերաբերյալ: Ըստ *«Strategy page»* ռազմական նորությունների կենտրոնի, այս գաղտնի ծրագիրը ստացել է «Մանհեթեն»[3] անվանումը՝ ամերիկյան միջուկային զենքի ծրագրի համանման անվանումով: Ծրագրի մշակումը կրկին վստահված է *DARPA*-ին: Դրա շրջանակներում նախատեսվում է ստեղծել փակ համակարգչային ցանց, որն իր հիմնական առանձնահատկությամբ նման է համաշխարհային ցանցին:

Նորամուծությունները մեկ անգամ ևս ցույց են տալիս տեղեկատվական ենթակառուցվածքների դերն ու կարևորությունը և սկզբունքորեն փոխում մեր պատկերացումները կիրառվող սպառազինությունների տեսակների վերաբերյալ 21-րդ դարում հնարավոր պատերազմների ժամանակ: ԱՄՆ-ը, լինելով տեխնոլոգիական նորամուծությունների կենտրոն, ջանք չի խնայում պահպանելու ռազմական գերակայությունն ամբողջ աշխարհում: Մեծածավալ ներդրումներ են կատարվել և պետական հավանության են արժանացել բազմաթիվ ծրագրեր, որոնց հիմնական դերակատարությունը վստահված է պաշտպանության ոլորտի գիտական հետազոտությունների հեռանկարային պլանավորման *DARPA* կենտրոնին:

Սուրեն Մովսիսյան
«Նորավանք» հիմնադրամ

[1] Անգլերեն անվանումը F6 (Future, Fast, Flexible, Fractionated, Free-flying Spacecraft United by Information Exchange).

[2] DARPA разрабатывает новую концепцию орбитальных спутников.

[3] Անգլերեն անվանումը՝ Manhattan Project.

КОНГРЕССМЕНЫ-РЕСПУБЛИКАНЦЫ РАССКАЗАЛИ О ХАКЕРСКИХ АТАКАХ ИЗ КИТАЯ[1]

Американские конгрессмены-республиканцы объявили о попытках взлома своих служебных компьютеров китайскими хакерами, передает в четверг агентство *Associated Press*.

Как утверждают члены палаты представителей Фрэнк Вулф *(Frank Wolf)* от штата Вирджиния и Крис Смит *(Chris Smith)* от штата Нью-Джерси, эти инциденты происходили в 2006г. и в начале 2007г. В общей сложности атакам хакеров подверглись шесть компьютеров, в которых хранились данные о политических диссидентах по всему миру.

Вулф и Смит, которые являются давними критиками позиции Китая в области соблюдения прав человека, убеждены, что китайские хакеры намеревались завладеть информацией о местонахождении диссидентов, чтобы осуществлять за ними слежку. По словам конгрессменов, некоторые американские политики пытались их отговорить от обнародования информации о попытках взлома компьютеров.

Получить комментарии по поводу заявлений Вулфа и Смита в ФБР и Белом доме агентству не удалось. Однако представитель Вирджинии рассказал AP, что его источникам в ФБР известно еще о нескольких попытках взлома компьютеров конгрессменов китайскими хакерами. Политик не исключил, что компьютеры Сената также могли быть целью хакерских атак.

Между тем продолжается расследование возможной кражи данных с правительственного ноутбука Министерства торговли США. Она предположительно была совершена представителями властей КНР во время визита главы ведомства в Пекин в декабре 2007г., когда Карлос Гутиеррес *(Carlos Gutierrez)* оставил компьютер без присмотра.

Напомним, с июля 2006г. Пентагон, Госдепартамент и Министерство торговли не раз сообщали, что подвергались компьютерным атакам, ответственность за которые возлагали на Китай.

[1] http://lenta.ru/news/2008/06/12/compromise/_Printed.htm

НОВЫЕ ПРИОРИТЕТЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ США

Трагические события, которые произошли в США 11 сентября 2001 года и повергли в шок весь мир, вновь напомнили человечеству об обратной стороне технического прогресса. Варварские террористические акты, совершенные группой террористов-смертников в Нью-Йорке и Вашингтоне, стали суровым испытанием не только для правительства и спецслужб, но и для всего американского общества. К своему удивлению мы узнали, что США – это далеко не самая безопасная и благополучная страна в мире, а американцы – это не только прагматики и бизнесмены, но и патриоты своей Родины, за которую они готовы отдать жизнь, как это сделали пассажиры Боинга под Питсбургом. Сейчас, когда на волне гнева и мести, буквально захлестнувшего США, Пентагон и ЦРУ пытаются взять реванш в схватке с невидимкой Бен Ладеном в горах Афганистана, на повестку дня вновь и вновь встает вопрос о безопасности информационных технологий.

Впрочем, почему только информационных: попробуйте назвать хоть одну сферу деятельности человека (связь, транспорт, авиация, космос, энергетика, водоснабжение, финансы, торговля, наука, образование, оборона, охрана общественного порядка, медицина и др.), где сейчас не применяются эти технологии и вы поймете, насколько зависимы мы все стали от битов, чипов, модемов... – одним словом всего того, что превращает нас помимо нашей воли из *«homo sapiense»* в *«homo informaticus».* Фактически во многих развитых странах сегодня активно реализуется концепция так называемого «электронного правительства». Можно поспорить о том, что далеко не все страны и народы приемлют новый «цифровой» порядок, что высокие технологии для многих просто недосягаемы и миллионы голодных людей вообще не знают о том, что есть сотовые телефоны, спутники, персональные компьютеры и Интернет, но факт остается фактом – человечество шагнуло в новое тысячелетие, имея в своих руках инструмент столь же созидательный как и разрушительный по своим возможностям одновременно.

Как установило ФБР, террористы-камикадзе готовились к своим ударам с помощью широко доступных программ, имитирующих полет самолета над Нью-Йорком и Вашингтоном, а для передачи инструкций в процессе подготовки и планирования террористической операции по захвату самолетов – электронную почту Интернет. Разрушение комплекса зданий только в Нью-Йорке, помимо человеческих жертв повлекло за собой закрытие биржи, падение курса акций, потерю десятка тысяч каналов передачи данных, перегрузку трафика в Интернет, уничтожение информации в компьютерах сотен фирм и офисов...

Для того, чтобы лучше осознать масштабы распространения информационных технологий в современном обществе, а следовательно и степень его технологической уязвимости обратимся к опыту США – стране, откуда к нам и пришли эти высокие технологии вместе с новыми проблемами. Американцы любят повторять, что они – нация эмигрантов, страна равных возможностей, где уснув бедняком можно проснуться миллионером. Количество желающих приехать на постоянное жительство в одну их самых богатых и развитых стран мира неуклонно возрастает из года в год, несмотря на все строгости американского законодательства, жестко регулирующего въездные квоты. США после распада СССР на протяжении последних десяти лет прочно занимают место государства-лидера со статусом мировой сверхдержавы. На земном шаре нет ни одного уголка, который не попадал бы в сферу американских национальных интересов.

Но вот парадокс – сегодня американцы вполне реально могут стать жертвами «кибернетического» Перл-Харбора, для подготовки и осуществления которого агрессору не понадобятся, как это было в прошлом, ни ракеты, ни самолеты, ни атомная бомба. Буквально в считанные минуты страна может оказаться парализованной, а через несколько часов стать ареной

ужасающих по своим последствиям беспорядкам среди населения, где в охваченной паникой еще недавно благополучной демократии стихийно начнут провозглашаться новые государственные образования, до боли знакомые нам по опыту Северного Кавказа. Что это – бред сумасшедшего, сюжет фантастического триллера или очередная журналистская утка? Это – сценарий Пентагона, американского военного ведомства, по коридорам которого вот уже 10 лет витает зловещая тень угрозы информационной войны, нависшей над Америкой после войны в Персидском заливе.

В ночь с 16-го на 17-ое января 1991 года, через сутки после истечения срока ультиматума ООН о выводе иракских войск с территории аннексированного 2 августа 1990 г. Кувейта, американские стратегические бомбардировщики и военные корабли нанесли удар крылатыми ракетами по военным объектам Ирака. Еще до подлета первых 50-ти крылатых ракет до целей группа армейских вертолетов внезапно на малой высоте атаковала и вывела из строя две главных иракских РЛС. Так началась операция многонациональных вооруженных сил по освобождению Кувейта «Буря в пустыне», которой суждено было войти в историю как война 21-го века.

За 43 дня боевых действий Ирак потерял 4000 танков (95%), 2140 орудий (69%), 1856 БТР (65%), 7 вертолетов (4%), 240 самолетов (30%), 143 корабля (87%). Потери коалиции составили соответственно: 4 танка (0,1%), 1 орудие (0,03%), 9 БТР (0,2%), 17 вертолетов (0,9%), 44 самолета (1,7%). Общее количество убитых со стороны 700000 союзных войск составило 148 человек (0,021%), из которых примерно 30% стали жертвами «огня по своим». Потери Ирака, армия которого насчитывала свыше полумиллиона человек, оцениваются в 9000 убитых (2%), 17000 раненых (3%) и 63000 пленных (12%). Свыше 150000 солдат (28%) дезертировали из иракской армии в ходе наземного наступления.

Но не пройдет и года после внушительно одержанной военной победы, еще будут полыхать факелы нефтяных скважин Кувейта, как в Пентагоне забьют тревогу: на смену эйфории придет отрезвление. Хорошо спланированная и блестяще проведенная военная операция с применением новейшего высокоточного оружия, самолетов-невидимок, приборов ночного видения, беспилотных самолетов-разведчиков, спутников и компьютеров могла окончиться полным провалом: военно-техническое превосходство победителя в одночасье превратилось в его ахиллесову пяту.

В секретной директиве Пентагона S-3600.1 появится совершенно новое и непривычное понятие – «информационная операция», которому суждено будет совершить подлинную революцию в военном деле. Как ни парадоксально, но в основу «информационной операции» против Ирака, как это уже официально записано в уставах и наставлениях вооруженных сил США, был положен классический прием ведения войны – дезорганизация управления. Исход поединка «Давида и Голиафа» решил внезапный удар в «голову» противника, потерявшего «зрение», «слух» и «речь» почти одновременно.

За несколько недель до начала ведения боевых действий специально обученные агенты ЦРУ с помощью портативных компьютеров в Багдаде внедрили программные «вирусы-закладки», которые в назначенный день и час отключили телефонные станции и радиолокационные посты, парализовав уже в первые минуты воздушного налета систему ПВО Ирака. Есть сведения, что истребители «Мираж» иракских ВВС по этой же причине не могли использовать свои бортовые РЛС в ходе отражения налета. Это позволило союзной авиации в первые несколько часов уничтожить основные объекты иракской системы ПВО и через 10 дней завоевать превосходство в воздухе.

Оружие возмездия – баллистические ракеты «Скад», которыми Ирак будет обстреливать Израиль и Саудовскую Аравию в ответ на прицельные авиационные налеты американцев, в большинстве случаев окажется малоэффективным против зенитных ракет «Патриот» и спутников системы раннего предупреждения. На угрозы Хуссейна применить химическое оружие президент Буш хладнокровно отдаст приказ о приведении стратегической ядерной триады США в полную боевую готовность. Весь мир, затаив дыхание, будет смотреть на экранах телевизоров прямые репортажи с театра военных действий.

По иронии судьбы «непобедимой» иракской армии в январе-феврале 1991 г. было суждено получить от НАТО урок немецкого блицкрига, за который Красная армия летом 1941г. заплатила миллионами убитых, раненных и пленных солдат и офицеров. Жесткая централизация системы военного руководства Ирака, большинство объектов которой было сосредоточено в Багдаде, а закрытые правительственные линии связи проложены через автомобильные и железнодорожные мосты, оказала Хуссейну медвежью услугу. Союзники, используя авиационные бомбы с лазерным наведением и крылатые ракеты со спутниковой системой навигации, к началу наземного наступления разрушили практически все коммуникации иракских войск. Попытки отдавать приказы из Багдада с помощью посыльных мотоциклистов только усугубили положение иракской армии, которая за время воздушных налетов уже была фактически деморализована. Миллионы листовок, сброшенных на головы иракских солдат призывали их держаться подальше от своих танков, бронетранспортеров и орудий, как объектов поражения высокоточного оружия, эффективность которого уже не вызывала сомнения.

Что же так напугало генералов в Пентагоне, пребывавших в зените своей славы? Сегодня в США созданы самые оснащенные вооруженные силы в мире: около 3 млн. гражданских специалистов и военнослужащих, включая резервистов имеют в своем распоряжении вооружение, технику и имущество на общую сумму в 1000 млрд. $, на содержание которых выделяется свыше 300 млрд. $ в год.

Для ведения такого большого разбросанного по всему миру «хозяйства», доставляющего немало организационных, технических и чисто человеческих хлопот, американцы содержат внушительный арсенал информационных ресурсов: свыше 2 млн. компьютеров, 100000 локальных сетей и 10000 информационных систем.

Для вооруженных сил США, где на одного военнослужащего приходится один персональный или бортовой компьютер, а количество информационных систем, в которых эти компьютеры интегрированы для решения боевых задач в ходе военных действий, исчисляется десятками тысяч, сценарий 1991 года означал бы полный крах. Обрушенные на головы иракцев 60 тыс. тонн боеприпасов, из которых 10% составили высокоточное оружие, включая 323 крылатые ракеты, не достигли бы своих целей, если бы противник вывел из строя хотя бы одну из этих систем, например, навигации или тылового обеспечения. Если вспомнить, что во время американских бомбежек Югославии устаревшая информация ЦРУ привела к «точному» попаданию крылатой ракеты... в здание посольства КНР – нейтральной страны, обладающей ядерным оружием, то нетрудно представить возможные последствия замены всего нескольких байт в «ядерном чемоданчике» президента США.

Но это еще не все. В отличие от Ирака, где для управления войсками использовалось 60% гражданских линий связи, в США этот показатель достиг 95%, включая использование глобальной сети Интернет и спутников связи Интелсат. Известны случаи, когда недавние выпускники военных академий, корректировали огонь своих артиллерийских батарей, используя электронные карты Пентагона за тысячи миль от своих боевых позиций в пустыне. Для непрерывного, практически в течение каждого часа, уточнения данных воздушной и космической разведки, необходимо было задействовать сотни спутниковых каналов одновременно. Большинство пилотов после вылета на задание перенацеливались уже в ходе полета, поражая цели с ходу, что значительно снизило потери союзной авиации.

Общедоступность и высокая оперативность обновления информации о боевой обстановке, в сочетании с ее наглядностью и высокой достоверностью «единой цифровой картины поля боя», превращают информацию не только в мощное оружие, но и уязвимую цель для противника.

Планирование операций, разведка, навигация, связь, материально-техническое снабжение, инженерное оборудование, транспортировка грузов, медицинское обеспечение, финансирование и расквартирование войск, заказ вооружений и электронная торговля прочно обосновались в паутине компьютерных сетей, в которые то и дело заглядывают через Интернет любознательные хакеры, где им есть что посмотреть в секретных файлах американских военных.

Военный флот выходит в Интернет

Америка – крупнейшая военно-морская держава. Сегодня в боевом строю военного флота США находятся свыше 300 военных кораблей, 4000 самолетов и вертолетов. Общая численность ВМС и морской пехоты составляет примерно 900 тысяч военнослужащих и гражданского персонала, из которых 88 тыс (10%) находятся за пределами США. Годовой бюджет ВМС – это 90 млрд. $ или 30% всего военного бюджета Пентагона. Ежегодно военно-морское ведомство тратит около 1.6 млрд. $ на автоматизацию и информационные технологии.

Американские ВМС в тандеме с морской пехотой начинают грандиозную и беспрецедентную по своей стоимости и масштабу охвата программу создания глобальной информационной сети NMCI (Navy Marine Corps Intranet). По данным военно-морского ведомства США стоимость программы оценивается в 7 млрд. $. В ходе ее выполнения в период 2001-2008 гг. предполагается объединить около 100 разрозненных в настоящее время ведомственных информационных сетей и ликвидировать порядка 200 телекоммуникационных шлюзов, задействованных в системе оперативного планирования и боевого использования кораблей, авиации и подразделений морской пехоты США. Общее количество компьютеров (серверов, настольных рабочих станций, портативных и карманных компьютеров) может достичь 360 тысяч ед., при этом они будут разбросаны по всему земному шару на 300 военных базах (Аляска, Исландия, Пуэрто-Рико, Гуам, Окинава, Гавайи, Куба и др.), включая континентальную часть США.

Сама идея создания подобной сети появилась как результат обобщения опыта совместного боевого использования разнородных (авиационных, морских и сухопутных) смешанных группировок вооруженных сил в так называемых конфликтах низкой интенсивности (Косово, Сомали и др.). В итоге военно-морские силы в рамках концепции Пентагона по реформированию и автоматизации ВС «общее видение 2020» выдвинули свою инициативу – «информационные технологии 21-го века», одной из важнейших составляющих которой и является данная программа.

Создаваемая сеть объединит все потоки информации, передаваемые в направлении «корабль-берег» и «берег-корабль», за счет использования универсального мультимедийного интерфейса и технологии Интранет. Пользователи сети будут иметь выход на все важнейшие правительственные, военные и коммерческие информационные системы, что позволит им оперативно решать задачи не только в интересах планирования и проведения военных операций, но и в личных целях (заказ авиабилетов, оплата счетов, медицинская диагностика и др.).

Пехотинец 21-го века

По оценкам Пентагона в текущем десятилетии 50% всех боевых действий будут вестись в условиях городских застроек (населенных пунктах), а к 2025 г. этот показатель может достигнуть 75-80%. Мировой опыт вооруженных конфликтов низкой интенсивности (Ливан, Гренада, Сомали, Косово, Чечня) показывает, что ведение боя в населенных пунктах характеризуется высокими потерями, быстрой сменой обстановки, неустойчивостью связи, плохой видимостью, низкой эффективностью применения тяжелых вооружений (авиации, танков), затрудненным тыловым снабжением и медицинским обеспечением войск.

Вот почему сухопутные войска активно разворачивают работы по созданию собственного армейского тактического Интранета по программе WIN-T, в ходе которой американские солдаты получат не только новую экипировку со шлемом-дисплеем, компьютером, радиостанцией, датчиком космической системы навигации и автоматической винтовкой, позволяющей с помощью специального прицела-перископа стрелять из-за укрытия ночью и в тумане, но и уникальным доступом к информационным системам планирования и ведения боевых действий.

Подсистема личной связи CRS, сопряженная с портативным компьютером и индивидуальным датчиком глобальной навигационной системы GPS, должна максимально облегчить солдату в бою все его действия, связанные с ориентированием на местности, оценкой обстановки,

ведением переговоров в звене отделение-взвод, передачей и получением видео изображений, опознаванием целей, ведением химической разведки, обнаружением мин и другими задачами. Вычислительная система состоит из двух компьютеров: ранцевого портативного и универсальной шины USB, которая обеспечивает обмен данными между основными подсистемами.

Для удобства пользования портативный компьютер оснащен индивидуально настраиваемой системой распознавания голоса. Связь солдата с его отделением в бою поддерживается с помощью двух радиостанций: индивидуальной типа Motorola (1755-1850 МГц) и общей, сопрягаемой с системой одноканальной цифровой связи «Sincgars» (30-88 МГц), что позволяет командиру в случае необходимости ставить ему задачи и получать от него донесения. Подсистема связи обеспечивает одновременный разговор трех абонентов и передачу данных (64 Кбит) в режиме засекречивания на расстоянии до 5 км. Для связи вне зоны видимости используется ретрансляция с автоматическим поиском ближайших радиостанций других пехотинцев или воздушных ретрансляторов (самолетов или вертолетов). Общий вес двух радиостанций составляет 656 г., а габариты – 14 см х 8 см х 2,5 см.

В качестве вычислительной платформы используется IBM совместимый портативный мультимедийный компьютер с упрощенной операционной системой Windows-2000, процессором Пентиум-75 Мгц, оперативной памятью 32 Мбайт, жестким диском объемом 340 Мбайт и сменной флэшпамятью 85 Мбайт, сетевой картой Ethernet. Для подключения периферийного оборудования в компьютере имеются шины PCI и ISA, с двумя разъемами RS-232. Общий вес портативного компьютера составляет около 1200 г, а габариты без внешних соединителей – 4 см х 18 см х 27 см. Диапазон рабочих температур от -15 до 49 град Цельсия. Предусмотрено несколько типовых вариантов установки вычислительной системы в зависимости от выполняемых боевых задач: для командира, солдата, инженера, разведчика, корректировщика огня. В командирском варианте предусмотрено подключения клавиатуры с трекболом и дисплеем VGA.

Общая стоимость программы «пехотинец» оценивается в 2 млрд. $, полномасштабная реализация которой предполагает поставку в войска в течение 2001-2010 гг. 34 тысяч комплектов. По оценкам Счетной палаты Конгресса США стоимость одного комплекта снаряжения оказалось завышенной от первоначальной более чем в 2,5 раза. В январе – феврале 2001 г. в шт. Калифорния были проведены первые полевые учения в ротном звене с использованием нового комплекта снаряжения пехотинца. В ходе учений за счет использования нового снаряжения условные потери противника возросли с 55% до 100%, а собственные потери снизились с 28% до 17%. По отзывам солдат снаряжение их вполне устраивает. Все электронные компоненты безотказно работали даже в воде. Каждый боец точно знал расположение своих товарищей и всегда мог выйти на связь.

Электронная торговля

Еще в мае 1998 г. в рамках широкомасштабной и долгосрочной инициативы по реформированию вооруженных сил Пентагон открыл новую программу по созданию единой системы электронной торговли EMALL, в рамках которой предполагается упорядочить процесс закупки вооружений и предметов материально-технического снабжения войск через Интернет. Для реализации этой программы в Агентстве материально-технического снабжения (тыла) ВС США DLA было создано управление электронной коммерции JECPO. Система электронной торговли создается по принципу Интернет-портала, который связывает сайты видов вооруженных сил и коммерческих фирм-производителей в интересах создания эффективной и безопасной торговли на основе рыночного механизма через прямую продажу-покупку, что обеспечит пользователям свободный доступ к предметам военных поставок посредством электронных каталогов и электронных биржевых операций.

За счет использования системы электронной торговли Пентагон предполагает сократить от 30 до 40 промежуточных этапов закупки вооружений, сведя их фактически до 10 он-лайн операций.

Например, в классической бумажной системе при закупке на сумму в 500$ только на административные расходы тратится от 150$ до 200$, в то время как в электронной системе эти расходы составят всего 2$. При этом сама процедура бумажного оформления заказа может занимать от 1 до 3 месяцев бюрократических согласований в различных инстанциях.

К основным преимуществам создаваемой системы электронной торговли EMALL можно отнести следующие: объединение системы электронной торговли с системами тылового снабжения и финансирования войск, все предметы снабжения будут постоянно находиться под контролем по мере их заказа, оплаты и поставок, устранение дублирования в заказах, централизованная регистрация покупателей и производителей, поиск по всем правительственным источникам информации, коммерческим каталогам и электронным торговым биржам, автоматический сбор статистики и формирование отчетов, эффективный маркетинг и реклама, стандартизация заказов вооружений, налаживание контактов и взаимопонимания между видами вооруженных сил в интересах снижения стоимости программ перевооружения и их реализации.

Однако, у электронной торговли есть и свои минусы, о которых следует помнить. Это, прежде всего, безопасность транзакций при проведении покупок и продаж через Интернет, где хакеры чувствуют себя как рыба в воде.

В 1999 г. было отмечено всего около 22 тысяч попыток проникновения и снятия информации с систем Пентагона; за первые 11 месяцев 2000 г. количество таких попыток возросло до 26 500.

В целях обеспечения безопасности доступа к информационным ресурсам и секретным объектам Пентагон проводит полномасштабную замену личных номеров военного и гражданского персонала с использованием технологии пластиковых электронных карт – «smart-cards». Каждая такая карта стоимостью 6$ будет иметь микросхему с аппаратной реализацией криптографического алгоритма, индивидуальный магнитный и штрих код владельца. В период с 2000 по 2005 гг. ВМС как головная организация этой программы получит 145 млн. $ для закупки электронных карт, компьютеров, программного обеспечения и электронных замков для установки на 800 военных объектах по всему миру.

В 2000 г. в системе электронной торговли Пентагона было зафиксировано свыше 5 миллионов наименований товаров и услуг, которые были задействованы по операциям купли-продажи в общей сложности на сумму 80 млн. $. По предварительным оценкам в 2001 г. каталоги баз данных электронной торговли МО США должны расширится до 12 млн. наименований, а объем торговых сделок по военным программам должен достигнуть 143 млн. $. В настоящее время в этой системе зарегистрировано около 175 тыс. фирм-производителей, заинтересованных в работе по военным контрактам. Для сравнения: в 2000 г. в общей сложности было сделано покупок через Интернет на сумму 33 млрд. $, в которых участвовали 20000 чел. При этом общие расходы из федерального бюджета на информационные технологии за этот же период составили 37.6 млрд. $.

Заказ вооружений

По оценкам Пентагона к 2005 г. свыше 120 тысяч (50%) госслужащих, занятых в программах приобретения (заказов, закупок и поставок) военной техники и имущества для вооруженных сил США, достигнут пенсионного возраста и могут быть уволены. Под угрозу будут поставлены сотни долгосрочных военных программ, от которых зависит не только национальная безопасность, но и экономика, а также благосостояние самой богатой нации в мире. Эта тревожная тенденция вынуждает американцев активно внедрять информационные технологии в военно-промышленном бизнесе.

Параллельно с развитием системы электронной торговли Пентагон активно внедряет передовые информационные технологии непосредственно в систему приобретения вооружений по военным контрактам, которых сегодня насчитывается до 332500 на общую сумму 852 млрд. $. За пять лет было оборудовано свыше 20000 удаленных терминалов автоматизированной системы военных контрактов SPS. К 2003 г. система должна охватить 43000 пользователей в 1100

районах земного шара. По данным за 2000 г. Пентагон осуществил закупку на 32 млрд. $ товаров и услуг с помощью системы SPS. Когда система будет полностью развернута и интегрирована в сеть Интернет, американские военные рассчитывают ежегодно экономить до 1.4 млрд. $ на закупках по военным контрактам.

Космическая фотосъемка

Не секрет, что основные функции современных космических аппаратов (спутников) связаны в основном с навигацией, метеорологией, связью и разведкой. Последняя является в настоящее время одним из приоритетных направлений в обеспечении информационного превосходства практически во всех сферах жизнедеятельности современного общества: военной, политической, научно-технической и экономической.

В ближайшие несколько лет предполагается перейти полностью на систему электронной торговли продуктами космической видовой разведки через Интернет.

Министерство обороны и разведывательное сообщество США в настоящее время начинают осуществлять широкомасштабные долгосрочные программы, направленные на полную замену их спутниковых арсеналов в ближайшие десять лет, стоимость которых оценивается в 60 млрд. долларов. Одновременно ставиться задача по увеличению окупаемости капиталовложений за счет реализации коммерческих проектов в этой области. После долгих колебаний Конгресс США санкционировал возможность коммерческого доступа к изображениям, получаемым со спутников IKONOS с разрешением в 1 м. Такая точность фотосъемки использовалась американскими военными во время войны в Персидском заливе для определения позиций иракских баллистических ракет. По некоторым оценкам Национальное агентство космической фотосъемки и картографии (NIMA) планирует получить от продажи своей продукции до 1 млрд. $ в год.

Для этого планируется создать распределенную базу данных с послойным отображением участков земной поверхности в цифровом формате, доступ к которой будет осуществляться на платной основе избирательно: каждый пользователь сможет увидеть только то, что ему можно будет увидеть без ущерба национальной безопасности США и их союзникам. Информация будет накапливаться не только за счет национальных, но и иностранных орбитальных ресурсов, что позволит иметь наиболее точное и полное представление об интересующих покупателя участках в различных спектрах (видимом, инфракрасном, ультрафиолетовом), ракурсах (черно-белом, цветном, двухмерном, трехмерном) и масштабах обзора (по углу, высоте и ширине полосы съемки). Эта же информация наряду с данными агентурной и радиоэлектронной разведки будет постоянно отслеживаться в базах данных разведывательного сообщества в интересах национальной безопасности.

Разведка

В США разведкой занимаются 14 спецслужб, входящих в так называемое разведывательное сообщество: ЦРУ, Разведуправление Министерства обороны (РУМО), Агентство национальной безопасности (АНБ), органы космической разведки Пентагона, разведуправления видов вооруженных сил, бюро разведки и исследований госдепартамента, занимающиеся разведывательной деятельностью подразделения министерств юстиции и финансов, а также Федеральное бюро расследований (ФБР).

Всего на нужды разведывательного сообщества из бюджета выделяется около 28 – 30 млрд. $. Большая часть этих средств идет на технические системы сбора, обработки и распределения информации.

Информационное превосходство при проведении информационных операций стало основной задачей разведки в 21-ом веке. Из опубликованных в открытой печати материалов следует, что многие вопросы реорганизации разведки касаются в основном информационных технологий.

Анализ боевых действий в Персидском заливе, в ходе которых широко использовалось высокоточное оружие, поставил на повестку дня вопрос об эффективности использования информации, добываемой разведывательным сообществом. Были проведены комплексные исследования по проблеме реформирования и реорганизации разведки, в которых участвовали свыше шести правительственных и частных научно-исследовательских организаций.

Разведывательное сообщество стало сильно зависеть от технических систем, используемых для сбора, обработки и распределения информации. В свою очередь новые технологии оказывают влияние на работу персонала и качество самих систем.

В силу того, что каждое шпионское ведомство США по соображениям безопасности создавало свои собственные системы сбора и распределения информации (АНБ – КРИТИКОМ, РУМО – ДЖЕЙВИКС, ДОДИИС, АМХС) с течением времени назрела острая необходимость в их объединении, и уже в начале 90-х годов была поставлена задача создать в ИНТЕРНЕТ невидимый для большинства пользователей специальный закрытый или как его еще называют секретный ИНТЕРНЕТ.

Хотя в этой секретной сети, получившей название ИНТЕЛИНК, также используется традиционный протокол TCP/IP, непосредственный доступ к секретной информации осуществляется через специальный протокол HTTPS при наличии специального броузера с набором криптографических алгоритмов, поставляемого только для зарегистрированных пользователей ИНТЕЛИНК.

Сеть ИНТЕЛИНК имеет четыре уровня доступа к разведывательной информации по степени секретности: первый уровень представляет особо важная информация для принятия политических решений, которую готовит и распределяет только ЦРУ через специальную сеть ПОЛИСИНЕТ для президента и Совета безопасности; второй – информация, имеющая гриф совершенно секретно, к которой имеют доступ около 50 тыс. пользователей, среди которых в свое время была и Моника Левински, когда она работала в Пентагоне; третий – секретная информация, связанная с планированием военных операций, к которой имеют доступ 265 тыс. пользователей сети СИПРНЕТ; четвертый – несекретная информация из открытых источников (печать, ИНТЕРНЕТ, телевидение, радио), которая составляет свыше 95% всей добываемой разведкой информации.

Как считают американские специалисты пользователи разведывательной информации ожидают, что они смогут получать информацию непосредственно по своему запросу, предпочитая иметь прямые контакты с источником информации.

В случае, если такой контакт невозможен, пользователь должен знать как его информация собирается для того, чтобы оценить ее достоверность.

В настоящее время уже ведутся работы по созданию соответствующей «виртуальной аналитической среды» в рамках разведывательного сообщества, которая соединит в одно целое тех, кто собирает, распределяет, анализирует и потребляет информацию в целях повышения производительности и отдачи каждого аналитика. В рамках «виртуального аналитического сообщества», все участники которого будут интегрированы в единую информационную систему предполагается повысить требования к стандартизации информационных технологий, включая создание единого органа закупок и механизма регулирования бюджета для модернизации систем в течение всего жизненного цикла.

Борьба со шпионажем и терроризмом

Арест высокопоставленного офицера ФБР Роберта Хансена, обвиняемого в сотрудничестве с КГБ/СВР с 1986 г., вызвал самый настоящий шок в разведывательном сообществе США, где еще не успели забыть скандального разоблачения офицера ЦРУ Олдрича Эймса в 1994 г. В деле Хансена, пожалуй впервые в мировой практике шпионажа, можно говорить о прецеденте: «крота вычислил» компьютер. Роберта Хансена без всякого преувеличения можно назвать

шпионом 21-го века, который не просто использовал современные информационные технологии, но делал это виртуозно, как настоящий профессионал.

Из представленного ФБР обвинительного заключения следует, что в своей шпионской деятельности Хансен, практически избегал прямых контактов с сотрудниками российской разведки, используя для оперативной связи флэш-карты, дискеты, карманный органайзер Palm Pilot, беспроводный удаленный доступ в Интернет и криптографические программы. Как установили следователи, Хансен постоянно набирал в графе поиска специальной базы данных ФБР не только собственное имя, но и такие ключевые слова, как «Россия», «КГБ», «шпионский тайник», а также свои кодовые обозначения для связи, чтобы установить, не попал ли он под подозрение. Все запросы, которые периодически делал Хансен компьютер неумолимо записывал в специальный журнал, по которому его в конце концов и «расшифровали» сотрудники ФБР.

В настоящее время ФБР совместно с АНБ ведут работы по созданию системы контроля за электронной почтой в Интернет. На программу технического перевооружения АНБ «Ground-Breaker» Конгресс выделил свыше 5 млрд.долл. и еще около 1 млрд. долл. дополнительно на переоснащение многоцелевой атомной подводной лодки класса «Sea wolf» для прослушивания подводных кабелей связи с помощью специальной аппаратуры. Названная в честь президента США Джими Картера новая субмарина SSN-23 должна была быть спущена на воду в декабре этого года, но по настоянию АНБ было принято решение провести ее переоборудование, а спуск лодки отложить до июня 2004 г. По сведениям, просочившимся в печать, после ввода в строй новой субмарины АНБ рассчитывает прослушивать не только обычные электрические кабели связи, что оно делало и раньше, но и … волоконно-оптические! Как это удастся сделать американцам - пока не ясно: для бесконтактного перехвата экранированного светового луча еще не придуман способ. Между тем, подводная лодка-шпион будет нести на своем борту специальный контейнер-камеру, из которой может быть осуществлен беспрепятственный доступ к любым подводным объектам.

Рожденный в кабинетах американского военного ведомства таинственный призрак-невидимка информационной войны за десять лет своего виртуального существования уже успел породить не мало проблем для тех, кто его создал. Сегодня без всякого преувеличения можно утверждать, что главная из них - защита информации. По оценкам ЦРУ не менее 100 стран располагают в той или иной мере возможностями ведения информационной войны, при этом доля компьютерных вирусов в Интернете, разрушающих информацию и ее носители выросла до 30%. Однако завеса глубокой тайны и строгой секретности, первоначально опущенные Пентагоном над собственными планами информационных операций создали явную диспропорцию между желаемым и достигнутым. Для страны, все сферы жизнедеятельности которой столь прочно связаны с информационными технологиями, грань между государственными и коммерческими, военными и гражданскими системами более чем условна.

Ежегодно США расходуют на информационные технологии только из федерального бюджета порядка 38 млрд. $, из которых около 20 млрд. $ (более 50%) составляют расходы военного ведомства. И это без учета десятков млрд. $. затрачиваемых на бортовые системы управления спутников, ракет, самолетов, танков и кораблей. Сегодня Пентагон это не только один из крупнейших владельцев, арендаторов и пользователей информационных и телекоммуникационных ресурсов, ведущих заказчиков программного обеспечения, компьютерного оборудования и средств цифровой связи, но и, по сути дела, законодатель государственной политики и промышленных стандартов в области информационной безопасности. Только в 2000 г. на защиту национальных информационных ресурсов в США было выделено 1,5 млрд. $, в то время как Пентагон истратил на защиту военных информационных систем 1,1 млрд. $.

В определенной степени это сказывается и на самих понятиях, связанных с защитой информации, которые постепенно трансформируясь из чисто военных терминов приобретают характер общегосударственных и промышленных стандартов. Производители оборудования и разработчики программных продуктов, заинтересованные в крупных государственных и

военных заказах, начинают прислушиваться к тому, что говорят в коридорах Пентагона об информационной безопасности.

Осознав на собственном опыте бессмысленность защиты информационных ресурсов без участия всех заинтересованных сторон, каковыми в США являются фактически не только все государственные структуры, промышленность, частный капитал, но и рядовые граждане, военное ведомство в буквальном смысле пошло в народ, активно пропагандируя свое видение общенациональной проблемы №1. Одним из примеров такого новаторского подхода является программа DIAP (Defense Information Assurance Program), в рамках которой с участием таких ведущих фирм как Lucent Technologies, IBM, Microsoft, Intel, Cisco, Entrust, HP, Sun, GTE, Bay Networks, Axent, Network Associates, Motorola закладывается фундамент информационной безопасности не только военной инфраструктуры, но и всего американского общества в целом на ближайшие 10 лет.

Когда в декабре 1996 г. в одной из секретных директив американские военные ввели в обращение новый термин - «гарантия информации» (IA - information assurance), на это мало кто обратил внимание, учитывая первоначально ограниченный круг лиц допущенных к документу. Однако лингвистическая причуда Пентагона имела далеко идущие последствия, с которыми сегодня вынуждено считаться все большее число пользователей и производителей высоких технологий.

В соответствии с секретной директивой Пентагона S-3600.1 *гарантия информации* определяется как «информационная операция или операции, связанные с защитой информации и информационных систем за счет обеспечения их готовности (доступности), целостности, аутентичности, конфиденциальности и непротиворечивости. Данные операции включают в себя восстановление информационных систем за счет объединения возможностей защиты, обнаружения и реагирования. При этом информация не будет раскрыта лицам, процессам или устройствам, не имеющим к ней прав доступа, будет обеспечена полная достоверность факта передачи, наличия самого сообщения и его отправителя, а также проверка прав на получение отдельных категорий информации, данные остаются в исходном виде и не могут быть случайно или преднамеренно изменены или уничтожены, будет обеспечен своевременный и надежный (по требованию) доступ к данным и информационным службам установленных пользователей, а отправитель данных получит уведомление факта доставки, также как получатель - подтверждение личности отправителя, и таким образом никто не сможет отрицать своего участия в обработке данных.»

Тем самым классическое понятие информационной безопасности (INFOSEC - information security) как состояние информационных ресурсов было расширено и дополнено гарантированием их надлежащего использования даже в том случае, если эти ресурсы будут подвергнуты деструктивному воздействию как извне, так и изнутри. Иными словами в политике информационной безопасности четко обозначился сдвиг в сторону активных организационно-технических мероприятий защиты информационных ресурсов. Похоже, что американцы взяли за основу пропаганды знаний в области информационной безопасности советскую систему гражданской обороны 60-х, 70-х годов, когда население учили не только тому как надевать индивидуальные средства защиты и укрываться в бомбоубежищах, но и как вести радиационный, химический и бактериологический контроль и восстанавливать объекты народного хозяйства после применения оружия массового поражения.

Заметим, что это не единственное нововведение Пентагона в лексиконе информационных технологий, которое стало достоянием общественности не смотря на гриф секретности первоисточника. К числу таковых можно отнести следующие: «информационное противоборство», «информационное превосходство», «информационные операции (общие и специальные)», «информационная среда», «атака на компьютерные сети», «вторжение в информационные системы» и др. С некоторых пор американское военное ведомство считает полезным публиковать отдельные несекретные фрагменты из своих засекреченных официальных нормативных документов (директив, инструкций, меморандумов, уставов и наставлений), повышая информированность общества о потенциальных угрозах национальной безопасности. Военные терпеливо и

настойчиво приучают все слои населения к своей терминологии, постепенно стирая грань между государством и обществом, обороной и производством, разведкой и предпринимательством, учебой и досугом.

Как результат, американское общество начинает пожинать плоды информационной революции в виде единых универсальных стандартов, применимых как в гражданском, так и в военном секторе. В качестве примера можно привести стандарт электронной подписи (PKI - public key infrastructure) X.509, разработанный Агентством национальной безопасности для применения не только в военных, но и гражданских информационных сетях и системах. В соответствии с принятым стандартом в США к 2003 г. будут выдаваться пять классов сертификата PKI, гарантирующих информационную безопасность на основе криптографических алгоритмов с открытым ключом в зависимости от степени секретности информации. Каждый сертификат будет включать такие сведения как разновидность класса, порядковый номер, криптографический алгоритм инстанции выдавшей сертификат, наименование инстанции, срок действия (до 10 лет), ключ (до 1024 бит), цифровую подпись и др. К концу 2001 г. Пентагон должен полностью перевести свою электронную почту на стандарт PKI.

Профессиональная подготовка персонала в соответствии с новыми требованиями в области информационной безопасности является ключевым направлением реализации программы DIAP, в рамках которой на учебный процесс выделяется в общей сложности около 80 млн. $ на период до 2005 г.. При этом предполагается открыть специализированные курсы дистанционного обучения (свыше 20) в так называемом «виртуальном университете информационной безопасности» на базе сайтов в Интернете, в которых будут обучаться основам «стратегии глубокой эшелонированной защиты информационных ресурсов» администраторы (2 недели) и специалисты (3-5 дней) практически из всех федеральных ведомств, включая ЦРУ, ФБР, НАСА, Минфина, Минюста, Минэнерго и др. Ожидается, что за 5 лет будет подготовлено в общей сложности не менее 100 тыс. дипломированных специалистов в области информационной безопасности, готовых к любым неожиданностям в киберпространстве.

В каждом штате на период чрезвычайных условий (землетрясений, ураганов, наводнений, катастроф, террористических актов) создаются так называемые резервные центры обработки информации, в которых периодически собирается, накапливается и обновляется наиболее важная информация, необходимая для организации управления всех жизненно важных служб (полиции, скорой помощи, пожарной охраны и др.) в случае выхода из строя основных центров обработки информации и телекоммуникационных систем. Как правило такие центры оснащаются автономными источниками энергоснабжения (дизель - генераторами), способными поддерживать нормальный режим функционирования резервных информационных центров в течение нескольких суток до восстановления стационарной системы энергоснабжения. В повседневных условиях работу таких центров обеспечивает ограниченный по численности технический персонал, имеющий все необходимые навыки для организации работы центра в чрезвычайных условиях.

Краткий обзор только некоторых наиболее важных и дорогостоящих программ развития информационных технологий в США на примере Пентагона показывает, что проблема информационной безопасности отдельно взятого ведомства по своему масштабу уже давно является общенациональной и для своего решения требует пересмотра устоявшихся подходов, принятия единых стандартов как в промышленности, так и в бизнесе, создания национальной системы подготовки специалистов соответствующего профиля, широкого информирования населения об угрозах и мерах по их предотвращению.

Александр Леваков
(академик Академии военных наук, Jetinfo)