УДК: 355.02(510) ; 351.86(510)

ОЦЕНЕ САД О СПОСОБНОСТИМА НАРОДНООСЛОБОДИЛАЧКЕ АРМИЈЕ КИНЕ (НОАК) ЗА ВОЂЕЊЕ САЈБЕР ШПИЈУНАЖЕ[1]

Милан Миљковић
Министарство одбране Републике Србије

Сајбер ратовање и шпијунирање постаје вероватна стратегијска алтернатива за државе које су процениле да у конвенционалној војној конфронтацији са САД неће превладати. У том смислу, амерички експерти оцењују да Кина види сајбер нападе и сајбер шпијунажу као компоненте интегралне стратегије којом планира да победи технички супериорнијег и бројчано јачег противника. Због тога је НОАК усвојио стратегију под називом „Интегрисано мрежно електронско ратовање“, *wangdian yitizhan* – кинески назив, која даје смернице за примену компјутерских мрежних операција (CNO) и одговарајућих техника и алата, где значајно место има и обавештајни рад и извиђање у сајбер простору. Сматрају да је прикупљање техничких информација о војним пројектима у САД вероватно координирано од стране Кинеског информативног центра за одбрамбену науку и технологију *(CDSTIC),* који је потчињен Главном одељењу НОАК за опремање. По оцени страних експерата, у оквиру НОАК, спровођење офанзивних мисија и електронско ратовање (EW) поверено је 4. управи Генералштаба НОАК (Управа за електронска против дејства),[2] док су дефанзивне мисије и обавештајни рад поверени 3. управи ГШ НОАК (надлежној за за сигнални обавештајни рад – *SIGINT*). Оцењују да Трећа и Четврта управа ГШ НОАК имају у својој надлежности бројне јединице које надгледају и прате стране комуникационе мреже, обезбеђује безбедност компјутерских и комуникационих система НОАК и спроводе сајбер извиђање приоритетних циљева у свету. Са доктринарног аспекта, сматрају да концепт народноослободилачког рата, примењен у области обавештајног рада, путем сајбер шпијунаже од стране „сваког Кинеза који се разуме у компјутерску технологију“ представља, у ствари, примену стратегије „тоталне и масовне шпијунаже“ на коју западни обавештајни експерти још немају ефикасан одговор.

Кључне речи: *интегрисано мрежно електронско ратовање*, *компјутерске мрежне операције*, *компјутерске операције за експлоатацију (CNE), сајбер шпијунажа, извиђање у сајбер простору.*

[1] Прирећено за The US-China Economic and Security Review Commission, Northrop Grumman Corporation Information Systems Sector, 7575 Colshire Drive, McLean, VA 22102, October 9.

[2] Генералштаб НОАК чини седам управа за: оперативни обавештајни рад, сигнални обавештајни рад, електронске контрамере, комуникацију и везу, мобилизацију, спољне односе и менаџмент.

Увод

Циљеви извиђања противничких комуникационих чворова су прикупљање обавештајних података, крађа софтвера, компромитовање интегритета система или базе података друге стране, као и управљање перцепцијом противника.[3] У вези с тиме, Кина је у западним медијима јавно цитирана као актер који се најчешће појављује иза активности сајбер шпијунаже, а САД су у последње време спремне јавно да потврде да сајбер шпијунажа коју спроводи Кина представља једно од највећих и најчешћих контраобавештајних изазова за САД.

Представници Владе САД оцењују да Кина од 1990. године развија капацитете за извођење сајбер напада и шпијунаже. Наводи се сведочење бившег директора ЦИА Џорџа Тенета, пред Комитетом Сената за владина питања, 1998. године, који је тада саопштио да „ЦИА има податке да неколико држава ради на развијању капацитета за информационо ратовање".[4] Такође, цитира се сведочење експерта ЦИА за информационо ратовање Џона Серабиана, фебруара 2000. године, пред Заједничким економским комитетом у вези са сајбер капацитетима Кине.[5] Серабијан је оценио да сајбер ратовање и шпијунирање постаје „вероватна стратегијска алтернатива за државе које су процениле да у конвенционалној војној конфронтацији са САД неће превладати". Тада је представник ЦИА навео извесне оцене неидентификованог кинеског генерала, који је, по тврдњи Серабијана изнео да „ми можемо да учинимо противничке командне центре нефункционалне, тако што ћемо променити податке у њиховима базама. Осим тога, можемо да слањем дезинформација доведемо до тога да противнички командни елементи доносу погрешне одлуке".

Наводе да је Кина развила и сопствени компјутерски оперативни систем сличан Линуксу, назван Кулин, који је развијен на кинеском Националном универзитету за одбрамбене технологије и чије је коришћење одобрила Народноослободилачка армија Кине (НОАК). То се узима као доказ да су у његовој изградњи учествовале и кинеске безбедносне службе. Циљ изградње овог оперативног система је да обезбеди додатну заштиту постојећим оперативним системима западне производње који се користе у Кини. У том смислу, Кулин има исту намену као и оперативни програм *Security-Enhanced Linux* који је наменски направљен за потребе америчке Агенције за националну безбедност (U. S. National Security Agency). Прва јавна верзија Кулина објављена је 2007. године. Иначе, поједини амерички званичници заступали су ставове да је Кулин израђен да би омео напредак конкурентних земаља у области сајбер ратовања.

Амерички обавештајни експерти оцењују да Кина поседује значајне обавештајне капацитете, као и да кинеске обавештајне службе имају посебан интерес на пољу прикупљања података везаних за модерну информациону технологију. Према годишњем извештају Министарства одбране САД из 2003. године, од 1991. године у Кини постоји око 4000 индивидуалних обавештајних организација. Многе од њих повезане

[3] SANS Institute, „Security Essentials with CISSP and CBK," Volume I, 2003 p. 522.

[4] George J. Tenet, Director of the Central Intelligence Agency, Testimony Before the Senate Committee on Government Affairs, June 24, 1998 <http://www.cia.gov/cia/public_affairs/speeches/1998/dci_testimony_062498.html>

[5] Congressional testimony of John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000 <http://www.cia.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html

су са државним институцијама, предузећима, истраживачким институтима и академијама које су у вези са кинеском одбрамбеном индустријом. Сматрају да је прикупљање техничких информација вероватно координирано од стране Кинеског информативног центра за одбрамбену науку и технологију *(CDSTIC),* који је потчињен Главном одељењу НОАК за опремање. Ово одељење надгледа комплексну мрежу фабрика, института и академија који су потчињени кинеској нуклеарној, аеронаутичкој, електронској, бродској и другим индустријама. Свака од ових институција има предузећа за увоз и извоз, која олакшавају увоз технологије и знања у Кину.

Кинеске обавештајне организације, по оцени америчких експерата, агресивно прикупљају податке о америчким достигнућима у науци и технологији, дајући тежиште на сектору високе технологије концентрисаном у Јужној Калифорнији, Силиконској долини. Обавештајно покривање САД од стране Кине може да укључује 1500 кинеских дипломата распоређених у око 70 представништва у САД, 15.000 кинеских студената који сваке године допутује у САД, око 10.000 Кинеза који долазе путем 2700 делегација које сваке године посећују САД.[6]

Поред класичних обавештајних активности, информације присутне у медијима (отворени извори) засигурно помажу кинеским напорима у прикупљању потребних информација. На пример, 1991. године Кинески информативни центар за одбрамбену науку и технологију *(CDSTIC)* издао је приручник за прикупљање научних и технолошких података, који у енглеској верзији носи назив *Sources and Techniques of Obtaining National Defense Science and Technology Intelligence*. Приручник даје детаљне информације о страним „отвореним изворима" и публикацијама у којима се могу наћи подаци о одбрамбеној технологији страних земаља. Са подацима о слабим тачкама америчке информационе инфраструктуре и другим подацима добијеним из отворених извора и другим методама,[7] кинеске обавештајне службе могу да своје активности фокусирају на обавештајне активности према метама високог значаја.

Амерички експерти закључују да је Народно ослободилачка армија Кине (НОАК) препознала да оружане снаге САД умногоме зависе од технологије, и то не само по питању командовања и контроле, него и за потребе прикупљања обавештајних информација и извођења прецизних напада. Оцењују да Кина види сајбер нападе и сајбер шпијунажу као компоненте интегралне стратегије којом планира да победи технички супериорнијег и бројчано јачег противника.

Кинеска стратегија за вођење компјутерских мрежних операција и обавештајног рада у сајбер простору

Одржавање под контролом протока информација код противника, као и остваривање информационе доминације над противником су једни од кључних циљева НОАК на стратегијском и оперативном нивоу, како је наведено у два најважнија јав-

[6] Federation of American Scientists Intelligence Resource Program, "Ministry of State Services," January 1998 <http://www.fas.org/irp/world/china/mss/ops.htm>

[7] Поред регуларних војних сајбер јединица, хакери или други појединци, обучени у програмирању и коришћењу компјутерских мрежа, основни су извшиоци сајбер шпијунаже. Ови појединци су често под покровитељством и вероватном подршком државног апарата земље из које је потекао сајбер напад.

но доступна кинеска војно теоријска доктринарна документа, у Науци о војној стратегији и Науци о војним операцијама.[8]

Наука о војној стратегији и Наука о војним операцијама идентификују противнички командно информациони и обавештајно извиђачки систем (C4ISR) као мету највећег приоритета за компјутерске мрежне операције и обавештајни рад у сајбер простору.

Због тога је НОАК усвојио стратегију под називом „Интегрисано мрежно електронско ратовање", *wangdian yitizhan* – кинески назив *или* INEW- енглеска скраћеница, која даје смернице за примену компјутерских мрежних операција (CNO) и одговарајуће технике и алате, где значајно место има и обавештајни рад и извиђање у сајбер простору.

Анализирајући наведену кинеску INEW стратегију, у чланку *Jane's Intelligence Review* објављеном 2002. године, пензионисани потпуковник ОС САД Тимоти Томас наводи да ова стратегија има три елемента: 1) извиђање, 2) напад и 3) заштиту. Мрежно и електромагнетно извиђање, по његовој оцени, омогућује НОАК да прикупља информације о потенцијалним метама, развија и израђује планове за напад на противничке критичне инфраструктуре. Компјутерски информациони напади обухватају, по оцени Томаса, следеће активности: ометање, саботирање и уништавање информација у противничком компјутерском мрежном систему уз употребу специјалне компјутерске опреме или софтвера. Заштита се односи на превенцију од противничког извиђања, надгледања и напада на кинеске компјутерске системе.[9]

Усвајање ове стратегије наводи на закључак америчке експерте да НОАК планира употребу компјутерско мрежних операција, како у мирнодопско време тако и за време ратних операција. INEW стратегија, заснива се на примени електронског ратовања (EW) у циљу извиђања, загушења, обмањивања и потискивања противничког информационог тока (од тренутка стицања информације, њене обраде, до њене дистрибуције). На основу тога, може да се закључи да НОАК, употребом операција CNA, има намеру да саботажом информационог тока противника утиче на његову перцепцију".[10]

Иначе, сматрају да је идејни творац *INEW* стратегије генерал мајор *Dai Qingmin*, промотер модернизације капацитета НОАК за вођење информационих операција. Оно што је интересантно јесте да поједини ставови генерала *Dai Qingmina*, и других кинеских експерата, потврђују да је Кина одлучна да развије и капацитете за спровођење сајбер шпијунаже и обмањивања. Током 2002. године, генерал Dai Qingmin, је у престижном листу *Кинеска војна наука* изнео шест форми информационог ратовања које развија НОАК. То су:

– оперативна безбедност,
– обмана,
– компјутерско-мрежни напади,
– електронско ратовање,
– обавештајни рад и
– физичка деструкција.[11]

[8] Wang Houqing and Zhang Xingye, chief editors, The Science of Campaigns, Beijing, National Defense University Press, May 2000. See chapter six, section one for an overview of information warfare in campaign settings. Peng Guangqiang and Yao Youzhi, eds, The Science of Military Strategy, Military Science Publishing House, English edition, 2005, p. 338.

[9] Jane's Intelligence Review,„Confrontation central to Chinese cyber warfare aims," June 1, 2002.

[10] OSC, CPP20020624000214, „On Integrating Network Warfare and Electronic Warfare," China Military Science, Academy of Military Science, Winter 2002.

[11] Dai Qingmin, „On Integrating Network Warfare and Electronic Warfare," China Military Science, Feb 2002, pp 112–117 as translated and downloaded from the FBIS web site.

Осим тога, *Dai Qingmin* је у чланку под називом „Нови погледи о информационом ратовању“ (*Innovating and Developing Views on Information Operations)* изнео да Кина своје технолошке недостатке може да превазиђе развијањем и применом добрих стратегија сајбер ратовања.[12] Неке од тих стратегија су: „Ометање или саботирање противничког информационог система, стварајући код противника лажну слику о намерама наших снага, уз истовремено извођење изненадног информационог напада, због чега непријатељ има погрешан увид о нашим намерама и због тога спроводи погрешне акције“.

Dai Qingmin наводи и девет метода сајбер и електронског ратовања, а поред осталих метод сајбер шпијунирања и обмањивања, коришћених у сајбер вежбама НОАК:

– убацивање информационих бомби.
– извођење информационог-електронског извиђања;
– измена података у рачунарским базама и мрежама;
– бацање информационог смећа;
– ширење пропаганде;
– спровођење информативног обмањивања;
– пласирање клонираних информација;
– организовање информационе одбране;
– формирање умрежених станица за прикупљање обавештајних података.[13]

Осим Dai Qingmina, и други истраживачи са Кинеске академије за војне науке, Кинеског националног одбрамбеног универзитета и Академије за командовање и комуникације у Wuhan-у објавило је радове везане за сајбер ратовање.[14] Интересантно је приметити да се кинески експерти, у својим текстовима, више фокусирају на извођење психолошких операција, обавештајни рад и обмањивање путем операција у сајбер простору, за разлику од америчких стручњака који тежиште у раду дају на компјутерским мрежним нападима.[15]

Повећан значај информационог ратовања (IW) у теорији и пракси Народноослободилачке армије Кине, усвајање INEW стратегије и ставови о значају примене обавештајних активности у сајбер простору, по оцени страних експерата, указује на то да Кина развија свеобухватне технике сајбер шпијунаже (computer network exploitation – CNE) ради подршке обавештајне делатности стратегијског значаја и стварања добре основе за успех у будућим конфликтима.

Водеће кинеске јединице за извођење компјутерских мрежних операција и обавештајни рад у сајбер простору

Као што је наведено, кинеска стратегија за интегрисано мрежно електронско ратовање *(Integrated Network Electronic Warfare – INEW)* подразумева примену офанзивних, тј. компјутерских мрежних нападних операција *(computer network attack* –

[12] Major General Dai Qingmin„Innovating and Developing Views on Information Operations," Beijing Zhongguo Junshi Kexue [China's Military Science Journal, Beijing] August 2000.

[13] Major General Dai Qingmin, „Innovating and Developing Views on Information Operations," Beijing Zhongguo Junshi Kexue, [China's Military Science Journal] August 2000.

[14] Op. cit. Department of Defense 2003 p. 36.

[15] Edward Sobieski writes that this could come as a result of the fundamental differences in strategic planning exhibited by Western and Eastern military planners, analogizing the differences in strategy with the differences between the games of Go and Chess. Op. cit. Sobieski 2001.

CNA) и дефанзивних задатака, где се сврставају обавештајна делатност у сајбер простору (*CNE)* и компјутерско-мрежна одбрана (*CNO)*.[16]

По оцени страних експерата, у оквиру НОАК, спровођење офанзивних мисија и електронско ратовање (EW) поверено је 4. управи Генералштаба НОАК (Управа за електронска против дејства),[17] док су дефанзивне мисије и обавештајни рад поверени 3. управи ГШ НОАК (надлежној за за сигнални обавештајни рад – *SIGINT*). Осим тога, западни стручњаци не потцењују ни значај многих јединица Милиције НОАК које су специјализоване за информационо ратовање.

Као посебно важан моменат за увођење сајбер нападних операција и сајбер шпијунаже у доктрину и праксу НОАК оцењују постављење генерала *Dai Qingmina* 2000. године за шефа 4. управе ГШ НОАК. Сматрају да је његовим постављењем 4. управа добила надлежност за вођење информационог ратовања и тиме је Кина почела са практичним спровођењем INEW стратегије.[18] У сваком случају, 3. и 4. управа ГШ НОАК сматрају се за две најзначајније кинеске формације надлежне за извођење сајбер операција.

Трећа управа ГШ НОАК

Трећа управа је раније носила назив Други биро Централне војне комисије и састојао се од три организационе целине које су биле одговорне за прикупљање, превођење и дешифровање страних војних података.[19]

Трећа управа ГШ НОАК, која је већ дуже време надлежна за реализацију сигналних обавештајних активности (SIGINT), упркос чињеници да у прошлости није спроводила офанзивне активности, са бројним особљем, искусним преводиоцима и техничарима, сматра се веома погодном за извођење компјутерских одбрамбених (CND) и шпијунских активности (CNE).

Ова управа има под својом надлежношћу бројне станице за сигнални обавештајни рад (SIGINT) на територији свих војних области Кине.[20] Намена јој је праћење и прикупљање података о страним сигналним комуникацијама, њихова анализа, као и заштита комуникација унутар НОАК.

---

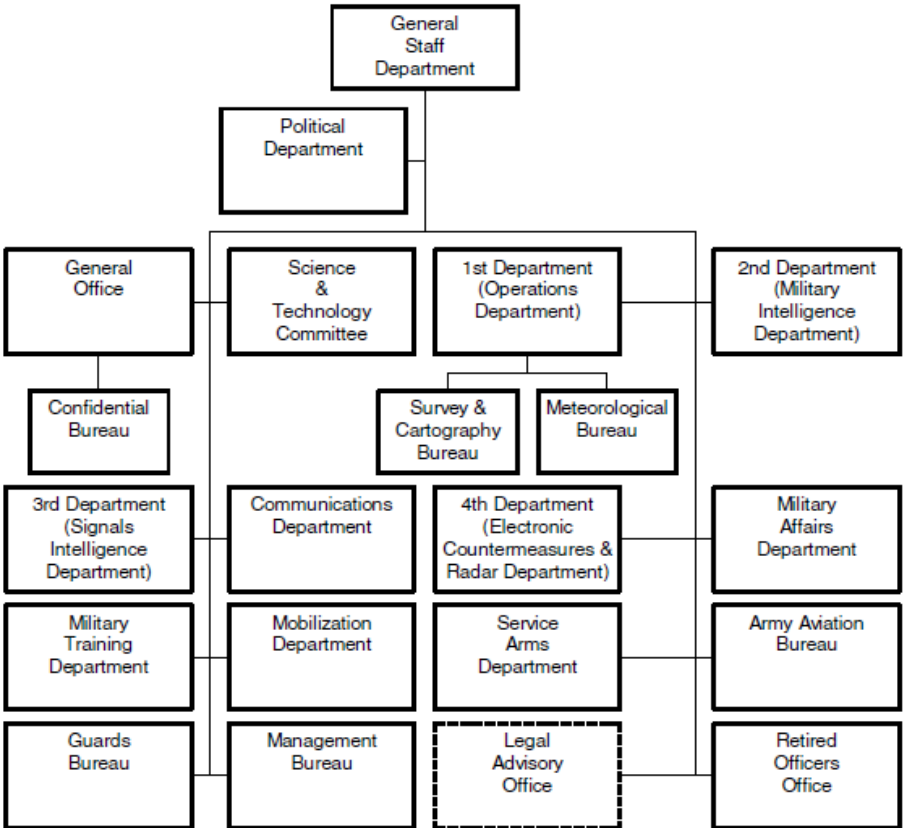
[16] Компјутерско-мрежне операције (CNO) једне су од најсавременијих и најмодернијих способности развијених за потребе подршке војних операција. Значај тих операција порастао је са наглим порастом коришћења умрежених компјутерских система и телекомуникационе инфраструктуре од стране војних и цивилних структура и организација. Компјутерско-мрежне операције (CNO), заједно са електронским ратовањем, користе се за напад, ометање, прекид и уништење противничких информационих и копјутерских система. У војним операцијама компјутерско-мрежне операције деле се на нападне (CNA) и одбрамбене (CND) и повезане компјутерске операције за експлоатацију (CNE). Компјутерске операције за експлоатацију омогућавају извођење операција и обавештајно прикупљање података преко компјутерских мрежа, са циљем да се из противничких база података прикупљају подаци.

[17] Генералштаб НОАК је састављен од седам управа за: оперативни обавештајни рад, сигнални обавештајни рад, електронске контрамере, комуникацију и везу, мобилизацију, спољне односе и менаџмент.

[18] Regarding the GSD 4th Department's leadership of the IW mission, see James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Beyond the Strait: PLA Missions Other Than Taiwan, Roy Kamphausen, David Lai, Andrew Scobell, eds., Strategic Studies Institute, April 2009, p. 272–273.

[19] The Third Department is also known as the Technical Reconnaissance Department. See –Lantern Through the Night: Central Military Commission Second Bureau, Xinhua, July 4, 2011, at http://www.js.xinhuanet.com/xin_wen_zhong_xin/2011-07/04/content_23160214.htm.

[20] Desmond Ball, „Signals Intelligence In China" Jane's Intelligence Review, 1 August, 1995.



Слика 1 – *Генералштаб НОАК*[21]

Мрежа SIGINT уређаја и инсталација у надлежности Треће управе је по процени америчких експерата способна за надгледање свих радио и телефонских комуникација. Са друге стране, Трећа управа такође је надлежна за заштиту компјутерских система НОАК, ради спречавања приступа осетљивим и тајним информацијама од значаја за националну безбедност.

Као њен пандан у САД, Агенција за националну безбедност – NSA, Трећа управа је проширила своје досадашње и традиционалне SIGINT активности. Сајбер шпијунажа или компјутерско-мрежна експлоатација (computer network exploitation CNE), како га називају у америчкој терминологији, представља најмодернију SIGINT активност и Трећа управа вероватно представља национални извршни орган за спровођење сајбер шпијунаже (CNE), пре свега због своје традиционалне главне

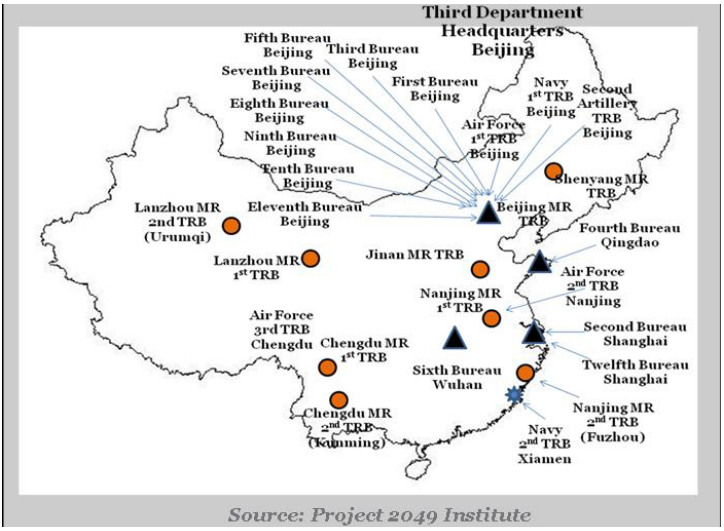
[21] Organizational chart from „The General Staff Department Of The Chinese People's Liberation Army: Organization, Roles, & Missions," by David Finkelstein, in The People's Liberation Army as Organization Reference Volume v1.0, James C. Mulvenon and Andrew N. D. Yang, eds, RAND Corp., 2002.

надлежности за SIGINT на државном нивоу, компјутерских и техничких капацитета за енкрипцију и декрипцију, као и највећи број запослених лингвиста.[22] Према незваничним изворима, Трећа управа ГШ НОАК има око 130.000 запослених, распоређених у штабовима 12 оперативних бироа и три истраживачка института.

Оперативни бирои Треће управе НОАК

Трећа управа ГШ НОАК има директну надлежност над 12 оперативних бироа. Штабови осам од дванаест бироа смештени су у Пекингу – два су базирана у Шангају, један у месту Qingdao, а један у месту Wuhan.[23]

Оперативне бирое Треће управе треба разликовати од Бироа за техничко извиђање *(Technical Reconnaissance Bureaus – TRBs)*, који се налазе под командом седам војних области, као и од бироа у надлежности видовских команди.[24]



Слика 2 – *Размештаји бироа за извиђање НОАК*

[22] See James Mulvenon, —PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability,ll in *Beyond the Strait: PLA Missions Other Than Taiwan*, eds. Roy Kamphausen, David Lai, and Andrew Scobell, Strategic Studies Institute, U.S. Army War College, April 2009, p. 274; and Bryan Krekel, —Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Northrop Grumman Corporation Information Systems Sector Report for the US-China Economic and Security Review Commission, at http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf. For an excellent review of Chinese cyber operations, see Desmond Ball, —China's Cyber Warfare Capabilities, Security Challenges (Australia), Vol. 7, No. 2 (Winter 2011), pp. 81-103, at http://www.securitychallenges.org.au/ArticlePages/vol7no2Ball.html.

[23] For reference to the First, Eighth, and S&T Intelligence Bureaus in Hanjiachuan, see – Introduction to the Hanjiachuan Military Retiree Institute, Haidian District Military Retiree Network, http://hdjxb.bjhd.gov.cn/znjg/jxs/jxs12/.

[24] Бирои за техничко извиђање (TRBs) своје извештаје достављају командама војних области и командама видова. Међутим, сматра се да Треће одељење НОАК овим бироима доставља задатке и смернице општег нивоа, као и задатке за прикупљање и анализу одређених СИГИНТ обавештајних података.

Бирои који су потчињени Трећој управи ГШ НОАК имају специфичне задатке, као што је пресретање радио и сателитске комуникације, криптологија, превођење страних порука и комуникација, информациона безбедност и обавештајна аналитика. Поред надгледања унутрашње комуникације између јединица НОАК, бирои Треће управе, који су размештени дуж кинеске границе, могу да надгледају и прате радио-саобраћај у иностранству и лоцирају стране предајнике путем радио-гониометрисања.

Штаб Првог бироа (Јединица 61786) налази се, као и Команда Треће управе, у северозападном делу Пекинга. У његовој надлежности је најмање 12 подбироа који су активни у различитим деловима Кине и немају регионалне задатке (покривање одређене територије) него функционалне, као што су декрипција, енкрипција и други задаци у вези са информационом безбедношћу.

Други биро (Јединица 61398) највероватније покрива територију САД и Канаде, фокусирајући се на политичке, економске и војне обавештајне податке. Потчињени подбирои су концентрисани у Шангају, осим једног за који се верује да се налази у близини места Kunming.

Трећи биро (Јединица 61785) и његов штаб налази се у јужном делу Пекинга, у предграђу Daxing. Трећи биро исто има функционалну мисију. С обзиром на потчињене саставе, мисија Трећег бироа може бити праћење радио-комуникација дуж граница Кине, радиогониометрисање и проналажење локација емитера. Биро има најмање 13 потчињених јединица.

Четврти биро (Јединица 61419) и његов штаб налази се у месту Qingdao и сматра се да је Четврти биро територијално надлежан за Јапан и Кореју.

Пети биро (Јединица 61565) и његов штаб налази се у у Пекингу, у дистрикту Daxing и највероватније да је тај биро територијално надлежан за Русију.

Шести биро (јединица 61726) и његов штаб смештен је у месту Wuhan, у дистрикту Wuchang. Његови подбирои распоређени су широм централне Кине, од града Xiamen на источној обали, до града Yunnan, што индикује да су усмерени ка Тајвану и Јужној Азији.

Седми биро (Јединица 61580) и његов штаб смештени су у североисточном пекиншком дистрикту Haidian. Задатак седмог бироа још није дефинисан. Подељен је на најмање десет подбироа. Запошљава преводиоце енглеског језика. Одређени инжењери специјализовали су компјутерско-мрежну одбрану и напад.

Осми биро (Јединица 61046) је, ценећи стране језике којима говоре његови припадници, вероватно фокусиран на западну и источну Европу, као и средњи Исток, Африку и Латинску Америку.

Девети биро вероватно служи Трећој управи ГШ НОАК за израду стратегијских обавештајних анализа и за управљање великим базама података. У односу на остале бирое најмање података има о овом бироу.

Десети биро (Јединица 61886) и његов штаб, који је некад носио ознаку јединица 7911 , налази се у Пекингу, у његовом северозападном делу, у насељу Xinxi Road. Овај биро је вероватно одговоран за територију Централне Азије, као и према одређеним областима у Русији, тежишно пратећи активности Русије на плану ракетних и нуклеарних проба.

Једанаести биро (Јединица 61672), распоред и концентрација његових подбироа на северу Кине, као и чињеница да његови лингвисти знају руски језик, указују да су његове активности усмерене према Русији. Остаје непознаница која је разлика у задацима овог и петог бироа, који такође у свом саставу има руске лингвисте.

Дванаести биро (Јединица 61486) и његов штаб налази се у Пекингу, у дистрикту Zhabei. Сматра се да је функционални задатак овог бироа праћење сателита, пресретање сателитске комуникације и прикупљање обавештајних SIGINT података путем прикупљачких станица лоцираних у свемиру.

Амерички обавештајни стручњаци закључују да специфични бирои Треће управе који су надлежни за сајбер шпијунажу (компјутерско-мрежну експлоатацију – CNE) остају и даље недовољно описани. Седми биро доводи се у везу са техничким аспектима сајбер операција. Осим тога, за поједине регионалне бирое, као што је Први биро, или Четврти биро у месту Qingdao, сматра се да су одговорни за превођење информација које су добијене пресретањем или путем сајбер извиђања, као и продукцију обавештајних информација добијених од преведених материјала. Такође, цени се да је Дванаести биро, који је одговоран за техничких извиђање, (TECHINT) проширио обим својих надлежности.

Истраживачки институти Треће управе НОАК

Команда Треће Управе има у свом саставу и целине надлежне за научно- истраживачки рад, као што су Научно-технолошки биро за сигнални обавештајни рад, Биро за сајбер извиђачку инфраструктуру и Биро за науку, технологију и опремање. Биро за науку, технологију и опремање у својој надлежности има три института која су одговорна за развој компјутерске опреме, сензорске технологије и криптографије. То су:

– 56. истраживачки институт. Народноослободилачка армија Кине поседује једне од најбржих суперкомпјутера. Овај институт је лоциран у месту Wuxi, у провинцији Jiangsu. Суперкомпјутери омогућавају формирање и разбијање софистицираних кодова и лозинки, што је изгледа један од задатака ових истраживачких института.

– 57. истраживачки институт, који је надлежан је за развој система за пресретање и обраду сигнала и

– 58. истраживачки институт, који је вероватно фокусиран на развој криптологије и информационе безбедности.

Четврта управа ГШ НОАК

Дискусија о кинеској сајбер инфраструктури била би некомплетна без разматрања улоге Четврте управе ГШ НОАК, надлежне за електронско ратовање. Ова управа, која је формирана 1990. године, одговорна је за вођење електронског ратовања (EW), укључујући ELINT и тактичке електронске подршке (ESM). Традиционална улога ове управе у извођењу офанзивних операција електронског ратовања (EW), постављање генерала Dai Qingmina за руководећег ове управе 2000. године, као и подаци из отворених извора о улози ове управе у примени INEW стратегије, указују, како сматрају амерички експерти, да ова управа има примарну надлежност у спровођењу офанзивних облика сајбер операција.

Четврта управа, која је вероватно надлежна за компјутерске мрежне нападе (CNA), има под својом командом најмање четири бироа, једну бригаду и два пука.

Сви они који треба да постану припадници Четврте управе обучавају се у Електротехничкој академији НОАК у месту Hefei.

Оперативне јединице Четврте управе су *ECM* бригада са штабом у месту Langfang, потчињени батаљони у местима Anhui, Jiangxi, Shandong и другим локацијама у Кини. Најмање две јединице су стациониране на Hainan острвима, од којих се једна највероватније ангажује на праћењу сателита САД. Јединице нивоа пукова распоређене су на Hainan острву и вероватно се такође користе за праћење страних сателита.

Бирои за техничко извиђање *(Technical Reconnaissance Bureaus*) у надлежности војних области

Бирои за техничко извиђање који су у надлежности седам војних области Кине, чији се Штабови налазе у местима Beijing, Chengdu, Guangzhou, Jinan, Lanzhou, Nanjing и Shenyang одговорни су за сигнални обавештајно-извиђачки рад према тактичким и стратегијским циљевима противника, али имају и задатак да реализују компијутерске-мрежне операције.[25] Задаци Бироа за техничко извиђање су прикупљање обавештајних података, лоцирање СИГИНТ система страних оружаних снага, анализа радио саобраћаја страних земаља, превођење, криптологија, компјутерска мрежна одбрана и компјутерска експлоатација (сајбер шпијунажа). Међутим, њихова примарна улога је подршка командама војних области, као и подршка граничним јединицама НОАК. Свака војна област под својом командом има најмање један биро за техничко извиђање.

Биро за техничко извиђање (Јединица 66407) **пекиншке војне области** је са својим штабом лоциран у планинском делу области Xiangshan. У свом саставу има руске лингвисте, а потчињене јединице су лоциране дуж границе са Монголијом.

Војна област Chengdu има два бироа за техничко извиђање. Први биро (Јединица 78006) има штаб у Chengdu. Забележена је потражња ове јединице за енглеским лингвистима. Други биро је лоциран у северном делу Kunminga са потчињеним јединицама у Baoshan, Malipo, и другим пограничним градовима.

Војна област Guangzhou (Јединица 75770) има биро за техничко извиђање са штабом у предграђу Guangzhoua и по својом командом има најмање осам јединица које су распоређене у јужном делу Кине. Регистровано је да су припадници овог бироа били ангажовани на праћењу комуникација преко интернета (VOIP) и проучавању интернет вируса.

Војна област Jinan има под својом командом биро за техничко извиђање (Јединица 72959) који је лоциран у месту Jinan, и цени се да запошљава око 670 специјалиста за разну технику, укључујући стручњаке за микроталасне релејне пресретаче.

Војна област Lanzhou има у својој надлежности два бироа за техничко извиђање. Први биро (Јединица 68002), који је лоциран у јужном делу града Lanzhou, у

[25] Dennis Blasko, „PLA Ground Force Modernization and Mission Diversification: Underway in all Military Regions," in Right Sizing the People's Liberation Army: Exploring the Contours of China's Military, Roy Kamphausen, Andrew Scobell, eds., Strategic Studies Institute, September 2007, p. 366- 372 Ellis L. Melvin, A Study Of The Chinese People's Liberation Army Military Region Headquarters Department Technical Reconnaissance Bureau, June 19, 2005 | Virtual Information Center, People's Republic of China Primer, 04 August 2006, available at: http://www1.apaninfo. net/Portals/45/VIC_Products/2006/08/060804-P-China.doc.

дистрикту Qilihe, има потчињене јединице у местима Kashi's Shule, Altay и Yining, које вероватно прате војне активности дуж кинеске границе са Индијом, Пакистаном, Таџикистаном, Киргистаном, Казахстаном, Русијом и Монголијом.

Војна област Nanjing има у својој надлежности два бироа за техничко извиђање који су вероватно усмерени према војним активностима Тајвана, као и активностима САД у Западном Пацифику.

Биро за техничко извиђање **Војне области Shenyang** (Јединица 65016), који је лоциран у Shenyan, у дистрикту Dongling, усмерен је према циљевима у Русији, Кореји и Јапану.

Јединице Милиције НОАК за информационо ратовање

Од 2000-те године, НОАК је почео са формирањем јединица Милиције НОАК за информационо ратовање,[26] које су попуњене стручњацима из комерцијалног ИТ сектора. Ове јединице представљају „оперативну везу" између јединица НОАК за вођење компјутерских мрежних операција и кинеских цивилних експерата за вођење CNO.[27]

Као пример наводи се податак да је почетком 2003. године у кинеским медијима објављена иницијатива власти из војног региона Guangzhou за формирање јединица милиције НОАК за информационо ратовање (IW) уз помоћ локалних ИТ компанија, које би биле база за персоналну, финансијску и инфраструктурну подршку јединицама Милиције НОАК за информационо ратовање.[28] Тако је гарнизон Guangzhou, користећи капацитете локалних ИТ фирми, формирао четири милицијска батаљона за вођење информационог ратовања.[29]

Осим тога, милицијска јединица у гарнизону Tianjin извршила је 2004. године преформацију потчињених јединица ради повећања капацитета за извођење операција под „ информатизованим условима", укључујући формирање наменских јединица за вођење информационих операција, како наводи дневни лист НОАК.[30]

---

[26] The PLA's 8 million strong militia system, under the control of the State Council and the Central Military Commission (CMC), is an active reserve system comprised of males 18-35 who are not currently serving in the PLA; the militia system augments active duty PLA units in virtually every area of military operations. See: China's National Defense in 2004, Information Office of China's State Council, December 2004, http://english.peopledaily.com.cn/whitepaper/defense2004/defense2004.html | China's National Defense in 2006¸ Information Office of the State Council of the People's Republic of China, December 2006, Beijing, available at: http://english.chinamil.com.cn/site2/newschannels/ 2006-12/29/content_691844.htm

[27] OSC, CPP20031002000138„Telecom Experts in Guangzhou Doubling As Militia Information Warfare Elements," Guofang, Academy of Military Science, 15 September 2003 | OSC, „PLA C4ISR Activities Roundup, 1 April-30 May 2006.

[28] „*Minbing Wangluo Zhan Fendui Zhize* (Duties of the Network Warfare Militia Unit), 16 March, 2008, available at: http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp?infoNo=26366. | China And Northeast Asia," *Jane's Sentinel Security Assessment* , April 3, 2009. | OSCCPP20090102670001, „PRC S&T: Ezhou Militia Establishes Network Presence," *Guofang,* Academy of Military Science, May 2001. | OSC, CPP20031002000138 „Telecom Experts in Guangzhou Doubling As Militia Information Warfare Elements," *Guofang,* Academy of Military Science, 15 September 2003.

[29] OSC, CPP20031002000138, Ibid. The exact date of creation for this unit is not specified in article, published in late 2003, however, the authors make reference to a series of these units' technical accomplishments that suggest the battalions were operational at the time of writing.

[30] OSC, CPP20050301000186, „Roundup of C4I Activities in PRC, 13 November 2004-15 January 2005," 15 January 2005.

Оцене о повезаности кинеских хакерских организација и НОАК

Аналитичари САД сматрају да хакере у Кини не спонзорише држава, већ су „контролисани од стране државе".[31] Као доказ тога наводе примере масовне мобилизације кинеских грађана за вођење сајбер операција и то после значајних међународних инцидената. На пример, после бомбардовања кинеске амбасаде у Београду, маја 1999. године, кинески хакери су напали бројне америчке политичке, војне и цивилне сајтове. Следећи пример је инцидент између извиђачког авиона РВ ОС САД и кинеског борбеног авиона 1. априла 2001. године, после чега су кинеске хакерске групе, као што је „Honker Union of China" и „Chinese Red Guest Network Security Technology Alliance", организовали масовне нападе на америчке компјутерске системе. Амерички извори, као интересантан податак, наводе чињеницу да се патриотска хакерска група Black Eagle Base, чији су припадници били ухапшени 2006. године, захвалила Министарству за државну безбедност[32] (guojia anquan ju) и Комисији НОАК за науку и технологију (COSTIND) за обуку њених припадника док су се налазили у затвору.

Наводе да су у међувремену многе од раније истакнутијих кинеских хакерских група трансформирале у легитимне фирме за компјутерску безбедност. Велике групе као што су „Xfocus" and „Black Eagle Base" преформирале су се у комерцијалне ИТ компаније и цени се да су у тесној вези са кинеском државном безбедношћу. Тако је на пример компанија „NSFocus", истакнута фирма за компјутерску и информациону безбедност, потекла од хакерске групе „Green Army Alliance", која је била посебно активна од 1997. до 2000. године.[33]

Амерички експерти претпостављају да је у целокупној операцији сајбер шпијунаже ангажован велики број група или појединаца који су појединачно ангажовани на различитим задацима. Ове групе су вероватно комбинација припадника НОАК, цивилне обавештајне службе и хакера. Овакве врсте напада често почињу са email порукама које у себи имају додате (attached) фајлове, који садрже програме који нападачу омогућавају да има контролу над компјутером жртве. Када такав фајл, обично слику или документ отвори програм компјутера жртве (Powerpoint, Wordpad, Adobe Acrobat или другим) почиње са активирањем „backdoor" програма. Тај иницијални продор emil-ом и злонамерним програмима често је само прва фаза напредне операције, јер подаци на рачунару прве жртве напада најчешће нису стварна мета нападача.

Анализа форензичких података у вези са продором злонамерних програма приписују се софистицираним операторима, хакерима, које спонзоришу државе, који су одговорни за специфичне задатке, као што су: 1) добијање и успостављање приступа мрежи, 2) извиђање циљне мреже ради идентификације информација од вредности и 3) извлачење података.

---

[31] iDefense, „Inside the China Eagle Union hacker group," *iDefense Intelligence Operations*, April 29, 2002 [White paper available upon request sent to iDefense at di@idefense.com]

[32] *US-China Economic and Security Review Commission Report on the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation October 9, 2009http://news.cnet.com/8301-13639_3-10381621-42.html?part=rss&subj=news&tag=2547-1_3-0-20*

[33] Scott Henderson, The Dark Visitor, p.29.

1) Први тим је намењен за улазак у компјутер жртве, одржавање флексибилног присуства на циљној мрежи и обезбеђивање да не само једна „врата“ остану отворена, већ да постоји више доступних врата, у случају да нека постану „затворена“;

2) Када је први тим успешно успоставио приступ противничкој мрежи, могуће је претпоставити да други тим обавља задатке извиђања, лоцирања и ексфилтрације циљаних података.

Користећи познавање противничке компјутерске мреже *(network intelligence)* током ранијих операција извиђања, тимови копирају податке са сервера противника до другог сервер који се понаша као „пролазна тачка“, где се прикупљени подаци компресују, шифрују, умножавају пре него што се испоручују кроз шифроване канале до више екстерних сервера који делују као „тачке за испоруку“. Ове крајње тачке, такође, могу бити маскиране, обезбеђујући да истражитељи не идентификују крајње одредиште података.[34]

Амерички експерти као доказ тврдње о могућем ангажовању хакера од стране НОАК наводе ставове кинеског експерта *Shen Weiguanga,* који су изнети у једном од првих докумената везаних за кинеску доктрину сајбер операција: „Они који ће узети улогу у информационом ратовању, не морају бити војници. Било ко, ко се разуме у компјутере може да постане 'борац у мрежи'…., брза мобилизација за потребе сајбер рата неће бити усмерена само према младим људима, ……. информационе и телекомуникационе компаније ће бити прве мобилизоване и прве ће бити ангажоване у борбеним операцијама ....“.[35]

Shen Weiguang, који сада важи за водећег стручњака у овој области, на тај начин описује концепт „борбе из куће“, која представља измењени и много персоналнији вид народноослободилачког рата, који ће многи Кинези водити из својих домова и са својим компјутерима.

Хипотетички, амерички експерти сматрају да НОАК ангажује хакерске организације користећи доктрину и филозофију „наоружаног народа“, што говори да тај концепт доживљава свој препород, користећи масовност и присутност компјутерске технике и претварајући је у масовно оружје. У закључку износе предност овог концепта, сматрајући да је, у поређењу са западним концептом обучавања великог броја војних специјалиста за сајбер ратовање, нискобуџетне хакерске групе могу да, исто тако, значајно подрже војне сајбер операције званичних оружаних снага, уз знатно мање ангажовање владиних капацитета.

Закључак

Америчке процене су да је Кина формулисала и примењује интегрисану стратегију дипломатске, информационе, војне и економке политике ради постизања националних циљева. Централна обавештајна агенција (ЦИА) и Министарство одбране САД у својим извештајима оцењују да Кина види сајбер ратовање као одрживу асиметричну стратегију у случају сукоба са технолошки супериорнијим противником.

[34] Brian Grow, Keith Epstein and Chi-Chu Tschang, „The New E-spionage Threat,” BusinessWeek, April 10, 2008, available online at:http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

[35] Lieutenant Colonel (ret.) Timothy L. Thomas, „Behind the Great Firewall of China: A Look at RMA/cyber warfare Theory From 1996-1998,” November, 1998, <http://fmso.leavenworth.army.mil/fmsopubs/issues/chinarma.htm>

Оцењују да су НОАК и кинеске безбедносне службе почеле са широком применом капацитета за сајбер шпијунажу ради интензивирања обавештајних операција према САД и другим развијеним земљама. Објашњавају да категорија података који су украдени немају инхерентну новчану вредност, као што имају бројеви кредитних картица или банковних рачуна, што је често у фокусу сајбер криминалних организација. Значајне информације војне и војнотехничке природе или анализе политике Владе САД нису такве да могу да се лако учине вредним и платежним на тржишту криминала, осим уколико немају купце које спонзорише држава, што подразумева целу активност спонзорише држава, без обзира на припадност оператера на рачунару који изводи операцију сајбер шпијунаже.

Обим ових сајбер операција, дубоко познавање противничке компјутерске мреже, карактеристика и природа података који су „извучени“, указује да нападаче подржава страна која је укључена у активности у вези са одбрамбеном технологијом, у активности односа Кине и САД, као и у прикупљање војних и обавештајних података о информационом систему и операцијама ОС САД.

Сматрају да Кина вероватно користи напредне капацитете НОАК за сајбер шпијунажу (CNE) ради подршке њене обавештајне активности усмерене према америчким владиним институцијама и индустријском сектору, уз коришћење дуготрајне, софистициране операције сајбер шпијунаже. За америчку страну проблем представља чињеница да су то дисциплиноване, стандардизоване операције које се примењују са софистицираном техником, уз примену најмодернијих софтвера, са дубоким познавањем противничке компјутерске мреже, као и са способношћу да се одрже активности непримећено у противничкој мрежи, некад и у трајању од неколико месеци, што компијутерски експерти називају *zero – day attack*.

Оцењују да Трећа и Четврта управа ГШ НОАК имају у својој надлежности бројне јединице које надгледају и прате стране комуникационе мреже, обезбеђују безбедност компјутерских и комуникационих система НОАК и спроводе сајбер извиђање приоритетних циљева у свету. Један од његових најјачих капацитета су велики број лингвиста који су специјализовани за области банкарства и финансијских трансакција, војних активности, енергетике и дипломатских послова. Комбинацијом примене СИГИНТ и компјутерскомрежне експлоатације (CNE), тј. сајбер шпијунаже, аналитичком обрадом обједињених материјала добијених од транскрипта телефонских разговора и пресретнутих e-mail порука, омогућава разумевање планова, способности, и активности организација или појединаца у блиској будућности. Технологија за препознавање кључних речи и гласова омогућава велику ефикасност у сакупљању информација усмерених према одређеним личностима и метама. Унапређени компјутери омогућавају ефикасно разбијање и енкрипцију софистицираних кодова и лозинки. Осим тога, надгледање и праћење појединих комуникационих канала могу да подрже софистициране психолошке операције и операције управљање перцепције противника. На основу расположивих информација, сматрају да Трећа управа ГШ НОАК има капацитета за спровођење CNE операција.

Са доктринарног аспекта, оцењују да концепт народноослободилачког рата, примењен у области обавештајног рада, путем сајбер шпијунаже од стране „сваког Кинеза који се разуме у компјутерску технологију“ представља, у ствари, примену стратегије „тоталне и масовне шпијунаже“ на коју западни обавештајни експерти још немају ефикасан одговор.

Литература

1. Academy of Military Science, May 2001. | OSC, CPP20031002000138 „Telecom Experts in Guangzhou Doubling As Militia Information Warfare Elements," Guofang, Academy of MilitaryScience, 15 September 2003.

2. Brian Grow, Keith Epstein and Chi-Chu Tschang, „The New E-spionage Threat," BusinessWeek, April10,2008,availableonline at: http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

3. Bryan Krekel, –Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Northrop Grumman Corporation Information Systems Sector Report for the US-China Economic and Security ReviewCommission, at http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

4. Congressional testimony of John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, before the Joint Economic Committee on Cyber Threats and the U. S. Economy, February 23, 2000 <http://www.cia.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html

5. Dai Qingmin, „On Integrating Network Warfare and Electronic Warfare," China Military Science, Feb 2002, pp 112–117 as translated and downloaded from the FBIS web site.

6. David Finkelstein, Organizational chart from „The General Staff Department Of The Chinese People's Liberation Army: Organization, Roles, & Missions," in The People's Liberation Army asOrganization Reference Volume v1.0, James C. Mulvenon and Andrew N. D. Yang, eds, RAND Corp., 2002.

7. Dennis Blasko, „PLA Ground Force Modernization and Mission Diversification: Underway in all Military Regions," in Right Sizing the People's Liberation Army: Exploring the Contours of China's Military, Roy Kamphausen, Andrew Scobell, eds., Strategic Studies Institute, September 2007, p. 366–372

8. Desmond Ball, „Signals Intelligence In China" Jane's Intelligence Review, 1 August, 1995.

9. Desmond Ball, – China's Cyber Warfare Capabilities, Security Challenges (Australia), Vol. 7, No. 2 (Winter 2011), pp. 81–103, at http://www.securitychallenges.org.au/ArticlePages/vol7no2Ball.html.

10. Ellis L. Melvin, A Study Of The Chinese People's Liberation Army Military Region Headquarters Department Technical Reconnaissance Bureau, June 19, 2005 | Virtual Information Center, People's Republic of China Primer, 04 August 2006, available at: http://www1.apaninfo. net/Portals/45/VIC_Products/2006/08/060804-P-China.doc.

11. Federation of American Scientists Intelligence Resource Program, „Ministry of State Services," January 1998 http://www.fas.org/irp/world/china/mss/ops.htm

12. George J. Tenet, Director of the Central Intelligence Agency, Testimony Before the Senate Committee on Government Affairs, June 24, 1998 <http://www.cia.gov/cia/public_affairs/speeches/1998/dci_testimony_062498.htm

13. iDefense, „Inside the China Eagle Union hacker group," iDefense Intelligence Operations, April 29, 2002, White paper available upon request sent to iDefense at di@idefense.com]

14. James Mulvenon, „PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Beyond the Strait: PLA Missions Other Than Taiwan, Roy Kamphausen, David Lai, Andrew Scobell, eds., Strategic Studies Institute, April 2009, p. 272–273.

15. James Mulvenon, „PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Beyond the Strait: PLA Missions Other Than Taiwan, Roy Kamphausen, David Lai, Andrew Scobell, eds., Strategic Studies Institute, April 2009, p. 272–273.

16. James Mulvenon, PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability,‖ in Beyond the Strait: PLA Missions Other Than Taiwan, eds. Roy Kamphausen, David Lai, and Andrew Scobell, Strategic Studies Institute, U. S. Army War College, April 2009, p. 274;

17. Jane's Intelligence Review, „Confrontation central to Chinese cyber warfare aims," June 1, 2002

18. Lantern Through the Night: Central Military Commission Second Bureau, Xinhua, July 4, 2011, at http://www.js.xinhuanet.com/xin_wen_zhong_xin/2011–07/04/content_23160214.htm.

19. Lieutenant Colonel (ret.) Timothy L. Thomas, „Behind the Great Firewall of China: A Look at RMA/cyber warfare Theory From 1996–1998, November, 1998, http://fmso.leavenworth.army.mil/fmsopubs/issues/chinarma.htm

20. Major General Dai Qingmin, „Innovating and Developing Views on Information Operations," Beijing Zhongguo Junshi Kexue, [China's Military Science Journal] August 2000

21. National Defense in 2006¸ Information Office of the State Council of the People's Republic of China, December 2006, Beijing, available at: http://english.chinamil.com.cn/site2/newschannels/2006–12/29/content_691844.htm

22. OSC, CPP20020624000214, „On Integrating Network Warfare and Electronic Warfare," China Military Science, Academy of Military Science, Winter 2002

23. OSC, CPP20031002000138, „Telecom Experts in Guangzhou Doubling As Militia Information Warfare Elements," Guofang, Academy of Military Science, 15 September 2003 | OSC, PLA C4ISR Activities Roundup, 1 April-30 May 2006.

24. OSC, CPP20050301000186, „Roundup of C4I Activities in PRC, 13 November 2004–15 January 2005," 15 January 2005.

25. Prepared for The US-China Economic and Security Review Commission, Northrop Grumman Corporation Information Systems Sector, 7575 Colshire Drive, McLean, VA 22102, October 9, 2009.

26. SANS Institute, „Security Essentials with CISSP and CBK," Volume I, 2003 p. 522

27. Scott Henderson, The Dark Visitor, p.29

28. US-China Economic and Security Review Commission Report on the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation October 9, 2009, http://news.cnet.com/8301–13639_3–10381621–42.html?part=rss&subj=news&tag=2547–1_3–0-20