УДК 323.2

С.Н. СОКОЛОВА, д–р филос. наук, доцент
Заслуженный деятель науки и образования
Российской академии естествознания,
главный научный сотрудник
Центра системного анализа и стратегических исследований,
Национальная академия наук Республики Беларусь, г. Минск

Статья поступила 10 октября 2016 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СЕТЕЦЕНТРИЧЕСКИЕ ВОЕННЫЕ ДЕЙСТВИЯ И ГИБРИДНЫЕ ВОЙНЫ В СОВРЕМЕННОМ ОБЩЕСТВЕ

В статье автор рассматривает вопросы, связанные с информационным обществом и гибридными войнами, сетецентрическими военными действиями, что особенно актуально для современного социума. Взрывоопасное информационное пространство, каким является сегодня современное общество, объективно требует повышения уровня информационной безопасности, разработки обновленных методов системного противодействия сетецентрическим военным действиям и угрозам гибридных войн.

Ключевые слова: *информационная безопасность, сетецентрические военные действия, гибридные войны, национальные интересы, кибератака, информационное пространство.*

Введение. В информационном обществе происходят процессы, которые неизбежно воздействуют на общественные отношения, детерминируя сферу безопасности современного социума. Как это ни парадоксально, но ни для кого не секрет, что сегодня достаточно часто в решении вопросов на уровне государств практикуются сетецентрические действия, осуществляются кибератаки, а значит, не исключено, что завтра могут стать реальностью и гибридные войны. Именно поэтому нельзя не согласиться с утверждением исследователя Р.М. Юсупова о том, что «безопасность сегодня является одной и глобальных проблем человечества в целом» [1, с. 99]. И действительно, геополитические амбиции и борьба за ресурсы, экономическая дестабилизация во многих современных государствах служит сегодня доказательством того, что структурные диспропорции во всех сферах жизнедеятельности общества неизбежно приводят к информационному терроризму, к жестоким террористическим актам (с применением взрывных устройств), а также к боевым действиям с применением химического и высокоточного оружия. В тоже время, в обществе растет число особо опасных преступлений, связанных с наркотиками, коррупцией и торговлей людьми.

Современная архитектоника международной обстановки и деятельность средств массовой коммуникации в обществе имеют агрессивный характер, что иллюстрирует только одно, а именно, в эпоху глобализации цивилизационный маятник находиться в опасной точке и, видимо, существует реальная опасность перерастания локальных военных конфликтов (между военизированными подразделениями и террористическими группировками) в третью мировую войну.

Поясню, что агрегация интересов политических лидеров, финансовой элиты современных государств приносит свои неоднозначные плоды, так как международный формат происходящих событий становиться все более агрессивным и деструктивным как по форме, так и по содержанию. Демонстрация военной силы различными государствами становиться в современном обществе не просто традиционным вариантом решения международных проблем, но и общепринятым явлением, которое артикулируется и тиражируется средствами массовой информации. Как справедливо отмечает А.Д. Тукало, диалогичность современной системы международной безопасности и «раскрытие маслообразующего потенциала безопасности заключалось в представлении о состоянии или цели, конституирующих взаимоотношений между индивидами и государствами, и обществами» [2, с. 88].

В такой неоднозначной ситуации сфера безопасности современного общества приобретает особый статус, когда защита своих национальных интересов (ресурсов) выходит за рамки одного государства и становиться глобальной проблемой, требующей консенсусного решения, а именно, выполнения ранее подписанных коллективных договоренностей на уровне глав государств. Именно по этой причине, несмотря на все усилия дипломатов, сегодня так и не удалось добиться мирного урегулирования военных конфликтов, прекращения террористических актов на территории современной Украины, Сирии, Афганистана, Ирака и Турции.

Следовательно, в современном обществе осуществляется борьба за ресурсы, происходят социально–политические изменения, которые свидетельствуют об особой актуальности вопросов, связанных с информационной безопасностью, сетецентрическими военными действиями и гибридными войнами. «Государства, которые считают, что ресурсная безопасность оказывает прямое воздействие на национальные интересы и сохранение суверенитета, могут, вероятно, изменить традиционное толкование вопроса о законности применения силы, что может привести к политическому и даже военному вмешательству в целях защиты доступа к ресурсам» [3, с. 143].

Основная часть. Сетецентрические военные действия представляют собой достаточно специфическую информационно–коммуникативную, социокультурную эклектику, которая позволяет активно трансформировать информационное пространство, перераспределять информационные ресурсы с целью быстрого воздействия или переформатирования общественных отношений. Сетевые технологии и современные коммуникации, в этом случае, представляют собой наиболее эффективный вид действий, достаточно мобильный, сильнодействующий, относительно автономный, так как конфликтующие стороны, независимо от того, на какой территории находиться предполагаемый противник, осуществляют активное военное вмешательство и не важно, какое современное оружие используется при этом различными государствами.

Гибридная война, как научная категория, характеризует многомерную экзистенцию современного человека, общества и государства. Как синтезирующая дефиниция, гибридная война носит комплексный характер и включает в себя широкий спектр финансово–экономических, военно–стратегических, социально–политических, культурно–исторических составляющих, включающих в себя информационную, сетецентрическую и кибервойну, а также сочетающих методы ведения традиционной войны с применением химического, биологического, ядерного оружия [4].

Акцентируя внимание на вопросах, связанных с гибридными войнами, необходимо пояснить, что, во–первых, нельзя не учитывать тот факт, что в информационном обществе элементом гибридной войны являются действия латентных сил, возникающих, как правило, в различных государствах по инициативе и финансовой поддержке иностранных граждан.

В этом случае, при исследовании угрозы гибридных войн, важно учитывать тот факт, что в процессе «… ослабления влияния национальных государств всё большую роль играют наднациональные центры власти, а также новые транснациональные социально–политические силы, как группы управленцев, сращенные с финансовой олигархией, и различного рода неформальные общности, включая те, которые отрицают

существующий миропорядок, в частности криминальные и террористические» [5, с.14].

Во–вторых, неоднозначность ситуации в социуме и особенно в финансово–экономической сфере, а также деструктивная динамика развития общественных отношений порождает системные противоречия, так как любому современному государству, которое является участником гибридной войны, применяется разноплановое давление, наносится ущерб национальным интересам, а значит, становиться менее эффективной сфера безопасности социума. Напомню, что национальный интерес, как категория социально–политическая, отражает осознание, или субъективизацию объективных потребностей государства, а национальная безопасность обеспечивает реализацию данных интересов в формате международных отношений.

В–третьих, гибридная война включает в себя множество рычагов воздействия (целенаправленное экономическое давление, подрывная деятельность спецслужб, воздействие на демографическую политику, информационное пространство) и практикуется регулярное дезинформирование граждан.

В этом случае, политическая и финансовая элита считает возможным при решении внешнеполитических и внутриполитических проблем использовать вооруженные силы, применять высокоточное оружие, а также нерегулярные вооруженные формирования на территории противника [6].

Смысловая доминанта, таким образом, выглядит следующим образом: гибридная война предполагает специальные технологии латентного характера, используемые с целью активного привлечения специально подготовленных граждан, военизированных формирований, банд, группировок террористов, которые могут применяться в сочетании с действиями вооруженных сил, специальных подразделений.

Рассматривая именно в таком ракурсе гибридные войны, можно предположить, что создается мерцающий эффект целенаправленной информационной агрессии, ангажированного воздействия различных сил, провоцирующих масштабные боевые действия на территории государств (участников конфликта) и переформатирование общественных отношений (финансово–экономическое, социально–политическое, военно–стратегическое доминирование, перераспределение ресурсов, территориальные претензии, тиражирование стереотипов поведения и ценностных приоритетов).

Специалисты и эксперты в Лондонском Международном институте стратегических исследований уверены, что гибридные войны включают в себя комплексное применение традиционного инструментария для ведения войны с целью оказания:

1) финансово–экономического давления;

2) получения морально–психологических преимуществ, ретрансляции особых ценностных приоритетов, инициированных с помощью дипломатии и различного рода гуманитарных мероприятий на международном уровне;

3) системно осуществляемых сетевых, информационно–сетевых операций (кибератак), в том числе и военных действий с обязательным участием спецназа, морской пехоты, разведывательных десантно–штурмовых сил.

В таком случае, сущность и предназначение гибридных войн проявляется в том, что подбор, синтез, анализ необходимой информации носит комплексный характер, так как источником организованного вторжения выступает не военная разведка, аналитические подразделения различных ведомств, а совершенно другие аккумулированные движущие силы. Информационная экспансия и современная коммуникация привели к масштабным изменениям в приемах ведения войны с помощью обновленных средств, информационно–сетевых технологий. Именно поэтому, для эффективного противостояния угрозам гибридных войн и обеспечения высокого уровня безопасности необходимо перейти к комплексной безопасности современного общества.

Во–первых, комплексная безопасность, как считает автор статьи, является объективной необходимостью своевременного реагирования сферы безопасности на вызовы, опасности, угрозы, возникающие в социуме, так как угроза гибридных войн носит комплексный характер.

Во–вторых, секретность информационно–семантического поля может быстро испариться под влиянием специально инициированных компьютерных вирусов,

специально созданных программ, кибератак и сетецентрических военных действий. Развитие современных коммуникационных технологий (особенно Интернета и социальных сетей) свидетельствует о необходимости использования политической элитой, экспертами, научным сообществом, военными специалистами информационной составляющей для обеспечения безопасности.

С учетом того, что в современном обществе активно осуществляются сетецентрические военные действия и существует реальная угроза активации гибридных войн, следует обратить особое внимание на то, что любая информация может не выполнить свое предназначение (сохранность, актуальность и конфиденциальность).

Аккумулируя в себе информационные аспекты безопасности современного общества, угроза гибридных войн приобретает универсальный характер, и, таким образом, требует разработки методов системного противодействия и перехода к комплексной безопасности.

В–третьих, общегосударственная стратегия в эпоху глобального ресурсного и военно–силового доминирования с целью решения основных геополитических вопросов предполагает использование многоуровневого и комплексного подхода к систематизации информации по вопросам, касающимся сферы безопасности.

При этом в информационно–семантическом поле необходимо особое внимание уделить таким интегральным показателям, как:

– развитие информационной инфраструктуры, индустрии переработки информации, соблюдение прав и свобод граждан в информационно–семантическом поле, гарантирующих сохранность, актуальность и конфиденциальность информации;

– приоритетность в обеспечении информатизации социальной сферы, материального производства и ресурсов, более профессионального регионального управления для реализации эффективной информационной государственной политики, а также высокопрофессиональная подготовка специалистов в области информационных технологий (более эффективная защита теле–видео–телекоммуникационных систем, информационных ресурсов);

– накопление и сохранность информационных ресурсов для использования в системе безопасности с учетом динамичного движения и современного развития информационно–семантического поля, инициирование информационной индустрии с целью выхода на международные рынки.

Заключение. В итоге, сетецентрические военные действия и гибридные войны необходимо исследовать с учетом того, что информационная безопасность является специфическим аспектом национальной безопасности общества, которая гарантирует защищенность национальных интересов в информационно–семантическом поле и социальном пространстве.

Современный этап развития общества характеризуется возрастающей ролью информационной составляющей, так как именно информационная инфраструктура, осуществляющая синтез, анализ, распространение информации носит комплексный характер и регулирует многомерные общественные отношения.

Источником информационного вторжения, как правило, выступает не военная разведка, аналитические подразделения различных ведомств, а совершенно другие движущие силы, связанные с утверждением на территории государства–участника новых правил игры, а значит, ценностных приоритетов и национальных ориентиров.

В связи с этим, учитывая сложный характер международной современной ситуации, необходимо предложить основные методы для системного противодействия угрозам гибридных войн:

1) *метод агрегирования* и антимонопольного развития инфраструктуры информатизации, согласованного с программами социально–экономического развития общества (интеграционная внешнеэкономическая деятельность в области информатизации в рамках общенациональной стратегии, учитывающей специфику регионов);

2) *метод приоритетного развития* и интенсивного финансирования научно–технических разработок в сфере безопасности (особенно в области искусственного интеллекта, робототехники, андроидного строительства и нанобиотехнологий);

3) *метод согласованности* концептуальных подходов в решении вопросов информатизации, создание территориальных инфраструктур, гибкое сочетание индивидуализации и коллективизма с целью получения системного эффекта в создании информационного пространства;

4) *метод координирующего воздействия* и масштабная реализация социально–экономического ориентированного механизма (создание регулируемого рынка в области информатизации), обеспечивающего единство и преемственность в результате эффективной государственной политики информатизации;

5) *метод прогнозирования* перспектив эволюционного развития информационно–семантического поля в эпоху глобализации на основе обновленных технологий, а также информационно–аналитическое обеспечение и реализация системы мониторинга национальной безопасности.

Структурные диспропорции, характеризующие современные геополитические тенденции и сложный алгоритм принятия политической элитой государственных решений, кибератаки, происходящие в информационном обществе, как показывает практика, становится сегодня традиционным вариантом решения международных вопросов для различных стран, основным правилом дипломатической риторики или руководством к действию, что тиражируется средствами массовой информации. Сетецентрические военные действия и гибридные войны в информационном обществе носят универсальный характер, и, таким образом, требуют разработки и применения обновленных методов системного противодействия угрозам с целью обеспечения более эффективной информационной безопасности современного социума.

Список литературы

1. Юсупов, Р.М. Наука и национальная безопасность; 2–е издание, переработанное дополненное / Р.М. Юсупов. – СПб.: Наука, 2011. – 369 с.
2. Тукало, А.Д. Безопасность общества и политика мультикультурализма. Посткультурное общество: стабильность и коммуникация / А.Д. Тукало. М., 2003. – 327 с.
3. Фомин, М.В. Технологии качества жизни и постиндустриальная эпоха / М.В. Фомин // Вопросы философии. – 2016. – № 3. – С. 139–147.
4. Соколова, С.Н. «Сетевые войны» в системе безопасности современного общества / С.Н. Соколова // Вестник ЗабГУ: теоретический и научно–практический журнал. – 2014. – № 3 (106). – С.127–131. То же [Электронный ресурс]. – Режим доступа : http: //www.zabgu.ru/files/vest_3_14_ot_01.04.pdf – свободный. – Загл. с экрана (Дата обращения 12.12.2014); Соколова, С.Н. К вопросу о биотерроризме и биобезопасности / С.Н. Соколова, С.А. Соколов // Проблемы безопасности российского общества: научно–практический журнал. – 2013. – № 1. – С. 10–19. То же [Электронный ресурс]. – Репозиторий Полесского государственного университета: [сайт]. – Пинск [2013–2014] – Режим доступа : http://www.psunbrb.by/sites/default/files/sites/default/files/02per/30.pdf – свободный. – Загл. с экрана (дата обращения 19.12.2014)
5. Кокошин, А.А. Национальные интересы, реальный суверенитет и национальная безопасность / А.А. Кокошин // Вопросы философии. – 2015. – №10. – С. 5–21.
6. Соколова, С.Н. Российское общество: специфика сферы безопасности и национальные интересы /С.Н. Соколова, А.А. Соколова // Известия Российской академии образования. – 2012. – № 2. – С. 420–432; Соколова, С.Н. Безопасность человека и общества / С.Н. Соколова // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. – 2013. – № 2. – С. 62–67. То же [Электронный ресурс]. – Репозиторий Полесского государственного университета: [сайт]. – Пинск [2013–2014] – Режим доступа : http://lib.psunbrb.by/bitstream/112/3078/1/11 pdf– свободный. – Загл. с экрана (дата обращения 18.12.2014); Соколова, С.Н. Философия безопасности: национальные ценности и сетевые войны / С.Н. Соколова. – Минск: Высшая Школа, 2014. – № 3. – С. 44–46; Соколова, С.Н. Сфера безопасности общества: угроза кибервойны и «сетевые войны» / С.Н. Соколова // Вестник Полесского

государственного университета. Серия общественных и гуманитарных наук. – 2014. – № 1. – С. 46–49. То же [Электронный ресурс]. – Репозиторий Полесского государственного университета: [сайт]. – Пинск [2014] – Режим доступа : http://lib.psunbrb.by/bitstream/112/7895/1/8.pdf – свободный. – Загл. с экрана (дата обращения 18.12.2014) ; Соколова, С.Н. Сфера безопасности общества и генезис политико–правовой реальности / С.Н. Соколова // Проблемы безопасности российского общества: научно–практический журнал. – 2015. – № 3–4. – С.15–24.

Резюме. В современном информационном обществе происходят процессы, которые актуализируют сетецентрические военные действия и угрозу гибридных войн. Именно поэтому для более эффективного противостояния этим угрозам и обеспечению достаточно высокого уровня безопасности современного общества необходимо перейти к комплексной безопасности.

Во–первых, комплексная безопасность, как считает автор статьи, является объективной необходимостью своевременного реагирования сферы безопасности на вызовы, опасности, угрозы, возникающие в современном обществе, так как угроза гибридных войн носит комплексный характер.

Во–вторых, секретность информационно–семантического поля может быстро испариться под влиянием специально инициированных компьютерных вирусов, специально созданных программ, кибератак и сетецентрических военных действий. Развитие современных коммуникационных технологий (особенно Интернета, социальных сетей) свидетельствует о необходимости использования политической и финансовой элитой, экспертами, учеными, военными специалистами информационной составляющей для обеспечения более эффективной безопасности общества.

С учетом того, что в современном обществе активно осуществляются сетецентрические военные действия, следует обратить особое внимание на то, что любая информация может исчезнуть, т.е. не выполнить свое предназначение, что требует разработки и обязательного внедрения основных методов системного противодействия угрозе гибридных войн.

В–третьих, общегосударственная стратегия в эпоху глобального ресурсного доминирования с целью решения основных геополитических вопросов предполагает использование комплексного подхода к систематизации информации по вопросам безопасности человека, общества и государства.

При этом в информационно–семантическом пространстве необходимо особое внимание уделить таким интегральным показателям, как:

– развитие информационной инфраструктуры, индустрии переработки информации, соблюдение прав и свобод граждан в информационно–семантическом пространстве, гарантирующих сохранность и конфиденциальность информации;

– приоритетность в обеспечении информатизации социальной сферы, материального производства, ресурсов, более профессионального регионального управления для реализации эффективной информационной государственной политики, а также высокопрофессиональная подготовка специалистов в области информационных технологий для более эффективной защиты теле–видео–телекоммуникационных систем, информационных ресурсов;

– накопление и сохранность информационных ресурсов для использования в системе безопасности с учетом динамичного движения, инициирование информационной индустрии с целью выхода на международные рынки.

В итоге, кибератаки, происходящие в современном информационном обществе, регулярная демонстрация военной мощи различными государствами становиться для различных государств не просто традиционным вариантом решения международных вопросов, а специфической дипломатической риторикой и руководством к действию, что тиражируется средствами массовой информации.

Abstract. In today's information society, there are processes that actualize the network–centric warfare and the threat of hybrid wars. That is why, to better confront these threats and national security of the modern society high enough level you must go to comprehensive security.

Firstly, integrated security, according to the author, is an objective necessity of timely response to the security sector to the challenges, dangers and threats that arise in today's society, as the threat of hybrid warfare is complex.

Second, privacy of information and semantic space can quickly evaporate under the influence of specially initiated by computer viruses, specially designed programs, cyber–attacks and network–centric warfare. The development of modern communications technology (especially the Internet, social networks) indicates the need for political and financial elite, experts, scientists, military experts of the information component of national security.

Given the fact that in modern societies actively implemented network–centric warfare, should pay special attention to the fact that any information may disappear, is not fulfill its purpose, it requires the development and implementation of compulsory basic methods of system to counter the threat of hybrid wars.

Third, the nation–wide strategy in an era of global resource domination in order to address the major geopolitical issues involves the use of an integrated approach to the systematization on security information.

In this case, in the information and semantic space is necessary to pay special attention to such integral indicators such as:

– The development of information infrastructure and information processing industry, respect for the rights and freedoms of citizens in the information and the semantic space, guaranteeing the safety and confidentiality of information;

– Priority in providing information of social sphere of material production, resources, a professional regional management for the implementation of an effective information policy of the state, as well as highly professional training of specialists in the field of information technology for more effective protection of tele–video–telecommunication systems and information resources;

– The accumulation and preservation of information resources for use in the national security system, taking into account the dynamic movement and the development of modern information and semantic space, the initiation of the information industry in order to reach international markets.

As a result, constant cyber–attacks occurring in today's information society, the regular display of military might become different states for different countries are not just the traditional way to solve international issues, specific diplomatic rhetoric, but a guide to action, that is replicated by the media.

SOKOLOVA Svetlana N., Doctor of Philos. Sc., Associate Professor
Honored Worker of Science and Education of the Russian Academy of Natural Sciences
National Academy of Sciences of the Republic of Belarus, Minsk

INFORMATION STCURITY: NETWORKCENTRIC MILITARY ACTIONAND HYBRID OF WAR IN MODERN SOCIETYSN

In the article an author considers the issues related to the information society and hybrid warfare, network–centric warfare, which is especially important for modern society. Explosive information space, what is today the society objectively requires an increase in information security, development of updated techniques for the system network–centric military action to counter threats and hybrid wars.

Keywords: *information security, networkcentric warfare, hybrid war, national interests, cyberattack, the information space.*

References

1. Yusupov R.M. *Science and National Security* SPb .: Science, 2011, 369 p.
2. Tukalo A.D. *Security Society and politics of multiculturalism. Postkulturnoe society: stability and communication*, Minsk, 2003, 327 p.

3. Fomin M.V. *Problems of Philosophy*. 2016, no 3, pp. 139–147.
4. Sokolova S. N. *Herald ZabGU: theoretical and scientific journal*, no 3 (106), 2014, pp. 127–131. The same Access: http://www.zabgu.ru/files/vest_3_14_ot_01.04.pdf – free (accessed 12/12/2014); Sokolova S.N., Sokolov S.A. *Problems of safety of the Russian society: scientific journal*, no 1, 2013, pp. 10–19. The same Repository Polesskie State University: [site]. – Pinsk [2013–2014] – Access mode: http://www.psunbrb.by/sites/default/files/sites/default/files/02per/30.pdf (accessed 12/19/2014).
5. Kokoshin A.A. *National interests, real sovereignty and national security, Problems of Philosophy*, no 10, 2015, pp. 5–21.
6. Sokolova S.N., Sokolov A.A. *Proceedings of the Russian Academy of Education*, 2012, no 2, pp. 420–432; Sokolova S. N. *Herald of the Polesskie State University a series of social sciences and humanities*. 2013, no 2, pp. 62–67. The same Repository Poesy State University: [site], Pinsk [2013–2014] – Access mode: http://lib.psunbrb.by/bitstream/112/3078/1/11 pdf– free (accessed 18/12/2014); Sokolova S.N. *Safety philosophy: national values, and network war*, Minsk, no 3, 2014, pp. 44–46; Sokolova S.N. *Bulletin of the Polesskie State University a series of social sciences and humanitie*s, 2014, no 1, pp 46–49. Repository Polesskie State University– Pinsk [2014] http://lib.psunbrb.by/bitstream/112/7895/1/8. pdf – free (accessed 18/12/2014); Sokolova S.N. *Problems of safety of the Russian society: scientific journa*l, 2015, no 3–4, pp.15–24.

Received 10 October 2016