УДК 159.9.01

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 20 сентября 2017 г.

РИСКИ И УГРОЗЫ ГИБРИДНЫХ ВОЙН В СОВРЕМЕННОМ ОБЩЕСТВЕ: ПАРАДОКСЫ РЕАЛЬНОСТИ

В представленной статье автор предлагает рассмотреть гибридные риски и угрозы гибридных войн в современном обществе. Гибридные войны, которые носят универсальный характер, актуализируют геополитические факторы экономической дестабилизации и связаны с международным терроризмом, экстремизмом, сетецентрическими военными действиями и кибератаками.

Ключевые слова: *гибридные риски, информационное общество, гибридные войны, комплексная безопасность.*

Введение. Глобальные процессы, происходящие в современном обществе, активная борьба за ресурсы между современными государствами доказывают, что структурные диспропорции во всех сферах жизнедеятельности социума порождают риски и гибридные войны, что детерминирует общественные отношения. Трансформации, активно происходящие в социальном пространстве, свидетельствуют о том, что современное общество динамично развивается, изменяя, в том числе, и сферу безопасности. «Все мы являемся свидетелями того, как современный мир стремительно меняется. Меняется, как мы видим, не в сторону стабильности и безопасности. Сегодня на планете происходят все более тревожные процессы. Усугубляются известные нам вызовы и угрозы, возникают и качественно новые» [1, с. 3].

Гибридные войны – это сложное явление, представляющее собой специфическую информационно-коммуникативную эклектику, которая позволяет деструктивно воздействовать на социальное пространство, изменяя информационные ресурсы с целью перефор-

матирования общественных отношений и перераспределения ресурсов. Именно в такой неоднозначной ситуации сфера безопасности общества приобретает глобальный статус, а защита национальных интересов выходит за рамки одного государства, так как становится всеобщей проблемой, требующей конструктивного диалога глав различных государств, обязательного выполнения подписанных коллективных договоренностей и консолидации усилий по борьбе с международным терроризмом. Гибридные войны, как правило, отражают сущностные трансформации современного человека, общества и государства. И как синтезирующая дефиниция объективно носит комплексный характер, включая в себя разновекторный спектр военно-стратегических, финансово-экономических, социально-политических составляющих (сетецентрические военные действия, кибервойна), а также органично сочетает методы ведения традиционной войны с применением химического, биологического и ядерного оружия. Такая многомерная, разновекторная динамика развития об-

щественных отношений порождает противоречия, так как к современному государству, которое является участником гибридных войн, применяется разноплановое давление, наносится ущерб национальным интересам, а значит, становится менее эффективной его сфера безопасности.

Современная интеграция, информатизация, а также борьба различных государств за перераспределение мировых ресурсов актуализирует гибридные риски и необходимость выработки методов системного противодействия угрозам гибридных войн. Информационная экспансия и современная коммуникация, интенсивное развитие информационно-сетевых технологий привели к масштабным изменениям в приемах ведения современной войны. И совершенно не случайно, что «… все страны мира сейчас решают одну масштабную задачу – необходимость обеспечивать устойчиво-безопасное развитие и актуальные потребности граждан, одновременно максимально инвестируя в новые технологии» [2, с. 141].

Гибридные риски, синтезируя внешние и внутренние факторы, отличаются от других рисков по месту и времени возникновения, по способу их анализа, методам описания. Гибридные риски представляют собой многомерное, эклектичное, независимое событие, которое можно рассматривать с учетом специфики развития информационного общества, реализации комплексной безопасности, что предполагает также акцентуацию на сложном процессе принятия управленческих решений, направленных на снижение вероятности возникновения деструктивного результата, вызванного реализацией предложенных идей и проектов.

Гибридные риски можно классифицировать на основании таких критериев, как время, сфера возникновения (производственная, коммерческая, финансовая), характер последствий. Гибридные риски по характеру последствий подразделяются на два вида: статические (военные конфликты, стихийные бедствия, несчастные случаи, преступные действия, коррупция, кибератаки, терроризм); динамические риски (конкурентоспособность на рынке, налоговое законодательство, резкое изменение курсов валют).

Необходимо отметить, что внешние факторы возникновения гибридных рисков свидетельствуют о том, что риски могут быть политическими, экономическими, демографическими, социальными, географическими, социокультурными, а внутренние риски обусловлены субъективным фактором (производственный потенциал, производительность труда, общественные отношения).

Гибридные риски, как считает автор статьи, сложное явление в социуме, свидетельствующее о сложных процессах в современном мире, в котором становятся не редкостью террористические акты, сетецентрические военные действия, кибератаки, информационные войны.

Основная часть. Интерес к гибридным рискам, как считает автор статьи, и гибридным войнам в информационную эпоху не случаен.

Во-первых, по причине того, что в современном мире элементом гибридной войны являются, как правило, действия латентных сил (оппозиции), которые возникают непосредственно по инициативе и финансовой поддержке представителей иностранных государств.

Во-вторых, динамика современных международных отношений, военные конфликты и кризисы свидетельствуют о том, что сегодня важно перейти к комплексной безопасности, так как, к сожалению, повседневной реальностью становится информационный терроризм, сетецентрические военные действия. В том числе, угрозы гибридных войн требуют особых усилий государственных институтов с целью активизации международного сотрудничества в сфере безопасности.

В-третьих, абсурдность современной геополитической ситуации заключается в том, что разноплановое и многоуровневое экономическое давление на различные государства наносит непоправимый ущерб национальным интересам, а значит, становиться менее эффективной национальная безопасность, что может привести к нестабильности и глобальному военному конфликту.

В-четвертых, гибридная война включает в себя множество рычагов воздействия (целенаправленное информационное, экономическое давление, подрывная деятельность спецслужб, воздействие на демографию, социальную структуру общества). Гибридная война предполагает регулярное дезинформирование граждан, и в этом случае становится возможным при решении внешнеполитических и внутриполитических проблем использовать вооруженные силы, применять высокоточное, химическое оружие и нерегуляр-

ные вооруженные формирования на территории противника.

По мнению специалистов, гибридная война представляет собой сложное, аккумулирующее в себе все виды современной войны явление, а точнее, комплексное применение традиционного инструментария для ведения оперативно-стратегических (военных и специальных) операций с целью оказания финансово-экономического давления и перераспределения ресурсов на территории другого государства, а также получения морально-психологических преимуществ, распространения и утверждения ценностных приоритетов для перезагрузки стереотипов поведения граждан другой страны, инициированных с помощью дипломатии, различных активно финансируемых гуманитарных мероприятий, организованных на региональном, международном уровне и регулярно осуществляемых сетевых, информационных операций (кибератак), в том числе военных действий с обязательным участием спецназа, морской пехоты, разведывательных десантно-штурмовых сил. Сущность гибридных войн заключается в том, что подбор, синтез, анализ необходимой информации носит комплексный характер, так как источником организованного вторжения выступает не военная разведка и не аналитические подразделения различных ведомств.

Гибридная война, в итоге, предполагает обязательное использование современных коммуникационных технологий, информационного пространства, латентных сетевых технологий, активное привлечение специально подготовленных граждан, военизированных формирований, группировок террористов, которые могут применяться в сочетании с действиями вооруженных сил и специальных подразделений. В таком случае, гибридные войны носят комплексный характер, так как источником организованного вторжения выступает не военная разведка, аналитические подразделения различных ведомств, а совершенно другие аккумулированные движущие силы.

Для преодоления экономической дестабилизации и максимально эффективного противодействия угрозам гибридных войн, а значит, обеспечения национальной безопасности необходимо не только осуществлять результативный мониторинг, что действительно необходимо, но и перейти к комплексной безопасности. Данный переход будет адекватным и своевременным ответом на существующие угрозы гибридных войн, что обусловлено современными тенденциями информационно-техногенной среды. Так, развитие современных коммуникационных технологий (особенно Интернета и социальных сетей) свидетельствует о необходимости использования политической элитой, экспертами, научным сообществом, военными специалистами информационной составляющей и семантического поля, постоянно изменяющегося под воздействием специально инициированных вирусов, современных универсальных компьютерных программ. Нельзя забывать, что в современном обществе доминирует информационный терроризм, а значит, угрозы гибридных войн становятся реальностью и, в этом случае, важно акцентировать внимание на информационной безопасности, так как в результате гибридного вторжения, сохраняемая банками информация, может не выполнить свое предназначение, а значит, потерять в результате кибератаки свою конфиденциальность.

В связи с этим, необходимо перейти к реализации методов системного противодействия угрозам гибридных войн: методу агрегирования и антимонопольного развития инфраструктуры информатизации, как синтеза программной реализации социально-экономического развития (интеграционная внешнеэкономическая деятельность в области информатизации, учитывающая общенациональную стратегию); методу приоритетности в развитии интенсивного финансирования научно-технических разработок, особенно в сфере безопасности (робототехника, искусственный интеллект, андроидное строительство, нанобиотехнологии, космическая промышленность и наноиндустрия); методу согласованности в решении вопросов, связанных с информатизацией, а также создание более эффективных территориальных инфраструктур с целью реализации системного подхода в создании единого информационного пространства; методу координирующего воздействия, реализации социально-экономического ориентированного развития, обеспечивающего преемственность и единство в результате государственной политики информатизации; методу прогнозирования перспектив развития информационно-семантического поля на основе современных коммуникационных технологий (информационно-аналитическое обеспечение и мониторинг национальной безопасности).

Заключение. В результате, сегодня угрозы гибридных войн являются глобальной проблемой цивилизации. Комплексная безопасность может и должна быть приоритетным направлением развития государств, особенно в ситуации, когда стремление к информационному доминированию, особенно в вопросах национальной безопасности, носит гибридный характер, объективно требуя внедрения методов системного противодействия гибридным рискам и угрозам гибридных войн. При этом в информационном обществе необходимо обратить особое внимание на такие интегральные показатели, как, во-первых, развитие информационной инфраструктуры, индустрии переработки информации при условии обязательного соблюдения прав и свобод граждан в информационно-семантическом поле, гарантирующих конфиденциальность информации.

Во-вторых, приоритетность в обеспечении информатизации социальной сферы, материального производства, ресурсов, более профессионального регионального управления для реализации эффективной информационной государственной политики, подготовки специалистов в области информационных технологий (например, более эффективная защита теле-видео-телекоммуникационных систем, информационных ресурсов).

И, в-третьих, накопление, сохранность информационных ресурсов, особенно, в сфере безопасности для интенсификации информационной индустрии с целью выхода на международные рынки.

К сожалению, сегодня во многих социумах доминирует аномальное окно возможностей, которое деструктивно воздействует на существующую реальность, смещая акценты в пользу дестабилизирующих факторов, что происходит по причине того, что постоянно инициируется маргинальный элемент, усиливающий негативные тенденции, изменяющий общественные отношения и трансформирующий социальное пространство.

Для более эффективного противодействия угрозам гибридных войн необходимо перейти к комплексной безопасности и более эффективно реагировать на гибридные риски, опасности, возникающие в обществе. Все это может исчезнуть под влиянием специально инициированных компьютерных вирусов, вредоносных программ, реализуемых специалистами для осуществления кибератак, а также активных сетецентрических военных действий. С учетом того, что в современном обществе осуществляются кибератаки, сетецентрические военные действия, следует обратить особое внимание на то, что информация может не выполнить свое предназначение (секретность, сохранность, актуальность, конфиденциальность).

Следовательно, развитие Интернета, социальных сетей, современных коммуникационных технологий свидетельствует о необходимости использования экспертами, учеными, военными специалистами информационной составляющей для обеспечения более эффективной комплексной безопасности.

Гибридная война, как синтезирующая дефиниция, несомненно, включает в себя самый широкий спектр политико-экономических, военно-стратегических, социально-правовых, культурно-исторических составляющих, сочетающих методы ведения традиционной войны. «Безопасность необходима личности и государству по той причине, что они находятся в постоянном движении, изменении и развитии, которое связано с преодолением противоречий и опасностей в практической деятельности и осуществляемой в условиях неопределенности и риска, реально существующих внешних и внутренних угроз» [3, с. 66].

В итоге, общегосударственная стратегия в эпоху глобальной интеграции, ресурсного, военно-силового доминирования предполагает более активное использование комплексного подхода, а также многоуровневой и более эффективной аналитической работы в сфере безопасности. Комплексная безопасность, несомненно, очень актуальна, по причине того, что в современном обществе существуют гибридные риски, а гибридные войны постепенно приобретают универсальный характер и становятся смыслообразующим парадоксом реальности.

Список литературы

1. Лукашенко, А.Г. Наша общая цель – построение сильного и безопасного государства /А.Г. Лукашенко // Белорусская думка. – 2017. – № 5. Май. – С. 3-20.
2. Фомин, М.В. Технологии качества жизни и постиндустриальная эпоха / М.В. Фомин // Вопросы философии. – 2016. – № 3. – С. 139-147.
3. Литвинов, Э.П. Философские основы концепции безопасности / Э.П. Литвинов // Пространство и время. – 2012. – № 1 (7). – С. 66-74.

Резюме. Современная интеграция, информатизация и борьба различных государств за перераспределение мировых ресурсов актуализирует гибридные риски и диктует необходимость выработки методов системного противодействия угрозам гибридных войн. Информационная экспансия и современная коммуникация, интенсивное развитие информационно-сетевых технологий привели сегодня к масштабным изменениям в приемах ведения современной войны.

Глобальные процессы, происходящие в обществе, активная борьба за ресурсы между современными государствами доказывают, что структурные диспропорции во всех сферах жизнедеятельности социума порождают гибридные риски и войны, что детерминирует общественные отношения, а также сферу безопасности общества.

Гибридные войны представляют собой специфическую информационно-коммуникативную эклектику, позволяющую деструктивно воздействовать на социальное пространство, изменяя информационные ресурсы с целью переформатирования общественных отношений и перераспределения ресурсов. Именно в такой неоднозначной ситуации сфера безопасности общества приобретает особый статус, а защита национальных интересов выходит за рамки одного государства, так как становится глобальной проблемой, требующей конструктивного диалога, обязательного выполнения подписанных коллективных договоренностей глав различных государств и консолидации усилий по борьбе с международным терроризмом.

В итоге, сегодня угрозы гибридных войн являются глобальной проблемой цивилизации. Комплексная безопасность может и должна быть приоритетным направлением развития государств, особенно в ситуации, когда стремление к информационному доминированию, особенно в вопросах национальной безопасности, носит гибридный характер, объективно требуя внедрения методов системного противодействия гибридным рискам и угрозам гибридных войн.

Гибридная война, как синтезирующая дефиниция, включает в себя самый широкий спектр политико-экономических, военно-стратегических, социально-правовых, культурно-исторических составляющих, а также информационную, сетецентрическую, кибервойну, сочетающую методы ведения традиционной войны с применением химического, биологического, ядерного оружия, что, в результате, может уничтожить современную цивилизацию.

Abstract. Modern integration, informatization and the struggle of the various States for the redistribution of world resources actualizes hybrid risks dictates the need for developing methods of system of counteraction to threats of hybrid warfare. Information expansion and modern communication, intensive development of information and network technologies led to major changes in the techniques of modern warfare.

Global processes taking place in society, an active struggle for resources between the modern States proves that structural imbalances in all spheres of life of society give rise to hybrid the risks and war that determines social relations, and security companies.

Hybrid wars are a specific information and communication eclecticism, in which the negative impact on social space, changing information resources with the aim of reformatting of social relations and redistributing resources. In such ambiguous situation, the security sector of the society acquires a special status and protection of national interests is beyond the scope of one state, as it is a global problem that requires a constructive dialogue, required the implementation of signed collective agreements of heads of different States and the consolidation of efforts to combat international terrorism.

As a result, today's threats of hybrid wars are a global problem of civilization. Comprehensive security can and should be a priority for the development of States, particularly in a situation where the pursuit of information dominance, particularly in matters of national security, is of a hybrid nature, objectively requiring the implementation of system of counteraction to threats of hybrid risks and dangers.

Hybrid warfare as a synthesizing definition, includes the widest range of political, economic, military-strategic, socio-legal, cultural-historical components, as well as informational, network-centric, cyber warfare, combining methods of conventional warfare involving chemical, biological, nuclear weapons that eventually can destroy modern civilization.

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

RISKS AND COMPLEX SECURITY COMPANIES: THE PARADOXES OF REALITY

In this article the author proposes to consider the category of hybrid risks associated with the threats of hybrid warfare in the information society, as well as comprehensive security. The hybrid wars that are universal in nature actualize the geopolitical factors of economic destabilization in different regions and which is associated with international terrorism, extremism, net-centric warfare, cyber-attacks.

Keywords: *hybrid risks, information society, hybrid wars, complex security.*

References

1. Lukashenko A.G. *Nasha obshhaja cel' – postroenie sil'nogo i bezopasnogo gosudarstva* [Our general purpose is the construction of strong and secure state]. *Belorusskaja dumka*, 2017, no. 5. May, pp. 3-20. (In Russian)
2. Fomin M.V. *Tehnologii kachestva zhizni i postindustrial'naja jepoha* [Technologies of Quality of Life and Post-industrial Era]. *Voprosy filosofii*, 2016, no. 3, pp. 139-147. (In Russian)
3. Litvinov Je.P. *Filosofskie osnovy koncepcii bezopasnost* [Philosophical Foundations of the Concept of Security]. *Prostranstvo i vremja*, 2012, no. 1 (7), pp. 66-74. (In Russian).

Received 20 September 2017