Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Юрий Даник, Тамара Малярчук, Чад Бриггс,
Connections QJ 16, no. 2 (2017): 5-27
https://doi.org/10.11610/Connections.rus.16.2.01

Рецензированная статья

Гибридная война: хай-тек, информационные и кибер конфликты

Юрий Даник,[a] Тамара Малярчук,[a] и Чад Бриггс [b]

[a] *Житомирский военный институт радиоэлектроники им. С.П. Королева, http://www.zvir.zt.ua*

[b] *Global INT*

Резюме: В этой статье рассматриваются передовые технологические, информационные и кибер компоненты гибридной войны и предприятие предлагаемых контрмер для противодействия информационным и кибер угрозам и нападениям. Основная гипотеза авторов состоит в том, что революционное развитие и быстрое применение технологий новаторскими способами во всех сферах жизни способствуют установлению и формированию основы для трансформации теоретических и практических парадигм войны и конфликта. Основным предметом данной статьи является гибридная природа современного конфликта.

Ключевые слова: Гибридная война, информационные операции, кибервойна, инновационная война, Украина.

Введение

Анализы геополитической и геостратегической среды показывают, что в настоящее время происходит переформулировка как философии, так и искусства ведения войны, процессы, которые были вызваны применением новых технологий, позволяющих использование разной интенсивности и разных стратегий в ходе конфликтов. Эти новые методы в сочетании с традиционным пониманием конфликта и безопасности часто обозначаются как «гибридная» война. В этой работе рассматривается природа гибридной войны в Восточной Европе, с особым вниманием к тактикам и страте-

гиям, используемых российскими и союзными силами в Украине с 2014 года.

Концепция гибридной войны не является чем-то абсолютно новым, представляя собой сочетание конвенциональных и неконвенциональных/ нерегулярных методов ведения войны, выходящих за пределы поля сражений и охватывающих экономические, дипломатические, информационные (в том числе психологические, кибер и дезинформационные) и политические способы противоборства.[1] Эта концепция основывается на первом месте на способности оказывать целенаправленное воздействие на удаленные объекты и процессы нетрадиционными военными средствами, в особенности на процессы и объекты, являющиеся критически важными для функций государства и вооруженных сил. В качестве асимметричного подхода, гибридная война направлена на достижение широкомасштабных последствий с использованием скромных средств, например, препятствование военным операциям противника или предотвращение получения политической поддержки населения.[2] В целом, при гибридных конфликтах имеет место координация так называемых мягких действий с использованием более целостной стратегии, которая варьирует в плане интенсивности на различных этапах (инициирование, острая фаза, решение), и которая направлена на дестабилизацию внутренних и внешних процессов государства. Конечной целью является подрыв данного государства путем стимулирования дестабилизации экономики, разочарования и недовольства населения, отчуждения меньшинств или обиженных групп населения, создания условий для контролируемой и неконтролируемой миграции, подавления гражданского сопротивления и подрыва критической инфраструктуры. К этому добавляется использование определенных разведывательных способностей, операций сил особого назначения, конвенциональных вооруженных сил и нерегулярных комбатантов (террористов, преступников, милиций, наемников, движений сопротивления, партизан и т.д.). Современными примерами гибридных конфликтов являются недавние и продолжающиеся боевые действия на Украине,[3] в Грузии,[4] и в последнее время, в некоторых странах Европейского союза.[5]

---

1 Frank G. Hoffman, “Hybrid Warfare and Challenges,” *Joint Forces Quarterly* 52 (2009): 34-39.

2 Keir Giles, *The Next Phase of Russian Information Warfare* (Riga: NATO Strategic Communications Centre of Excellence, 2016), http://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

3 Volodymyr P. Gorbulin, Oleksandr S. Vlasiuk, Ella M. Libanova, Oleksandra M. Liashenko, *Donbas and The Crimea: The Value of Return* (Kyiv: National Institute of Strategic Studies, 2015); Michael Kofman, “Russian Hybrid Warfare and Other Dark Arts,” *War on the Rocks*, March 11, 2016, http://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts (31 August 2017).

Предложенная здесь концепция слегка отличается от некоторых представлений о гибридной войне, бытующих на Западе (Западом, Западным миром или Западной цивилизацией являются страны в Европе, Северная Америка, Австралия, Израиль, Япония, Южная Корея и т.д., объединенные общими взглядами и восприятием некоторого единства ключевых культурных, политических и экономических признаков, выделяющих их на фоне других стран),[6] которые сфокусированы на так называемой «Доктрине Герасимова» о маскировке, проведения операций ниже порога открытой конвенциональной войны при сохранении способности правдоподобно отрицать свое участие.[7] Наоборот, в этой работе описаны некоторые из тактических приемов, используемых при поддержке сил часто (но не всегда) проводящих операции в конвенциональной манере, которые усилены применением новых технологий, позволяющих более глубокое проникновение асимметрических действий в критические элементы и жизненно важные системы противника. Вкратце, критическими элементами системы являются существенные ключевые элементы (компоненты, подсистемы) разных систем, касающиеся трещин, слабых мест в системе.[8] Оказание давления на эти болевые точки может привести к каскадным, синергетическим, деструктивным системным изменениям (разрушению) критических компонентов и связанных с ними систем.[9]

Применение средств гибридной войны направлено на наиболее критические уязвимости в материальных системах – коммуникациях, инфраструктуре или транспорте. Все чаще государственные и негосударственные акторы осуществляют нападения на уязвимые точки идеологий и институций, а также используют социальное недовольство или восприятия

---

4 David J. Smith, “Russian Cyber Capabilities, Policy and Practice,” *inFocus Quarterly* (Winter 2014), www.jewishpolicycenter.org/2013/12/31/russian-cyber-capabilities/ (31 August 2017).

5 See, for example, Martin Kragh and Sebastian Åsberg, “Russia’s Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case,” *Journal of Strategic Studies* 40, no. 6 (2017): 773-816, https://doi.org/10.1080/01402390.2016.1273830.

6 Patrick J. Buchanan, *The Death of the West: How Dying Populations and Immigrant Invasions Imperil Our Country and Civilization* (New York: St. Martin's Griffin, 2002).

7 Andrew Monaghan, “The ‘War’ in Russia’s ‘Hybrid Warfare’,” *Parameters* 45, no. 4 (2015): 65-74.

8 Brad Roberts, *Asymmetric Conflict 2010*, Report no. IDA-D-2538 (Alexandria, VA: Institute for Defense Analysis, 2000).

9 Vladimir Sazonov, Kristiina Müür and Holger Mölder, eds., *Russian Information Campaign Against the Ukrainian State and Defence Forces* (Tartu: NATO Strategic Communications Centre of Excellence and Estonian National Defence College, 2016), http://stratcomcoe.org/download/file/fid/7504.

коррупции для уравнивания сил на поле конфликта.[10] Эти существенные стратегические слабости дали возможность достижения большего успеха тем, кто использует методы информационной или асимметричной войны против Запада. Доминирование неолиберальных идей привело к расширению пропасти между богатыми и бедными и увеличило давление на средний класс. В результате этого произошли фундаментальные изменения в экономической, социально-политической и психологической ситуации, происходит переоценка основных ценностей, имеет место рост популизма во многих странах по всему миру. Референдум о Брексите в Объединенном Королевстве в 2016 году и избрание Дональда Трампа президентом США отражают обеспокоенность социально-экономическими условиями, ставя под сомнение такие институции с многолетней историей, как Европейский союз и НАТО.[11]

Сохранение конкурентоспособности и ведущей роли на мировой сцене требует соответствующей экономической мощи и высокого уровня развития образования и науки, ресурсов, которые находятся, главным образом, в распоряжении центров глобального могущества. Страны, у которых нет доступа к этим ресурсам, чувствуют отставание и потерю возможностей, а темпы хай-тек развития в экономическом секторе и секторе обороны неизбежно приводит к утрате их ведущей позиции и перераспределению сфер влияния между более могущественными акторами. Стремление к захвату контроля над конкурирующими «центрами мирового могущества» и желание получить беспрепятственный доступ к стратегическим ресурсам или, наоборот, предотвратить такое развитие ситуации, приводит к нарушению границ или к поглощению их зон безопасности и сфер влияния. В результате этого имеет место опасное взаимное сближение сфер влияния центров мирового могущества с неизбежным конфликтом их интересов.

Эти конфликты можно рассматривать как хантингтоновские столкновения цивилизаций, в которых культурные и религиозные различия народов являются первичным источником конфликтов в мире после Холодной войны. Американский политолог Сэмюель Хантингтон утверждает, что будущие войны будут вестись не между государствами, а между культурами.[12] Эти столкновения могут быть так же макиавеллевскими попытками

---

[10] Elīna Lange-Ionatamišvili, *Redefining Euro-Atlantic Values: Russia's Manipulative Techniques* (Riga: NATO Strategic Communications Centre of Excellence, 2016), http://stratcomcoe.org/download/file/fid/7350; Haroro J. Ingram, "Three traits of the Islamic State's information warfare," *The RUSI Journal* 159, no. 6 (2014): 4-11.

[11] Ronald Inglehart and Pippa Norris, "Trump, Brexit, and the Rise of Populism: Economic Have-nots and Cultural Backlash," HKS Working Paper No. RWP16-026 (Harvard Kennedy School, 2016), https://www.hks.harvard.edu/publications/trump-brexit-and-rise-populism-economic-have-nots-and-cultural-backlash.

[12] Samuel P. Huntington, "The Clash of Civilizations," *Foreign Affairs* 72, no. 3 (Summer 1993): 22-49.

подрыва стратегических противников, поскольку лидеры часто будут ощущать потребность развивать проекцию военной силы, которая не будет приводить к *ultima ratio regum*[13] решениям, при которых вооруженный конфликт может привести к уничтожению обеих сторон. Есть необходимость в новых инструментах достижения целей без прямой и видимой агрессии.

Намерение было найти технологии, которые могут не только обеспечить новый уровень мощи вооружений, но и способность использовать слабые места во всех сферах функционирования государства. В отличие от информационных кампаний в прошлом, новые технологии дают возможность достигать стратегических целей неконвенциональными и когнитивными эффектами (технологии социального влияния и манипулирования, кибер сфера, информационное оружие, возможности нанесения существенного вреда системам управления государства). Такие технологии, как социальные медиа, сделали возможным, чтобы заинтересованный актор мог дистанционно оказывать влияние на все основные институции и на инфраструктуру государства. Это стало основой для неконвенциональных посягательств на территорию, часто даже без использования конвенциональных военных компонентов. Или их присутствие сделало возможным использование организованных и поддерживаемых извне движений сопротивления и террористических движений, которые тоже могут способствовать достижению стратегической цели создания нестабильности и нанесению ущерба институциям без применения военного насилия.[14]

Таким образом, «гибридная война» является хай-тек конфликтом. Это продолжение политики государства и/или коалиций, политических групп, транснациональных корпораций и негосударственных акторов. Целью конфликта является навязывание воли акторов их оппонентам через интегрированные адаптивные и асимметрически синхронизованные деструктивные средства влияния на них в многомерном пространстве и в разных сферах жизни. Гибридная война рационально сочетает конвенциональные и неконвенциональные компоненты с упором на использование множества источников и режимов нападения, синергию результатов и высокий уровень неопределенности для оппонентов относительно конечных стратегических целей.

В гибридных конфликтах основными целями являются захват контроля над обществом, осуществление влияния на умонастроения людей, манипулирование людьми, которые отвечают за принятие важных решений в государстве. Противник пытается манипулировать основными ценностями, мотивационными факторами, культурным базисом и стратегической, коммуникационной и критической инфраструктурой страны. Это достигается

---

[13] Последний довод королей (использование оружия).

[14] Сергей Г. Чекинов и Сергей А. Богданов, «Природа и содержание войны нового поколения», *Военная мысль* 4 (2013): 12-23.

комплексным, сбалансированным осуществлением влияния с использованием мягкой и жесткой силы. Вот почему критические элементы систем, другими словами, объекты асимметричных действий в гибридных конфликтах, являются важными для ключевых элементов систем (компонентов, подсистем) государства, политических, дипломатических, социальных, технических, социотехнических, энергетических, финансовых, кибер, социо-кибер, информационных и других систем. Влияние на них в пределах оптимальных мер и корреляций параметров пространства, времени и ресурсов для оказывающей это влияние стороны приводит к желаемым, целенаправленным, быстрым, каскадным, синергетическим и деструктивным для этих систем изменений (нарушений) в их отношениях, структурах, процессах и результатах функционирования.

Гибридная война в Украине

Одной из отличительных характеристик «гибридной войны» на Украине является то, как широко она заняла все аспекты общественной жизни, сколько широкомасштабной, многомерной и мультифакториальной информации сконцентрировалось в психологических и кибер источниках. Хорошим примером такой деятельности являются новаторское и высокотехнологическое оружейное и военное оборудование, использованное при аннексии Крыма в 2014 году и боевые действия на востоке Украины[15] с 2014 года:

- Электронные военные системы и комплексы и другие виды электронных контрмер;
- Современные информационные и коммуникационные системы;
- Новаторские системы управления вооружением;
- Интегрированные разведывательно-ударные комплексы;
- Новаторское, в том числе автоматизированное, программное обеспечение;
- Комплексы для ведения информационно-психологических операций и действий в киберпространстве;
- Системы контроля окружающей среды и космические системы;
- Роботизированные системы (в частности, комплексы беспилотных летательных аппаратов) и контрмеры.

Технология существует не сама по себе, а как часть более широкой и стратегически спроектированной кампании по подрыву доверия в центральные институции. Первоначальной целью было создание условий для

[15] Смотри российский сайт о военных технологиях, http://www.rusarmy.com, и сайт Информационного агентства «Российского вооружения», http://www.arms-expo.ru.

утери гражданского доверия к правительству Украины путем осуществления информационной кампании, направленной на дискредитацию государственной власти, руководства украинских вооруженных сил и поощрения расширения преступной и сепаратисткой деятельности. Эта информационная кампания вызвала социально-политическую дестабилизацию в стране и продолжает оказывать отрицательное влияние и теперь.[16]

Эта стратегия успешно интегрировала новаторские кибер технологии в координации с тщательно спланированными действиями неконвенциональных и нерегулярных сил на месте, что привело в 2014 году к аннексии Крыма и к военному конфликту на юго-востоке Украины. В ответ на неконвенциональные и конвенциональные угрозы безопасности, как было упомянуто выше, большинство стран, располагающих способностями для быстрого реагирования, сосредотачиваются на двух основных компонентах их аппарата безопасности:

- Потенциал сдерживания, состоящий из традиционных видов вооруженных сил (сухопутные силы, военно-воздушные силы, военно-морские силы);
- Инновационный военный потенциал. Этот потенциал включает военное оборудование и личный состав Сил для специальных операций, информационно-психологические операции и средства электронной борьбы, а также кибер силы (кибер разведка, кибер безопасность и кибер операции), службы разведки (электронные средства разведки, разведка с использованием открытых источников (РИОС), технические виды разведки, наблюдения и рекогносцировки (PHP) и т.д.), коммуникацию для оперативного контроля, военные подразделения, которые оборудованы роботизированными (беспилотные летательные аппараты) комплексами и средствами для противодействия для соответствующих нападений, другие высокотехнологические ресурсы и меры.[17]

Создание высокотехнологических средств ведения военных действий

Технологический прогресс всегда был движущей силой военной стратегии. Технологически интенсивные войны связаны с проектированием и широким использованием передовых технических средств, систем и комплексов, созданных наиболее развитыми странами. Эти новшества дают определенным странам очевидное преимущество в ходе боевых действий без необходимости сосредотачивать преобладающие конвенциональные

[16] Jānis Bērziņš, “Russia’s new generation warfare in Ukraine: Implications for Latvian Defense Policy,” *Policy Paper* no. 02 (Riga: Center for Security and Strategic Research, National Defence Academy of Latvia, April 2014).

[17] Юрий Г. Даник, Д. Ищенко, О. Манько, «Военные аспекты классификации передовых технологических систем», *Научный журнал Житомирского военного института им. С. Королева* 8 (2013): 5-13 (на украинском).

Фотография 1: Применение инновационных конструкций помехозащищенных роботизированных комплексов военным персоналом Житомирского военного института им. С. Королева.

силы. Однако, более передовые в технологическом отношении государства могут быть более уязвимыми к определенным видам нападений.[18]

Новые возможности для воздействия на уязвимые места в сочетании с новым оружием и военным оборудованием привело к разработке, реализации и практическому использованию в ведущих странах новых стратегических концепций ведения военных действий: «Глобальная война», «Глобальная видимость», «Глобальное покрытие», «Сетецентрическая война», «Гибридные войны», «Стратегический паралич», «Параллельные войны», войны с использованием «Контролируемого хаоса», «Неограниченные войны», «Контролируемые войны» и т.д. Эти передовые концепции берут в расчет боевое воздействие на потенциального противника с расстояния путем использования разведывательной информационной поддержки, информационного и точного оружия, робототехнических технологий и других средств. Новаторские технологии управления, в отличие от прямых боевых действий, позволяют проведение атак в основном против приоритет-

[18] Юрий Даник и О.О. Труш, «Особенности обеспечения национальной безопасности в среде передовых технологий», *Государственная организация* 1 (2010), http://nbuv.gov.ua/UJRN/DeBu_2010_1_42 (на украинском).

ных целей с максимальной скоростью и точностью действий, воздействующих на «критические» компоненты на любой части территории государства (региона) без необходимости физического присутствия. Реализация такой проекции силы позволяет достижение стратегических целей без преодоления традиционных препятствий к победе в плане времени, расстояния и интенсивной логистики живой силы. Если целью стратегии безопасности является дестабилизация противника и использование его слабостей в критических узлах (подсистемах, компонентах, объектах), тогда нет необходимости контролировать его территорию силой. Наоборот, эти уязвимости, утечки безопасности, слабые логистические звенья, щели в системе безопасности, позволяют осуществлять подрыв существенных систем, необходимых для продолжения или даже для начала борьбы. Нефункционирование системы или любое другое деструктивное воздействие на объект делает государство, которое не смогло предпринять превентивные меры, неспособным использовать свой потенциал для адекватного ответа на последующие военные действия.

В сущности, государственная поддержка обороны в условиях гибридных угроз и гибридных военных действий требует существования сбалансированного и полномасштабного сектора национальной безопасности и обороны. Вооруженные силы остаются ключевым компонентом национальной безопасности, который должен реагировать на современные и будущие вызовы и угрозы. Вооруженные силы должны располагать современным оружием и военным оборудованием, адекватной организацией и подразделениями с квалифицированным личным составом. Этот квалифицированный персонал должен быть в состоянии вести интенсивные информационные и специальные операции с задачей оказывать воздействие на экономику, политику, энергетические системы, информацию и коммуникации, командование и управление, местное население и население страны противника.

Военные компоненты гибридной войны

В число особенностей военного компонента для высокотехнологических и гибридных войнах входят:

- Переход от стратегического управления к оперативному боевому управлению, основой которого является менеджмент поля боя в реальном времени и информационное превосходство над действиями противника: разведка, принятие решений и реализация, воздействия (лишение)[19]
- Переход от первичных ответственностей по ведению боевых действий к кибер и аэрокосмической среде, в том числе PHP[20]

[19] Joseph S. Nye, “Soft Power,” *Foreign Policy* 80 (Autumn 1990): 153-171.

[20] David A. Deptula and James R. Marrs, “Global Distributed ISR Operations: The Changing Face of Warfare,” *Joint Force Quarterly* 54 (2009): 110-115.

- Расширение арсенала средств ведения войны на основе роботизации, стелс концепций и дистанционных военных действий
- Формирование и использование ситуационных и автоматизированных комплексов и систем наблюдения и нападения
- Широкое использование эффективных нелетальных вооружений [21]
- Расширенное использование групп нерегулярной милиции (паравоенных формирований) [22]
- Соответствующее расширенное использование асимметричных боевых действий
- Расширение роли и участия Сил особого назначения [23]
- Расширение зависимости от радиоэлектронных, психологических и информационных средств ведения боевых действий через использование кибер активов [24]
- Переход к адаптированным к противнику методов ведения войны во всех сферах действий.[25]

Информационные и кибер действия

Сочетание исследований и анализа боевых действий показывает, что связанные с киберсферой действия и информационная война расширяются как в плане спектра, так и в плане значения для воюющих сторон. В этом контексте, гибридная война и использование кибер активов как части этого, являются наиболее важными факторами для понимания будущей дуги конфликта. Боевым действиям в Иловайске и Дебальцево на Украине предшествовал существенный подъем активности в информационном пространстве. Широко распространялась негативная информация о ключевых должностных лицах вооруженных сил Украины и представителях правительства (обычно вспышки отрицательной информации предшествовали

[21] Brian Rappert, *Non-lethal Weapons as Legitimizing Forces? Technology, Politics, and the Management of Conflict* (Abingdon, UK: Routledge, 2003).

[22] Frank G. Hoffman, "Complex Irregular Warfare: The Next Revolution in Military Affairs," *Orbis* 50, no. 3 (2006): 395-411.

[23] Dan Madden, Dick Hoffmann, Michael Johnson, Fred Krawchuk, John E. Peters, Linda Robinson, and Abby Doll, *Special warfare: The Missing Middle in US Coercive Options*. (Santa Monica, CA: RAND, 2014).

[24] Patrick M. Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Force Quarterly* 79 (2015): 46-53.

[25] Василь М. Телелим, Д. П. Музыченко и Ю. Ж. Пунда, «Планирование сил для сценариев 'Гибридной войны'», *Наука и оборона* 20, № 3 (2014): 30-35 (на украинском).

началу новой боевой кампании).[26] Эта массовая практика, которую Дугган называет кибер агрессией, дополняется дезинформацией с прокси и фальшивых фронтов в Интернете.[27]

Информационные и психологические операции (действия) врага в кибер пространстве требуют использования разных Интернет ресурсов. Примерами информационных и психологических операций являются подготовка и распространение конкретной информации в социальных сетях и других Интернет ресурсах, направленной на дискредитацию украинских властей, командования АТО и военного состава в рамках кампаний «Если не генералы», «Генералы-предатели Украины», «Слава украинской артиллерии» и т.д. Дезинформация, или непроверенная, фальшивая информация, в том числе с использованием специальных технологий для повышения рейтинга таких сообщений, часто распространяются в национальном кибер пространстве как военно-патриотические ресурсы. Необходимо отметить, что некоторые из этих Интернет ресурсов имеют хостинг в Российской Федерации[28] (Фотография 2).

Контент-анализ и моделирование потоков онлайн новостей во время наиболее интенсивных действий в Дебальцево в феврале 2015 года с использованием технологии для мониторинга новостей «InfoStream»[29] демонстрируют флуктуации амплитуды до критической для распространения сообщений степени.

Анализ СМИ показал существенные последствия от массового использования широко распространяемых, социально-политических информационных кампаний. Во-первых, ожидается, что кибер агрессия против ключевых фигур в правительстве стимулирует расширение диапазона негативных информационных потоков, направленных на углубление существующего гражданского недоверия и антигосударственного поведения. Когда такая информация доходит до социальных медиа, распространение фальшивой и зловредной информации поощряет убеждения и поведение, которые в нормальных условиях были бы ограничены существующими социальными нравами и общественными ожиданиями. Даже если информация не порождает сознательное изменение убеждений, она может оказывать влияние на интерпретацию будущей информации, создавая эффективный

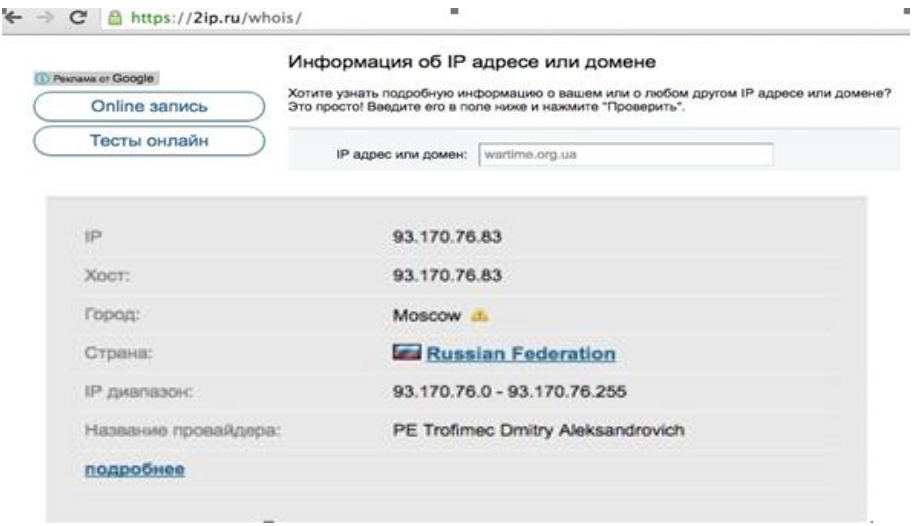
---

[26] Относительно примеров информационных операций дискредитации должностных лиц украинских вооруженных сил, смотри " Если бы не генералы ...," www.segodnia.ru/content/168270, https://topwar.ru/85589-esli-by-ne-generaly-pozornaya-istoriya-ukrainskoy-armii.html, http://colonelcassad.livejournal.com/2474409.html.

[27] Duggan, "Strategic Development of Special Warfare in Cyberspace."

[28] Смотри, к примеру, http://wartime.org.ua.

[29] InfoStream – Технология мониторинга новостей, http://infostream.ua.



Фотография 2. Пример Интернет ресурса, дискредитирующего командование вооруженных сил Украины, размещенном на сервере в Российской Федерации.[29]

фон и опорные пункты для толкования.[30] Это может добавить в картину местного агрессора, желающего оказывать влияние на ход конфликта с тем, чтобы ослабить поддержку подвергающемуся нападению правительству. В некоторых случаях такая информационная война может заменить кинетические операции, подрывая оборонительные кампании еще до того, как они начались.

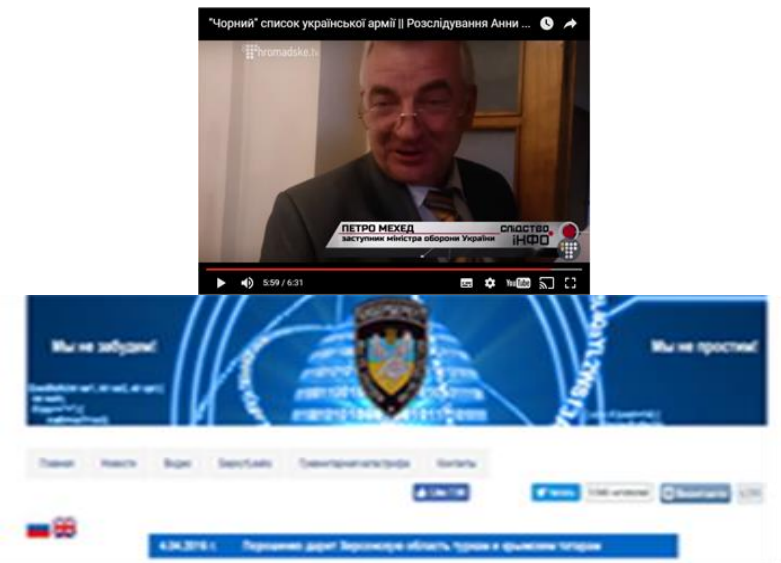
Кибер агрессия часто скрывает своих акторов и мотивов под плащом технологических методов, которые могут маскировать их манипулятивные цели. В число методов сокрытия входят анонимные претензии к властям, новости, манипулированные полуистинами, повторение сообщений, информационная перегрузка, кибер-псевдо операции (государство, выступающее в обличии повстанцев), использование «наручных кукол» (правительственные агенты, играющие роль онлайн комментаторов) и астротурфинг (создание ложных низовых движений).[31]

На Украине последствия таких действий после 2014 года привели к дискредитации Вооруженных сил, недовольству и недоверию, направленных в первую очередь против основных военных и политических властей в государстве, к сомнениям в необходимости военных действий, к нанесению

[30] Elizabeth Stoycheff and Erik C. Nisbet, "Priming the Costs of Conflict? Russian Public Opinion About the 2014 Crimean Conflict," *International Journal of Public Opinion Research* (2016): edw020. https://doi.org/10.1093/ijpor/edw020.

[31] Duggan, "Strategic Development of Special Warfare in Cyberspace."

ущерба гражданской морали и поощрению дезертирства среди военного персонала. При отсутствии конкретных контрмер против дискредитации украинских вооруженных сил, при недовольстве и недоверии, можно ожидать ослабления государственных и военных способностей, необходимых для ответа на агрессию. Более того, действия национальных медиа порталов, непреднамеренно или организованные Российской Федерацией, усугубили и без того уже сложную ситуацию призывами поощрять простые нарративы. Опора СМИ на ненадежные или фальшивые источники, подаваемые в негативном плане новости и критика действий руководства вооруженных сил, способствовали информационной кампании противника.[32] Российские силы смогли использовать уже существующие



Фотография 3. Пример манипулированием репутацией руководства Вооруженных сил средствами массовой информации.[33]

[32] Sazonov, Müür and Mölder, eds., *Russian Information Campaign Against the Ukrainian State and Defence Forces.*

[33] "Кибер Беркут", https://cyber-berkut.org, это Интернет бренд, за которым скрываются хакерские нападения главным образом на государственные и гражданские веб ресурсы в Украине. Глава бренда неизвестен. Jeffrey Carr, автор *Inside Cyber Warfare: Mapping the Cyber Underworld* (O'Reilly Media, 2009, 2011), считает, что это группа российских активистов. Группа описывает свои цели, в число которых входят борьба против неофашизма, национализма и воли правительства в Украине. Смотри также ТВ программу на Первом национальном ТВ канале Украины "Черный список украинской армии» (часть I), www.youtube.com/watch?v=BAlDnaG4VeM, и (часть II), www.youtube.com/watch?v=ksydsCllv0g.

уязвимости в социальной, политической и экономической системе для того, чтобы привести к открытому конфликту, причем климакс таких операций совпал с началом кинетических операций в Донбассе в 2014 году. Использование кибер активов стало формой проецирования силы, которое способствовало инициированию кризисов далеко впереди и за линией фронта, созданию форм более сложных кризисов, которые оказывали влияние на инфраструктуру, на банковскую систему, на политическое руководство, а не только на вооруженные силы, воюющие на передовой. Опять же, расширение традиционного военного конфликта не есть новая стратегия, но новые технологии обеспечивают как наличие средств, так и уязвимых мест, позволяющих проведение таких операций в масштабах, не часто имевших место ранее, и при меньших расходах на ресурсы со стороны агрессора.

Эффективная превенция и обнаружение информационных и психологических операций врага в кибер пространстве и наша быстрая реакция требуют создания национальных центров для контрмер против информационных и кибер атак. Национальные центры должны объединять и облегчать координацию между интернациональными центрами, обеспечивающими принятие контрмер против кибер угроз. Национальные центры должны обеспечивать мониторинг и обнаружение деструктивных воздействий и идентифицировать признаки, механизмы (стратегии, тактики, технологии, формы и методы) их реализации. Они должны выявлять источники и варианты распространения опасного содержания, взаимосвязь во время операции (действий) между разными Интернет ресурсами для определения цели действий и возможных последствий.

Мерами для нейтрализации деструктивных информационных и кибер воздействий являются:

- Предупреждение собственников (если они известны) Интернет ресурсов об ограничениях, касающихся распространения ложной, недостоверной информации с рекомендацией об ее стирании, если эта информация наносит ущерб субъектам и объектам национальной безопасности (личностям, обществу, государству)
- Создание публичных регистров ненадежных/подозрительных ресурсов.

В случаях, когда невозможно определить хозяина или модератора, а содержание может превратиться в реальную угрозу для субъектов и объектов национальной безопасности, дается рекомендация заблокировать электронные информационные ресурсы, стереть содержание и т.д.

Кризисные ситуации

Кризисные ситуации появляются, когда внешние силы (агрессия и/или естественные) используют уязвимости и поражают критические системы в целевом регионе или целевой силе. Эти кризисы могут быть результатом

информационных или кибер действий в условиях гибридного конфликта, результатом осуществления информационных, психологических и кибер угроз (напр. террористических, военных, дипломатических, политических и т.д.), направленных против критической инфраструктуры государства или системы управления и командования вооруженными силами. Утеря или интенсивная деградация работоспособности может быть осуществлена как нелинейная функция, т.е. воздействие может не быть очевидным до полного сбоя целевой системы.

Эффективные меры в кризисных ситуациях в кибер пространстве в соответствии с опытом АТО (операция в оккупированных районах Украины) могут быть реализованы при:

- Систематическом развитии форм, методов и средств оперативного обнаружения, защиты и предприятия активных контрмер против информационных угроз в киберпространстве
- Научном исследовании и развитии потенциала для разработки специального программного обеспечения и аппаратных средств для информационной деятельности в киберпространстве
- Профессиональном военном образовании и квалификации, основанных на боевом опыте и уроках практики в этой сфере
- Проведении прикладной национальной и международной подготовки, компьютерных военных игр и консультаций
- Усовершенствовании подготовки и образования военных и гражданских специалистов в сфере информационной и кибер безопасности
- Оперативной реализации уроков практики в национальных и международных системах безопасности.

Опыт показывает, что эффективное использование методов гибридной войны приводит в целом к непредсказуемым схемам кризисов и реакций. Для практиков гибридной войны, как правило, не существуют четко запрограммированные результаты и последовательность событий, и потому те, кому приходится реагировать на такую стратегию, должны уметь адаптироваться к динамичной и быстро меняющейся среде.

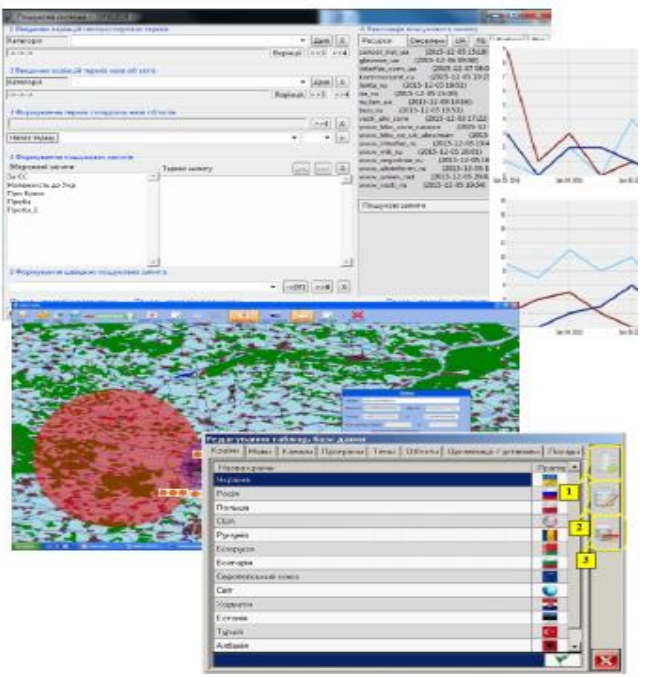
Технологический дизайн хорошо известных систем контрмер в кризисных ситуациях, формы, методы и использование систем должны быть направлены на формирование статически избыточной структуры целевой системы. Распределение задач между всеми компонентами кибератак на систему часто является равномерным с выбором компонентов только в соответствии с их предназначением. Увеличение количества и плотности потока кризисных ситуаций приводит к структурной сложности систем, созданных для реакции на них. Схема распределения обеспечивает информационное дублирование данных и приводит к усложнению их передачи и обработки. Те же принципы лежат в основе проектирования программного обеспечения, предназначенного для осуществления процесса опера-

тивного выявления, защиты и предприятия активных контрмер против информационных угроз в киберпространстве. Упомянутые подходы не являются достаточно эффективными в реальных условиях конфликта, когда противник применяет равные или превосходящие ресурсы для информационной войны, за которыми следует использование мягкой силы или кинетических операций для достижения его целей. Такой подход является ключевой особенностью современных гибридных войн.

Тщательное применение принципов ситуационного управления дает возможность для рационального распределения и перераспределения собственных ресурсов и концентрации сил на критических (для обеспечения безопасности) направлениях действий врага.

Методы фрактального анализа, самоорганизации и бифуркационные модели дают возможность вовремя обнаруживать угрозы и кризисные ситуации, прогнозировать их развитие и реальные цели.

На практике такой подход увеличивает эффективность контрмер против средств информационной войны в результате улучшения систем предупреждения, комплексности и точности информации и своевременности реакции.



Фотография 4. Внешний вид одного из комплексов контрмер против психологически-информационного воздействия.

Фотография 5. Автоматизированная система контент-мониторинга информации в социальных Интернет сервисах «Monitoring-C».

Сферы гибридной войны

Критически важным соображением является воздействие действий агрессора, желающего увеличить внутреннюю нестабильность во многих сферах (Фиг. 2). Желаемое воздействие может включать повышение недоверия к институциям и общим ценностям, эрозию экономической активности и доверия, приведение в замешательство объективности, экспертизы, идеологии и других источников социальной кохезии.[34]

Гибридные войны отличаются существенно от традиционных войн как в плане инициирования, так и протекания, используются разные стратегии и оперативные средства. Гибридные войны похожи на нерегулярные конфликты (или ИВ – иррегулярные войны) в смысле использования иррегулярных или невоенных сил, или по крайней мере, сил, скрывающих свою национальную принадлежность, оставаясь анонимными или использующими фальшивый камуфляж под местные милиции. В реализации операций участвуют силы особого назначения, саботажно-рекогносцировочные группы и разведывательные подразделения разных оттенков.[35] Для некоторых вооруженных сил или государственных сил безопасности, специальные операции могут подразумевать осуществление специфической информационной или кибер деятельности, электронных операций или саботаж-

[34] Телелим, Музыченко и Пунда, «Планирование сил для сценариев ‘Гибридной войны’»; Кофман, «Русская гибридная война и другие темные искусства»; Валерий Герасимов «Значение науки в прогнозировании», *Военно-промышленный курьер* 8 (2013): 1-3.

[35] Gerasimov, “The Value of Science in Prediction.”

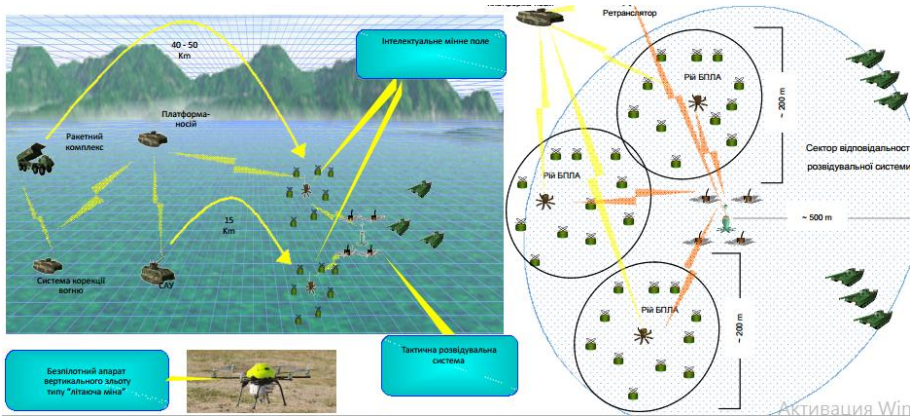
ных действий, направленных на разрушение критических узлов, которых нельзя добиться традиционными средствами.

Следовательно, делом первостепенной важности для обороны государства в современных условиях является создание эффективных систем контрмер. Такие системы должны включать передовые в технологическом отношении разведывательные, электронно-разведывательные, информационные и психологические операции и кибер операции, которые могут быть скоординированными для создания общей стратегии и автономными так, чтобы их можно было бы осуществлять отдельно или как часть других операций.

Ключевым элементом такой независимой функциональности в PHP и боевых операциях является разработка и использование беспилотных мобильных средств. Расширение использования беспилотников в разных функциональных областях (разведка, электронное противодействие, нанесение ударов и т.д.) и разные среды функционирования (земля, вода, воздух, амфибийные) является важным соображением для обеспечения гибкости в динамичных конфликтных ситуациях.

Применение способностей в сфере передовых методов разведки и реакции должно разрабатываться параллельно с подготовкой военного и гражданского персонала, который будет работать с системой. Нельзя рассчитывать, что технология будет работать как надо без высоко квалифицированного персонала, который может использовать, поддерживать и далее развивать комплексные системы, необходимые для работы при изме-

Фигура 1: Сферы гибридной войны.



Фотография 6. Комплекс ударных беспилотных летательных аппаратов для специальных операций «Летающие мины».[36]

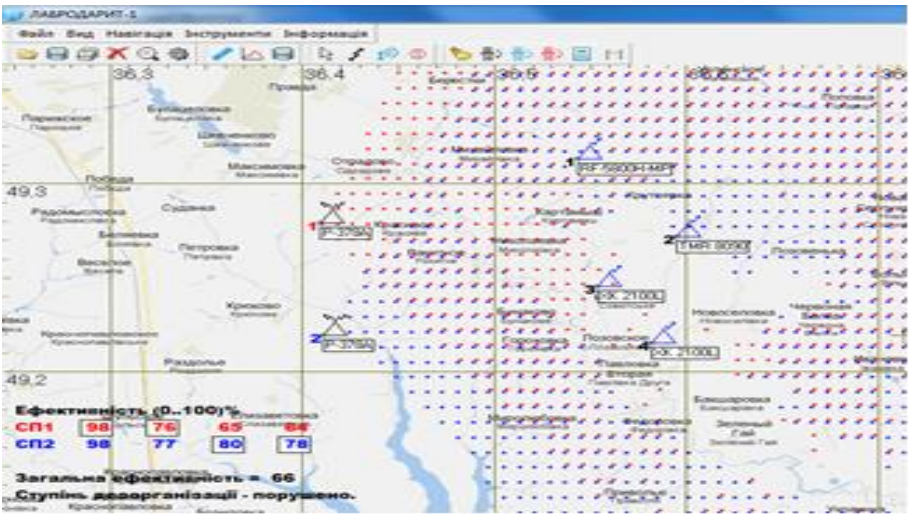
няющемся характере поля боя. На полные, эффективные боевые способности можно рассчитывать только тогда, когда стратегия и технология разрабатываются в координации с профессиональной квалификацией. Непрофессиональное использование таких технологий часто является причиной для плохих результатов их работы, как случается, например, когда стандартные оперативные процедуры при подготовке ссылаются на более старые концепции проблемы (к примеру, кибер взлом информационных сетей рассматривается как техническая проблема, а не как риск для национальной безопасности).

Кластер передовых технологий для обороны

За подготовку и менеджмент карьерного развития личного состава в сфере обороны в первую очередь отвечает государство. Поэтому для обеспечения соответствующего уровня поддержки обороны страны должны сосредоточиться на создании и развитии технологических систем в секторе обороны с интегрированными исследовательскими и экспериментальными способностями. Расширяя диапазон функций вне пределов раннего предупреждения, обеспечиваемого центрами «гибридных угроз», учрежденных в некоторых странах НАТО, такие кластеры будут предназначены для разработки соответствующих технологий и стратегий против будущих угроз, которые они должны быть в состоянии идентифицировать.

Предлагаемый Кластер передовых технологий для обороны будет включать:

[36] Это разработка Житомирского военного института им. С. Королева.



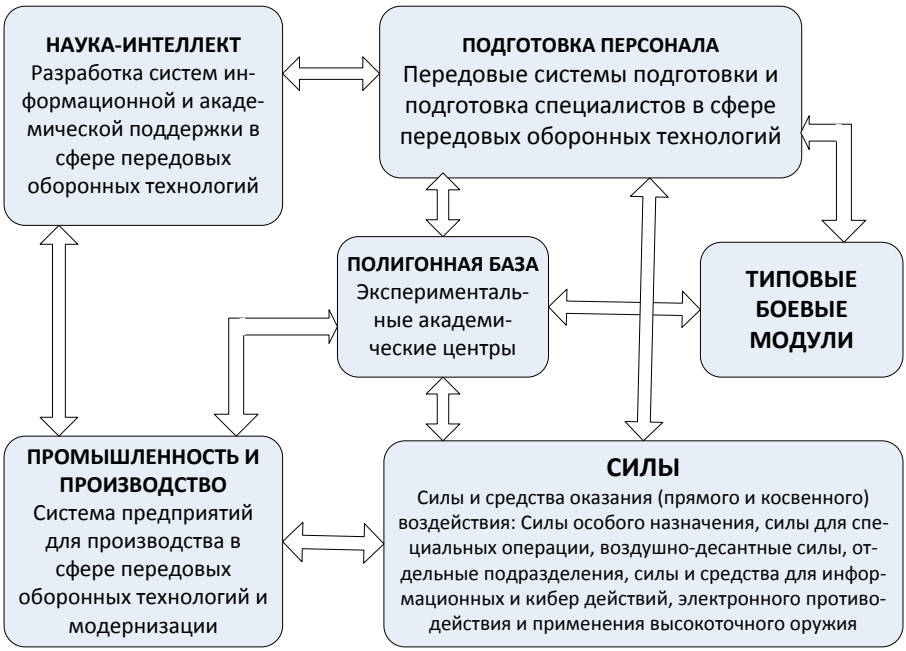
Фотография 7. Скриншот из планирующей системы для электронной борьбы для планирования боевого расположения подразделений.

- Робастную систему военного исследовательского потенциала с соответствующей научной организационной структурой
- Академическую ориентацию на экспертизу в области передовых технологий
- Научно-производственный комплекс с стационарными и мобильными образцами оружия и военного оборудования, командных пунктов и лабораторий
- Передовые в технологическом отношении экспериментально-боевые и боевые подразделения, сформированные в соответствии с результатами академических/научных исследований кластера (Фигура 2).

Практическая подготовка военного персонала, испытания и использование новых технологических систем вооружения и военного оборудования и формирование новых подразделений должны основываться на разработках оборонного технологического кластера и действующих военных подразделений.

Что касается Украины, необходимо создать Военный научно-технический экспертный центр в сфере передовых технологий с целью:

- избежать дублирования функций разных организаций
- обеспечить концентрацию в одном месте работ по исследованию, разработке, производству, испытаниям и использованию передовых технологических систем



Фигура 2: Кластер передовых технологий для обороны.

- подготовки персонала в сфере передовых технологий для всех родов войск в Вооруженных силах и других министерствах и институтах в секторе национальной безопасности и обороны государства
- использования военного компонента, промышленной и производственной базы региона
- избегания дополнительных расходов финансов и времени.

Реализуемость такого центра можно доказать и поддержать, основываясь на опыте ведущих стран, собранного в ходе исследования новаторских идей и их реализации в военной сфере, например DARPA (Управление для перспективных исследовательских проектов Министерства обороны США). Рациональную проработку всех практических вопросов Кластера передовых технологий для обороны следует провести в тесной координации с центральными органами командования и управления Вооруженными силами. Он должен работать напрямую с силами, сотрудничая с центральными органами управления. Центральные органы управления корреспондируют с военными частями и подразделениями с их полигонной базой и взаимодействующими организациями/структурами.

Заключение

Политика государства в отношении передовых технологических, информационных и кибер систем обеспечения безопасности стала одним из наиболее важных компонентов национальной политики безопасности в военной сфере. Современные технологии изменили способности оказания воздействия на силы противника, порождая необходимость в реорганизации менеджмента и защиты против мягких и военных способов воздействия, в том числе, подготовки личного состава для непрерывного поддержания боеготовности сил. Опыт разных стран, которые уже столкнулись с новыми формами гибридной войны, доказывает, что высокий уровень состояния национальной безопасности и обороны нужно поддерживать даже в условиях мирового экономического кризиса и существенно уменьшенных расходах на вооруженные силы. Расширение поля боя за пределы кинетических операций и нападений на инфраструктуру требует комплексного использования как доктрин традиционных сил, так и нового технологического и синергетического планирования.

Опыт военных конфликтов в последнем десятилетии показывает, что стратегическим преимуществом располагает тот из акторов, кто первым поймет и начнет применять новые технологии, кто может использовать их как усилитель своих способностей и потому может взять верх над превосходящими конвенциональными силами, – и часто даже без провоцирования устойчивой реакции. Командиры должны использовать новые методы и доктрины, даже только для того, чтобы понимать новые методы и доктрины, которые может применить противник. Использование передовых технологических систем дает возможность повысить эффективность уже существующего военного потенциала государства при меньших расходах, возможно даже одной третью традиционного бюджета. Рассматривая концепции национальной безопасности и национальные военные стратегии, государства наиболее развитых стран отдают высший приоритет образованию и науке как инструментам создания технологически интенсивных средств военных действий, применяя новаторские технологии управления и способствуя быстрой и убедительной победе в настоящих и будущих военных конфликтах.

Об авторах

Генерал-майор Юрий Даник является профессором и доктором технических наук. Он закончил с красным дипломом Высшее военное училище радиоэлектроники в Житомире, Харьковский военный университет (оперативно-тактический уровень), Национальную академию публичной администрации при президенте Украины, Национальный университет обороны Украины (оперативно-стратегический уровень). Он является экспертом по военному искусству, национальной обороне и безопасности, информационной и кибербезопасности, электронной войне, проектированию и применению роботизированных комплексов и развитию специальных сил. У него имеется боевой опыт в применении высоких технологий.
E-mail: zhvinau@ukr.net

Тамара Малярчук имеет степень магистра наук. С 2013 года она работает в житомирском военном институте им. С. П. Королева, и в 2014 году поступила в аспирантуру Житомирского государственного университета им. Ивана Франко. В 2014-2016 годах она посещала форумы и семинары по электронному обучению (в национальных академиях обороны Болгарии и Румынии), организованные странами НАТО и членами инициативы Партнерство ради мира. В 2015 году Тамара закончила курс по военной английской терминологии в Национальной академии обороны Польши в Варшаве. В мае 2016 года она прошла курс в Языковом институте обороны в Лэкланде, Сан Антонио, Техас, США. Она проводит исследования по электронному обучению, новаторским технологиям в диагностировании и лечении ПТСР, манипулятивным технологиям в веб-среде.
E-mail: maliarchuktamara@gmail.com

Доктор Чад Бриггс является главным консультантом компании Global INT. У него степень доктора по политологии, полученная в Университете Карлтона в Канаде, и он специализируется на переводе комплексных научных данных в системах оценки риска и стратегического планирования. До этого он работал с Департаментом энергетики США по критически важным оценкам безопасности, и в 2010-2012 был председателем комитета инициативы «Минерва» по энергетической и экологической безопасности при Авиационном университете Военно-воздушных сил США. Он является старшим научным сотрудником Института экологической безопасности в Гааге, профессором публичной политики в РИТ Косово и адъюнкт-профессором по глобальной безопасности при университете им. Джона Хопкинса.
E-mail: cbriggs9@jhu.edu.