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

Андраш Худик, *Connections QJ* 19, № 4 (2020): 29-44
https://doi.org/10.11610/Connections.rus.19.4.02

Рецензированная статья

Лучшие практики в применении концепции устойчивости: создание способностей для гибридной войны и кибербезопасности в Силах обороны Венгрии

Андраш Худик

Резюме: В своей Глобальной стратегии внешней политики и безопасности ЕС применяет устойчивость как всеобъемлющую концепцию внутренней и внешней безопасности. Параллельно с этим, на саммите 2016 года в Варшаве лидеры Североатлантического союза решили повысить устойчивость НАТО к полному спектру угроз. Каждый член НАТО должен быть устойчивым к серьезным потрясениям, вызванными стихийными бедствиями, отказом критически важной инфраструктуры, средствами гибридной войны или вооруженным нападением. Гибридная война, включая кибератаки, считается серьезной проблемой безопасности.

Стратегия национальной безопасности Венгрии, принятая в 2020 году, подтверждает, что основной международной рамкой политики Венгрии в области безопасности и обороны является членство в НАТО и ЕС, и подчеркивает необходимость повышения устойчивости страны к гибридным атакам. В этой статье представлен анализ применения концепции устойчивости в оборонном секторе Венгрии. Он знакомит нас с развитием устойчивости сил обороны Венгрии к гибридным угрозам, включая их кибер-компонент, а также дает лицам, принимающим решения, варианты для выбора в отношении военных и информационных инструментов национальной мощи. Автор определяет потенциальные гибридные угрозы против Венгрии, возможный сценарий кибератак и направления усилий для достижения максимально возможного уровня устойчивости к таким угрозам. Он принимает во внимание политическую и военную среду, а также более широкие национальные проблемы с учетом гибридных угроз и основных характеристик и дилемм кибервойны, таким образом стремясь способствовать применению концепции устойчивости в Венгрии.

Ключевые слова: устойчивость, политика безопасности, вооруженные силы, разведка, гибридная война, киберзащита, ЕС, НАТО, Венгрия.

Введение: Применение концепции устойчивости в Венгрии

Целью применения концепции устойчивости является усиление способности систем, организаций, политик и отдельных лиц оптимально реагировать на внешние воздействия. Многие эксперты сходятся во мнении, что «недавний энтузиазм по поводу концепции устойчивости во многих публикациях по политикам устойчивости является следствием ее соответствия неолиберальному дискурсу. Это не означает, что идея устойчивости сводится к неолиберальной политике и неолиберальному управлению, но она точно соответствует тому, что они пытаются сказать и сделать».[1]

Идеология неолиберализма в первую очередь видит гарантию экономического роста, благосостояния, свободы и общего блага в «либерализации» рынков. Неолиберальное государство радикально отходит от перераспределения, характерного для государства всеобщего благосостояния, принимает меры, благоприятствующие бизнесу и рынку, для защиты доходов частного капитала и превращает граждан в предпринимателей и потребителей.

Крах неолиберальной гегемонии после 2008 года привел к новой волне популизма. Популистские партии и движения включают в себя как левых, так и правых деятелей. Одна из их немногих общих черт заключается в том, что все они критикуют правящую элиту и ее идеологию заявляя, что элиты угнетают людей.

Согласно левой риторике, социальная и экономическая политика популистского правительства Орбана в Венгрии заключается в укреплении национального капиталистического класса, продаже дешевой рабочей силы иностранным промышленным инвесторам, при этом дисциплинируя этих рабочих и осуществляя централизованный контроль над бедными, в основном живущими в сельских районах. Целью его культурной политики является продвижение официальной венгерской идеологии эпохи до 1938 года: консервативная, христианская, националистическая идеология, основанная на исторической лжи, с несправедливой социальной системой, атмосферой ненависти и скрытым намерением вернуть территории, утраченные после Первой мировой войны. Орбан воспринимает неолиберальный Европейский Союз, тайные мошеннические действия международных капиталистов, олицетворяемые Джорджем Соросом, и мигрантов как врагов, чтобы объявить своих политических оппонентов врагами нации и взять на себя роль ее спасителя.

В то время как правительство атакует некоторые ценности ЕС перед политической аудиторией и вызывает громкое противостояние, с точки зре-

[1] Jonathan Joseph, “Resilience as Embedded Neoliberalism: A Governmentality Approach,” *International Policies, Practices and Discourses* 1, no. 1 (2013): 38-52, https://doi.org/10.1080/21693293.2013.765741.

ния экономических процессов, оно является подчиненным союзником европейских капиталистов.[2] Из-за конструктивистских элементов политики Виктора Орбана по установлению режима,[3] демократия, верховенство закона и плюрализм в Венгрии стали ограниченными и привели к созданию страны с нелиберальной демократией. В Венгрии те, кто находится у власти, полагают, что левые и либералы не являются частью нации, и все, что является левым или либеральным, будь то личность, любое произведение искусства, или просто точка зрения или подход, должно считаться чуждым и должно быть отвергнутым, потому что оно противоречит официальному национальному христианскому консервативному курсу.

Возможно, этот политический климат также способствует тому факту, что в Венгрии только оборонная наука, связанная с НАТО, инициирует разработку концепций безопасности и правоохранительной деятельности на основе устойчивости. Однако более правдоподобное объяснение состоит в том, что, в отличие от общепринятой всеобъемлющей политики безопасности и подхода к кризисному управлению, в отношение устойчивости мы должны сосредоточиться на решениях на национальном уровне. Многие венгерские эксперты считают это свидетельством целесообразности усилий по разработке комплексного подхода на национальном уровне, которые были начаты в нашей стране в 2010 году.

Большинство венгерских экспертов по политике безопасности считают, что в 2014 году во время украинского кризиса и НАТО, и ЕС нашли адекватный ответ на гибридные угрозы в повышении устойчивости стран и в поддержке военных усилий с помощью гражданских инструментов (гражданской готовности). Сама суть этого решения заключается в скоординированном применении военных и гражданских компонентов кризисного менеджмента, что также является основным принципом комплексного подхода.

Таким образом, можно считать, что предпосылки, фундаментальные принципы и инструментарий, применяемые для обеспечения устойчивости и гражданской готовности, практически совпадают с самим комплексным подходом; они являются всего лишь его переосмыслением в другом контексте. Поэтому, устойчивость и гражданская готовность не повлекли за собой иной образ мышления или набор требований. Тем не менее, их нельзя рассматривать как идентичные каким-либо уже существующим комплексам задач в соответствии с каким-либо законодательством.

---

[2] Тамаш Героч и Чаба Елинек, «Система венгерского национального сотрудничества в контексте Европейского Союза – об интеграции Венгрии в ЕС, исторический и социологический подход», *Analízis* (2018): 12-33 цитата на стр. 23, www.regscience.hu:8080/xmlui/bitstream/handle/11155/1768/jelinek_nemzeti_2018.pdf, – на венгерском.

[3] Gábor Illés, András Körösényi, and Rudolf Metz, "Broadening the Limits of Reconstructive Leadership – Constructivist Elements of Viktor Orbán's Regime-building Politics," *The British Journal of Politics and International Relations* 20, no. 3 (2018): 790-808, https://doi.org/10.1177/1369148118775043.

Следовательно, необходимо законодательно назначить национального координатора как для обеспечения устойчивости, так и для обеспечения гражданской готовности, а также для определения объема задач национального уровня, органов и организаций, ответственных за их выполнение, сотрудничающих организаций и процессуальных правил сотрудничества. Учитывая, что эта задача требует тесного и всестороннего сотрудничества всего правительства, эффективное выполнение этих обязанностей должно входить в компетенцию и возможности системы администрации обороны.[4]

Создание в Силах обороны Венгрии способностей для противодействия гибридной и кибервойне

Венгерские силы обороны

Венгерские силы обороны (ВСО) – это национальные силы обороны Венгрии. С 2007 года в Венгерских вооруженных силах действует единая командная структура. Министерство обороны осуществляет политический и гражданский контроль над армией. Подчиненное министерству Командование объединенных сил координирует и командует подразделениями ВСО.

В вооруженных силах несут действительную службу 28 000 человек. В 2019 году военные расходы составили 1,904 миллиарда долларов США, или около 1,2% ВВП страны, что значительно ниже целевого показателя НАТО в 2%. В 2016 году правительство приняло решение, согласно которому обязалось увеличить расходы на оборону до 2% ВВП, а численность действующего персонала – до 37 650 к 2026 году. Военная служба является добровольной, хотя в военное время может осуществляться и призыв.

Согласно Конституции Венгрии, тремя столпами безопасности нации являются способности ВСО, система Альянса и граждане.

В феврале 2017 года Министерство обороны обнародовало программу развития Зриньи 2026, которая направлена на повышение способностей действующих вооруженных сил, численности резервных сил, военной коммуникационной и информационной систем, а также для киберзащиты. Эти меры кажутся адекватными шагами для повышения устойчивости к гибридным угрозам.

Подход к повышению устойчивости к гибридным атакам

Гибридная война означает «использование военных и невоенных инструментов в интегрированной кампании, направленной на достижение внезап-

[4] Ласло Кесели, «Гибридная война и национальная устойчивость, или перезагрузка комплексного подхода», *Katonai Jogi és Hadijogi Szemle [Военное право и Обзор военного права]* 1 (2018): 29-62, цитата на с. 61-62, http://epa.uz.ua/02500/02511/00008/pdf/EPA02511_katonai_jogi_szemle_2018_1_029-062.pdf. – на венгерском.

ности, захват инициативы и получение психологических, а также физических преимуществ с использованием дипломатических средств; сложные и быстрые информационные, электронные и кибероперации; тайные, а иногда и открытые военные и разведывательные действия; и экономическое давление».[5] Другими словами, гибридные атаки сочетают в себе военные и невоенные, а также скрытые и открытые средства, включая дезинформацию, кибератаки, экономическое давление и развертывание нерегулярных вооруженных групп, а также использование регулярных сил. В настоящее время гибридная война считается серьезной проблемой безопасности; к этой более широкой категории угроз относятся кибератаки, которые воспринимаются как одна из основных угроз современному обществу каждой страны.

На фигуре 1 показан проект Сил обороны Венгрии в области повышения устойчивости к гибридным атакам, основанный на выводах Адриана Фехера.[6] Фехер следовал шагам методологии армейского строительства,[7] и поэтому описывает желаемую среду, определяет проблему и рекомендует оперативный подход. После модификации этим автором подход, используемый в проекте, состоит из шести целей, семи итогов и 15 предлагаемых результатов, которые должны повысить уровень устойчивости к гибридным угрозам и, таким образом, защитить страну. На фигуре показано сопоставление инструментов национального могущества с каждым из результатов.

Основная логика предлагаемого подхода заключается в том, что Венгрии нужна гибридная стратегия защиты для борьбы с потенциальными гибридными угрозами. Военный инструмент национальной мощи должен расширять свое значение и способствовать повышению информационной мощи, развитию потенциала информационного сдерживания для защиты суверенитета Венгрии посредством участия граждан. В то же время существует потребность в поддержке со стороны других агентств в создании потенциала информационного сдерживания для защиты населения от враждебной пропаганды и кибератак. Поскольку военный инструмент сильно зависит от других инструментов национального могущества, ВСО должны поддерживать и улучшать сотрудничество с другими заинтересованными сторонами, чтобы осуществлять «общегосударственный» подход. Область информации и связанные с ней информационные операции играют важную роль в гибридной войне. Исторически сложилось так, что военные операции в

---

[5] James K. Wither, “Making Sense of Hybrid Warfare,” *Connections: The Quarterly Journal* 15, no. 2 (2016): 73-87, цитата на стр. 76, https://doi.org/10.11610/Connections.15.2.06.

[6] Adrian Feher, “Hungary’s Alternative to Counter Hybrid Warfare,” Thesis (Fort Leavenworth, Kansas: U.S. Army Command and General Staff College, 2017), 128, 123, https://apps.dtic.mil/dtic/tr/fulltext/u2/1038681.pdf.

[7] Headquarters, Department of the Army, *Army Design Methodology*, ATP 5-0.1, July 1, 2015, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp5_0x1.pdf.

первую очередь сосредоточивались на способностях противника и только во вторую очередь – на ослаблении его решимости, тогда как информационные операции нацелены на ослабление его решимости и силы воли.

Целью информационных операций является достижение превосходства в лидерстве, информационного господства и информационного превосходства путем использования психологических операций и операций по обеспечению операционной безопасности, военному обману, физическому уничтожению, радиоэлектронной войне, общественной информации, компьютерным сетевым войнам и военно-гражданскому сотрудничеству с использованием военных информационных систем и разведывательной информации.[8] В доктрине информационных операций, применяемой в настоящее время Силами обороны Венгрии, детали концепции информационных операций еще не разработаны. Элементы информационных операций лишь частично отражают действия и способности, которые должны быть достигнуты в информационной среде. Эксперты утверждают, что главная задача, стоящая перед Силами обороны Венгрии, заключается в достижении способности решать сложные информационные вопросы: быстро получать, обрабатывать и интегрировать информацию в цикл принятия решений, а также контролировать нарративы о конфликтах в информационном пространстве.

Цель проекта: **Защита суверенитета и независимости Венгрии за счет повышения устойчивости к гибридным угрозам**		
Цели	Итоги и инструменты	Результаты
Обладать потенциалом военного сдерживания, чтобы остановить врага и поддержать интервенцию сил НАТО в Венгрии.	Повышение способностей добровольных резервных конвенциональных сил **(В&И)** и создание добровольческих неконвенциональных резервных силы **(В&И)**	1, 2, 3, 4, **5**, 7, 9, 10, 12, 13, 14, 15
Обеспечение конституционного порядка и оказание поддержки	Создание способностей для добровольной гражданской готовности (**В&И**)	1, 2, 3, 4, 6, 7, 9, 10, 12, 13, 14, 15

[8] Жолт Хейг, «Методология определения критических информационных инфраструктур, информационная война», ENO Advisory Ltd., 1 августа 2009 г., с. 88, https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf; Жольт Хейг и Иштван Вархеги, «Интерпретация киберпространства и кибервойны», *Военная наука* (2008): 5-10, на венгерском языке, http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf.

центральному правительству	Достичь приверженности граждан делу защиты нации **(И)**	1, 2, 3, 4, **5**, 7, 8, 9, 10, 12, 15
Помощь союзникам по НАТО в условиях коллективной обороны	Увеличение экспедиционного потенциала действующих сил (**В**)	1, 2, 3, **5,** 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Развитие информационных способностей для сдерживания	Защита граждан от средств враждебного влияния и национальных сил от кибератак **(И)**	1, 2, 3, **5**, 6, 7, 9, 10, 13, 15
Предотвращение неожиданности	Создание интегрированных средств разведки, наблюдения и рекогносцировки - обеспечение оперативной безопасности **(И)**	2, 3, **5,** 6, 9, 15
Следование «общегосударственному» подходу к обороне	Обеспечить межведомственное взаимодействие **(ДИВЭ)**	1, 2, 3, 4, **5**, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Результаты: (1) Повышение патриотизма через социальные и традиционные СМИ; (2) Устранение ложного чувства безопасности; (3) Выявление и опровержение ложных новостей; (4) нанятие волонтеров; (5) **Увеличение способностей для кибервойны**; (6) Улучшение контрразведки для выявления и обнаружения предупреждающих сигналов; (7) Проведение совместных и комбинированных учений (упражнений); (8) Устранение / интеграция экстремистских групп и создание движения сопротивления; (9) Выявление уязвимостей и пробелов в способностях; (10) Установление децентрализованного командования и управления с безопасной связью; (11) Обеспечение быстрого реагирования через правовую систему; (12) Создание систему готовности и мобилизации; (13) Обеспечить обучение и экипировать силы; (14) Создание предварительно размещенных запасов; (15) Обеспечение координации лиц, принимающих решения;		

Фигура 1: Проект по повышению устойчивости к гибридным атакам.
Сокращения: ДИВЭ - инструменты дипломатии, информации, военного дела и экономики; В (военный инструмент), И (информационный инструмент), В&И (военный и информационный инструмент).

В то же время необходимо развивать оперативные возможности ВСО в киберпространстве и обеспечивать их интеграцию как в военное планирование, так и в выполнение операций. С этой целью Силы обороны Венгрии должны принять новый образ мышления, в первую очередь сосредотачиваясь не только на проведении боевых действий, но и на желаемых результатах таких военных операций, включая влияние таких результатов. В военной

доктрине необходимо более широкое толкование системы информационных инструментов. Недостаточно рассматривать их как выполняющих простую вспомогательную функцию.

Киберзащита в Венгрии

Основные аспекты и дилеммы кибервойны

Как правило, в кибервойне государства начинают свои операции в разведывательных целях с подрывными или деструктивными намерениями и делают это напрямую или с привлечением третьих сторон, таких как хакеры. Атаки могут быть нацелены на критически важные публичные инфраструктуры, в частности на ИТ, информационные и коммуникационные системы, используемые в оборонном секторе. Кроме того, все более распространенными становятся враждебные действия с использованием социальных сетей и Интернет-платформ для воздействия на гражданское общество. В более широком смысле кибервойна охватывает все атаки, осуществляемые в киберпространстве, с полезными результатами для нападающего в военном или политическом плане.[9] Опыт показывает, что кибератака ложится серьезным бременем на страну только в том случае, если она скоординирована (связывает военное управление со стратегической целью, которой подчиняется каждое оперативное действие), происходит волнами (типы и цели атак разнообразны, непредсказуемы и они осуществляются последовательно), является многосекторальной (затрагивает несколько отраслей, в то время как координация обороны обычно охватывает лишь небольшой круг секторов), поддерживается информацией, полученной разведкой (информация, необходимая для атак, поступает не только из открытых источников, но и в результате сбора и анализа разведданных), и в первую очередь осуществляется для нанесения ущерба противнику. Цель состоит в том, чтобы заставить страну и ее граждан почувствовать атаку, т.е. такие атаки должны быть очень очевидными и включать эмоциональные воздействия – характеристики, которые отличают их от кибершпионажа.[10] Кибератаки обычно не используются государствами в деструктивных целях в мирные периоды, поскольку пребывание в «серой зоне» между миром и

[9] Тибор Рожа, «Теория, практика и тенденции информационных операций», *Оборонное обозрение 5* (2019): 82-84; Габор Берк, «Киберпространство, его опасности и текущее состояние киберзащиты в Венгрии», *Обзор национальной безопасности 3* (2018): 5-21, http://epa.oszk.hu/02500/02538/00024/pdf/EPA02538_nemzetbiztonsagi_szemle_2018_03_005-021.pdf; Жолт Чутак, «Новая война новых времен – когнитивная безопасность в эпоху информации и кибервойн», *Оборонное обозрение 5* (2018): 33-45, http://real.mtak.hu/84099/1/hsz_2018_5_beliv_033_045.pdf. – все источники на венгерском языке.

[10] Csaba Krasznay, “Protecting Citizens in a Cyber Conflict,” *Military Engineer* 7, no. 4 (December 2012), 142-151, цитата на стр. 144, http://hadmernok.hu/2012_4_krasznay.pdf.

войной наилучшим образом служит их интересам. Это не значит, что они не смогут выйти за пределы этой зоны в случае необходимости.

Основная дилемма кибервойны – отсутствие международного регулирования киберпространства. Хотя большинство государств-членов ООН признают расширение сферы действия международных соглашений в отношении киберпространства, их применимость по-прежнему проблематична.[11] Это связано с тем, что не существует международно признанного определения того, что мы называем кибератакой или кибероружием. Кроме того, при кибератаке обычно не происходит четкого объявления войны, злоумышленники остаются скрытыми в киберпространстве, а ожидаемые последствия также остаются неоцененными. Поэтому серьезное внимание уделяется применению соответствующих конвенций к операциям в киберпространстве.[12]

Инициатива «Парижский призыв к доверию и безопасности в киберпространстве» [13] была создана, чтобы гарантировать безопасность киберпространства на международном уровне. Венгрия присоединилась к инициативе, но крупнейшие владельцы кибер-арсенала (США, Израиль, Иран, Китай, Великобритания или Россия) не сочли это необходимым.

Киберзащита НАТО

Противодействие кибератакам является одним из основных приоритетов для НАТО. Однако в отношении обычно используемых терминов кибервойна или кибератака следует отметить, что в официальной терминологии НАТО нет согласованного определения кибервойны или кибератаки, а примеры определений можно найти только на уровне государств-членов.

В основном это связано с отсутствием границ в киберпространстве и постоянным расширением диапазона типов атак, которые оно допускает, а также с интересами Альянса. НАТО не считает определение понятия кибератаки необходимым, потому что оно индивидуально оценивает одновременные, но разные типы атак, чтобы принять решение о характере реакции на уровне альянса.

С 2007 года НАТО уделяет особое внимание киберзащите и кибервойне. В 2012 году киберзащита была включена в планирование обороны Североатлантического союза, а на саммите в Уэльсе в 2014 году были приняты ру-

---

[11] “Trends in International Law for Cyberspace,” NATO Cooperative Cyber Defense Centre of Excellence, May 2019, https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf.

[12] David P. Fidler, “The UN Secretary-General’s Call for Regulating Cyberwar Raises More Questions than Answers,” Council of Foreign Relations, March 15, 2018, www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers.

[13] Ministry for Europe and Foreign Affairs, “Cyber Security: Paris Call of 12 November 2018 for Trust and Security in the Cyber Space,” *France Diplomacy*, www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

ководящие принципы НАТО по киберзащите. В Уэльсе Североатлантический союз заявил, что признает действительность международного права в киберпространстве, и включил киберзащиту в число задач коллективной обороны НАТО.[14]

В 2016 году в коммюнике Варшавского саммита союзники расширили сферу боевых действий, традиционно охватывающих море, воздух и сушу, включив в нее киберпространство,[15] и заявили, что кибератака против государства-члена может рассматриваться Североатлантическим союзом как атака на НАТО в целом и, при необходимости, в ответ могут быть приняты коллективные меры.

В Варшаве было принято Обязательство по киберзащите, в соответствии с которым государства-члены предприняли существенное и быстрое развитие защиты своих национальных сетей и инфраструктур в соответствии со статьей 3 Вашингтонского договора, развитие всеобъемлющего потенциала киберзащиты и усиление сотрудничества в выявлении и понимании угроз при улучшении образования и обучения в области кибербезопасности. Важным шагом в развитии потенциала киберзащиты НАТО является создание, начиная с 2018 года, Оперативного киберцентра (СуОС) для координации кибероперациий Североатлантического союза в рамках Главного штаба союзных сил в Европе (SHAPE).

В своих киберспособностях НАТО различает пассивные и активные оборонные способности: первые состоят в основном из превентивных способностей, способностей для менеджмента инцидентов, для восстановления данных и систем в пределах своей собственной сети. Активные – это способности наступательного характера для сдерживания и устранения угроз, выходящих за рамки собственных сетей.[16]

Кибербезопасность в Венгерских силах обороны

В Венгрии защита от киберугроз и определение киберпространства как театра военных действий появилось в стратегических документах еще в 2012 году. В 2018 году киберпространство, как автономный театр военных действий, было включено в венгерское законодательство (раздел 80 Закона CXIII 2011 г.). Направления и условия развития венгерских военных киберспособностей изложены в Национальной военной стратегии (2012 г.), Национальной стратегии кибербезопасности (2013 г.), Концепции кибербезопас-

[14] "Wales Summit Declaration," *NATO e-Library*, September 5, 2014, articles 72 and 73, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[15] "Warsaw Summit Communiqué," *NATO e-Library*, March 29, 2017, articles 70 and 71, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[16] Susan Davis, "NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence," NATO Parliamentary Assembly, April 18, 2019, pp. 4-6, www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087_STC_19_E%20-%20NATO.pdf.

ности Венгерских сил обороны (2013 г.), вышеупомянутых Варшавских обязательствах, Программе развития Зриньи до 2026 года. В Венгрии защита от киберугроз и определение киберпространства как театра военных действий появилось в стратегических документах еще в 2012 году. В 2018 году киберпространство как автономный театр военных действий было включено в венгерское законодательство (раздел 80 Закона CXIII 2011 г.). Направления и условия развития венгерского военного киберпотенциала изложены в Национальной военной стратегии (2012 г.), Национальной стратегии кибербезопасности (2013 г.), Концепции кибербезопасности Венгерских сил обороны (2013 г.), вышеупомянутых Варшавских обязательствах, Программе развития Зриньи до 2026 года.

Национальная военная стратегия определила «создание способностей для сетевой войны» как одну из основных целей, которую должны достичь Силы обороны Венгрии. С одной стороны, компьютерно-сетевая война направлена на то, чтобы повлиять на работу сетевых ИТ-систем противной стороны, ухудшить их работоспособность и сделать невозможной работу, а с другой стороны, она направлена на поддержание функционирования наших собственных аналогичных систем.[17] График создания этих кибервозможностей был определен в Концепции кибербезопасности Венгерских сил обороны. В этом документе первоначальный уровень возможностей кибербезопасности должен быть достигнут до 2014 года, базовый уровень способностей для обеспечения кибербезопасности – в период с 2014 по 2016 год, а полные способности для кибербезопасности – после 2016 года. Концепция направлена, *среди прочего*, на защиту жизненно важных компонентов информационной системы, снижение их уязвимости и как можно более быстрое устранение потенциального ущерба.

Разработки в области кибербезопасности, инициированные Силами обороны Венгрии, составляют неотъемлемую часть программы оборонной политики. В рамках этой программы был создан Центр ВСО менеджмента электронных инцидентов. Кроме того, в Силах обороны Венгрии могут потребоваться дальнейшие организационные и функциональные изменения для создания единой системы кибербезопасности. С этой целью также следует уточнить тип организаций по кибербезопасности для отдельных командных уровней. Основная задача в области кибербезопасности – сократить время реакции и повысить эффективность разведки.

На сегодняшний день большинство задач по кибербезопасности Венгерских сил обороны выполняет Военная служба национальной безопасности

[17] По словам Хейга и Вархеги, «компьютерно-сетевая война включает в себя следующие действия: картирование структуры компьютерных сетей; изучение иерархических и операционных функций на основе характеристик их трафика; регистрация содержимого потока данных в сети; вводящая в заблуждение, подрывная деятельность в сетях; изменение и уничтожение содержания программ и данных целевых объектов, а также вопросы защиты от аналогичных действий противостоящей стороны».

(ВСНБ). В последние годы в исполнение Инструкции Минобороны № 85/2014 ВСНБ инвестировала в развитие разведывательных способностей и способностей, позволяющих осуществлять менеджмент киберинцидентов.

На парламентских слушаниях в 2019 году начальник Генерального штаба указал, что в ближайшем будущем предусматривается развитие киберспособностей (которых в то время не было). В 2020 году правительство определило области в рамках киберспособностей и операций Венгерских сил обороны, которые необходимо применять или развивать, а парламент добавил к Закону о национальной обороне особые правила, касающиеся военных операций в киберпространстве.[18]

Хотя подробности не являются полностью общедоступными, оборонный бюджет на 2020 год показывает, что киберразвитие вооруженных сил является основным приоритетом.

Сценарий гибридной атаки против Венгрии

Само собой разумеется, что за последние десять лет на национальном уровне был достигнут значительный прогресс в области киберзащиты и безопасности. Однако мы остаемся относительно беззащитными и уязвимыми для хорошо структурированной и скоординированной серии кибератак. По словам Фехера, эти атаки могут привести к

> наиболее опасному курсу действий врага, когда агрессор проводит гибридные операции полного спектра, и он может найти достаточно сторонников для борьбы с центральной властью, таким образом удерживая конфликт ниже порога статьи 5. При скрытой поддержке Сил специальных операций и конвенциональных сил противник может достичь фундаментальной внезапности, парализовать систему командования и управления, успешно бороться с венгерскими силами безопасности и установить функциональную альтернативную политическую власть на оккупированных территориях. В этой ситуации Венгрия вынуждена бороться без официальной помощи НАТО на оккупированных или неоккупированных территориях.[19]

Основываясь на этом предположении и тезисе д-ра Ласло Ковача и д-ра Чаба Краснаи о сценарии кибератаки против Венгрии, я хотел бы представить процесс эскалации, который вполне возможен сегодня (фиг. 2).

Результаты

10 декабря 2019 года Европейский совет принял заключения, устанавливающие приоритеты и руководящие принципы сотрудничества ЕС в противо-

[18] Prime Minister's Office, *T/8029th Bill proposal* (12 November 2019), 5, 21-22, https://www.parlament.hu/irom41/08029/08029.pdf.

[19] Feher, "Hungary's Alternative to Counter Hybrid Warfare."

действии гибридным угрозам и для повышения устойчивости к этим угрозам. В заключениях содержится призыв к применению комплексного подхода к противодействию гибридным угрозам, работающего во всех соответствующих секторах политики более стратегическим, скоординированным и согласованным образом.

В случае Венгрии контроль над ДИВЭ, поддерживающее и активно участвующее население, адекватная военная мощь, эффективная разведка и контрразведка, а также повышение киберустойчивости, по-видимому, являются соответствующими приоритетами, где устойчивость определяется как «способность подготовиться к изменяющимся условиям и адаптироваться к ним, противостоять сбоям и быстро восстанавливаться…, [и] включает способность противостоять преднамеренным атакам, авариям или естественным угрозам или инцидентам и восстанавливаться после них».[20]

Киберустойчивость – это способность субъекта противостоять, реагировать и восстанавливаться после киберинцидентов, обеспечивая непрерывность его работы.[21] Стратегические кибератаки могут быть нацелены на критически важную инфраструктуру и коммунальные предприятия страны, в то время как оперативные кибератаки направлены против вооруженных сил противника.

В то же время кибератаки – это тип информационных операций в рамках информационной войны, направленные на «коррумпирование, опровержение, деградацию и использование информации и информационных систем и процессов противника, одновременно защищая конфиденциальность, целостность и доступность своей собственной информации».[22]

Потенциал в информационной сфере жизненно важен для государства, чтобы подготовить граждан к негативному влиянию врага, сохранить или восстановить взаимодействие между государством и народом и положить конец ложному чувству безопасности граждан.

Согласно интерпретации НАТО, устойчивость на национальном уровне – это сочетание готовности гражданского населения и военного потенциала.[23] Это означает, что мы должны решать следующие задачи: повышение осведомленности общества в области информационной безопасности;

---

[20] “Resilience,” Glossary, NIST Information Technology Laboratory, Computer Security Resource Center (source: NIST SP 800-53 Rev. 4), https://csrc.nist.gov/glossary/term/resilience.

[21] Kjell Hausken, “Cyber Resilience in Firms, Organizations and Societies,” *Internet of Things* (2020), 100204, https://doi.org/10.1016/j.iot.2020.100204.

[22] Anil Chopra, “Cyber Warfare a Key Element of Multi Domain Wars – Time to Push India,” *Air Power Asia*, June 3, 2020, https://airpowerasia.com/2020/06/03/cyber-warfare-a-key-element-of-multi-domain-wars-time-to-push-india/

[23] Gustav Pétursson, “NATO’s Policy on Civil Resilience: Added Value for Small States?” SCANSE Research Project, Policy brief no. 5 (26 June 2018): 2, http://ams.hi.is/wp-content/uploads/2018/06/NATO%C2%B4s-Policy-on-Civil-Resilience-Added-Value-for-Small-States.pdf.

I.	Кибератака (первая фаза возможной гибридной атаки – кибератака)
I.1. Психологические операции	1. Запугивание: новости о предполагаемой слабости венгерской киберзащиты появляются в блоге, поддерживаемом иностранной секретной службой. 2. Распространение: новости, появившиеся в блоге, распространяются в социальных сетях, достигая десятки тысяч пользователей. 3. Обмен. Благодаря обмену через псевдопрофили, созданные иностранными разведывательными службами, новости появляются в большем потоке новостей и распространяются дальше. 4. Освещение: из-за большого количества публикаций бульварная пресса также начинает освещать эту тему, и вскоре она становится темой и в уважаемых СМИ.
I.2. Эффектные атаки	1. Проводятся атаки с перегрузкой против определенных правительственных веб-сайтов, в результате чего некоторые услуги становятся недоступными в течение нескольких часов. 2. Взламываются веб-сайты некоторых муниципальных ведомств и служб поддержки, и на их главных страницах появляются сообщения с угрозами Венгрии. 3. В Интернете появляются базы данных, содержащие персональные данные десятков тысяч граждан Венгрии.
I.3. Влияние на политику	1. В случае утечки типа Wikileaks электронные письма государственных органов публикуются под заголовком HunLeaks; международная пресса начинает их анализировать. 2. «Венгерский Сноуден» передает секретные документы расследующему журналисту. Их анализирует международная команда журналистов. 3. Расследование, заказанное в результате предыдущих атак, обнаруживает сложное вредоносное ПО в ИТ-системе поставщика общественных услуг. Целью вредоносного ПО является получение данных. Согласно отчету о расследовании, вредоносная программа работает не менее двух лет.
I.4. Инфраструктурные атаки	1. Атаки на телекоммуникации. Большинство телекоммуникационных услуг становятся недоступными. Государственные коммуникации также затруднены. Координация защиты замедляется и блокируется. 2. Атаки на финансовую систему: Интернет-банкинг приостановлен; международные финансовые операции также приостановлены.

	3. Нападения на электроснабжение и транспорт: происходят отключения электроэнергии на районном уровне; транспорт парализован.
II. Агрессор осуществляет полный спектр гибрид-ных операций	Агрессор проводит комбинацию специальных и конвенциональных военных операций, использует агентов разведки, политических провокаторов, влияние средств массовой информации, экономическое запугивание, доверенных и подставных лиц, военизированные формирования, террористов и криминальных элементов. Агрессор может добиться фундаментальной неожиданности, парализовать систему командования и управления, успешно бороться с венгерскими силами обороны и безопасности и установить функционирующую альтернативную политическую власть на оккупированных территориях. В этой ситуации Венгрия вынуждена бороться без официальной помощи НАТО на оккупированных или неоккупированных территориях.

	Развитие устойчивости на национальном уровне	Развитие устойчивости на уровне ВСО
I. Гибридная атака	Назначение национального координатора по вопросам устойчивости и гражданской готовности, определение национальных задач, органов и организаций ответственные за их выполнение и участвующие в их выполнении, а также процедуры сотрудничества. Администрация обороны кажется подходящей системой для обеспечения полного сотрудничества между государственными органами.	Реализация предложенного проекта (фигура 1), чтобы достичь желаемой цели (конечное состояние), защита страны за счет повышения устойчивости к гибридным атакам. На фигуре указаны инструменты национальной мощи для достижения каждого результата.
II. Кибератака	Повышение осведомленности об информационной безопасности в обществе, усиление организаций киберзащиты, создание альтернативных, аварийных инфраструктур, усиление набора инстру-	Основная задача ВСО – решать информационные проблемы комплексным образом: как быстро получать и обрабатывать информацию и интегрировать ее в цикл принятия решений, так и контролировать

	ментов для скоординированной централизованной киберзащиты, укрепление партнерских отношений между административной, деловой и научной сферами.	нарратив о конфликте в информационном пространстве. Необходимо создать оперативные способности в киберпространстве и их интеграцию в военное планирование и исполнение.

Фигура 2: Возможная гибридная атака на Венгрию и обеспечение устойчивости.

укрепление организаций киберзащиты, создание альтернативных, аварийных инфраструктур (элементов); усиление инструментария для скоординированной централизованной защиты; укрепление партнерства между административной, деловой и научной сферами; повышение устойчивости ВСО к гибридным атакам, включая кибератаки, путем выполнения предложений в этой статье.

Чтобы обеспечить устойчивость к киберугрозам, ВСО должны уметь решать информационные проблемы комплексным образом: как для быстрого получения и обработки информации, так и для интеграции ее в цикл принятия решений, а также для управления нарративами о конфликте в информационном пространстве.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Благодарность

Connections: The Quarterly Journal, Vol. 19, 2020, вышел при поддержке правительства США.

Об авторе

Андраш **Хугик**, доктор военных наук, полковник полиции в отставке, главный советник венгерской полиции. Он инженер, экономист, политолог. Он бывший советник ГУАМ, ОБСЕ, МППЕС и Совместного механизма расследований ООН и ОЗХО. Прежде чем присоединиться к этим международным организациям, он служил в военной разведке, службе внутренней безопасности венгерских правоохранительных органов и в контртеррористическом центре Венгрии. E-mail: seniorhugyik@gmail.com.