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

Людвиг Лайнхос, *Connections QJ* 19, № 1 (2020): 9-20
https://doi.org/10.11610/Connections.rus.19.1.02

Национальная политика кибербезопасности

Кибер оборона в Германии: вызовы и путь вперед для Бундесвера

Генерал-лейтенант Людвиг Лайнхос

Служба кибер операций и информационного обеспечения Бундесвера, Германия

Резюме: Сегодняшние конфликты во все большей степени протекают в гибридных формах, в том числе и в виде атак на технические сети и кампании, направленные на оказание влияния на общественное мнение. Бундесвер ответил на такое развитие ситуации путем объединения своих способностей в этой сфере, сочетая их в Службу кибер операций и информационного обеспечения. Наряду с классическими видами вооруженных сил – сухопутными, военно-воздушными и военно-морскими – эта служба, со своим личным составом численностью приблизительно в 14 500 человек, вносит существенный вклад в общегосударственное обеспечение безопасности.

Ключевые слова: кибер домен, кибер операции, критическая инфраструктура, гибридная угроза, совместный центр комплексирования, фьюжн центр.

Основные моменты политики в сфере кибербезопасности

В Германии обеспечение кибербезопасности – т.е. состояния, при котором риски, исходящие из киберпространства, сведены к приемлемому минимуму – является общегосударственной задачей. Это записано в Белой книге от 2016 года,[1] текущего основного документа, определяющего политику безопасности Германии. В очень небольшом числе областей внутренняя и

[1] "White Paper on German Security and the Bundeswehr," 2016, https://issat.dcaf.ch/download/111704/2027268/2016%20White%20Paper.pdf.

внешняя безопасность так же тесно переплетаются между собой, как в киберпространстве. Сюда входит и совместная защита критической инфраструктуры.

Тем не менее, даже при межведомственном подходе, существуют определенные сферы ответственности. Например, федеральное министерство внутренних дел отвечает за кибербезопасность и защиту гражданской инфраструктуры. Оно так же несет основную ответственность за стратегию Германии по вопросам кибербезопасности. Федеральное министерство иностранных дел формирует политику в сфере международной кибербезопасности, тогда как федеральное министерство обороны отвечает за кибероборону.

Чтобы проводить свои операции, Бундесвер в качестве военной организации, в частности зависит от наличности, конфиденциальности и надежности данных, от базированных на ИТ услугах и от сетевой инфраструктуры. По этой причине, стратегия кибероборонны Бундесвера делает особый упор на защиту дружественных систем. Важным инструментом для обеспечения этой защиты является комплексная, цифровая картина ситуации, которая охватывает информационное пространство и доступна для других государственных ведомств, как часть сетевого подхода. В информационном пространстве люди воспринимают, интерпретируют и распространяют информацию за рамками технической сферы. Существенным аспектом наших соображений является то, что называют «общественным мнением».

В дополнение к превентивным мерам, реактивные и активные меры (операции в кибер домене и в информационном домене) также стали необходимостью, когда речь идет о защите дружественных систем. Операции в киберпространстве и в информационном пространстве могут иметь форму как независимых, так и поддерживающих операций. В случае конфликта, они являются возможным вариантом для начальных операций, которые в случае необходимости могут осуществляться в период, когда конвенциональные силы еще не приведены в боевую готовность. Операции в кибердомене и в информационном пространстве подчиняются тем же юридическим ограничениям, что и остальные силы Бундесвера.

В дополнение к общегосударственному подходу, другим основным принципом кибероборонны Германии является мультинациональность – как и целостной политики Германии в сфере безопасности. Мы стремимся работать совместно с партнерами по ЕС и НАТО как на двухсторонней, так и на многосторонней основе, а также в рамках ООН для того, чтобы обеспечить кибербезопасность и создать соответствующую юридическую основу.

Вызовы перед политикой безопасности

Федеральное правительство Германии считает угрозы, исходящие из киберпространства и из информационного пространства одним из ключевых вызовов, с которыми сталкивается политика безопасности Германии. Дигита-

лизация проникла во все сферы жизни и наряду со все больше увеличивающейся взаимосвязанностью личностей, организаций и государств, предлагает уникальные возможности. В то же время, однако, она делает управление, общества и экономики особо уязвимыми.

После Варшавского саммита в 2016 году,[2] НАТО рассматривает киберпространство в качестве независимой сферы проведения операций – подобную сухопутному, воздушному, морскому и космическому пространству. В кибер пространстве, среди прочего, вооруженные силы могут использовать подходящее программное обеспечение для разведывания и последующего воздействия на системы противника. В практическом плане, это может означать прерывание логистических цепей, искажение данных, необходимых для ведения операций, или ограничение работоспособности ключевых систем командования и управления (К2) и информационных систем противника.

Включая не только электромагнитный спектр, но также и в особенности информационного пространства, Бундесвер намеренно дал более комплексное определение этой новой среды военных действий, чем НАТО. Действия в информационной среде, например кампании фальшивых новостей, продолжают расширяться, предоставляя возможность намеренно вызывать волнения населения. На международные и национальные конфликты во все в большей степени оказывает влияние пропаганда и дезинформация. Поэтому информация становится одним из ключевых ресурсов будущего.

Кибер и информационное пространство отличаются от классических сред ведения операций несколькими уникальными особенностями. Оно характеризуется высокой степенью сложности. Территориальность дополняется виртуальной реальностью. Кибер и информационный домен не может быть разделен на секторы боевых действий четкими пространственными границами. То же самое относится и к маневрированию силами. Тем не менее, в кибер и информационном пространстве могут быть реализованы физические результаты. Место, в котором операции в кибер и информационной среде дают результаты, однако, может быть в десятках тысячах километрах от места, в котором были инициированы действия. Время тоже играет другую роль, учитывая, что результаты в киберпространстве могут быть достигнуты на любом расстоянии без запаздывания. При соответствующей подготовке, результаты могут быть реализованы почти в реальном времени.

Проблемой является и атрибуция атак. Благодаря технологическим возможностям, такие действия могут быть замаскированы очень хорошо. Кроме того, существует большое количество групп возможных авторов нападений и большое число возможных мотивов. К настоящему моменту,

[2] "NATO Warsaw Summit Communique," July 2016, paras 70-71, www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber.

дигитализация дала возможность негосударственным акторам добиваться с помощью кибератак результатов, которые до этого были под силу только государственным игрокам.

В итоге можно сказать, что сегодняшние конфликты в наибольшей степени характеризуются своей гибридной природой. Нападения в киберпространстве и дезинформационные кампании, которые остаются ниже порога вооруженного нападения, необходимо брать в расчет также, как и массированное использование кибероперации в качестве существенной составной сценария национальной и коллективной обороны. Поэтому, существенное значение имеет четкий анализ, дающий информативную картину ситуации.

В качестве Руководителя Службы кибероперации и информационного обслуживания я считаю, что моя ответственность не ограничивается до минимизации упомянутых выше рисков. Для Бундесвера дигитализация дает огромные возможности, которые буду рассмотрены ниже.

Структуры для реализации политики и общегосударственный контекст

Возможные угрозы для государственного управления, для экономики и для общества многогранны и включают кражу данных, шпионаж, нанесение урона критической инфраструктуре, нарушение государственных коммуникаций, и они разнообразны, как и ведомства, которые занимаются ими. Часто для использования слабостей интерфейса между сферами ответственности, например между внутренней и внешней безопасностью, применяются гибридные стратегии.

Поэтому, сплочение рядов и создание системы обмена на национальном уровне являются абсолютной необходимостью. На стратегическом уровне архитектуры государственной кибербезопасности, ответственность за координацию сотрудничества в рамках федерального правительства, а также между государственным управлением и бизнесом, лежит на Национальном совете по кибербезопасности. На оперативном уровне, еще в 2011 году под эгидой Федерального управления по информационной безопасности, которое подчиняется Федеральному министерству внутренних дел, был учрежден Национальный центр киберреагирования, являющийся форумом для содействия сотрудничеству между государственными ведомствами в кибер и информационной сфере. В сотрудничестве со всеми ключевыми игроками, Национальный центр киберреагирования претерпевает дальнейшую адаптацию к статусу межведомственной институции оперативного уровня. Это является важным шагом к созданию более эффективных структур для обеспечения будущей способности Германии действовать в данной сфере. И здесь незаменимым является участие национальных интернет провайдеров. В качестве представителя Бундесвера, Служба кибероперации и информационного обслуживания активно способствует этому процессу. Когда адаптация Национального центра киберреагирования будет закончена,

его можно будет использовать для распространения информации, предоставляемой Объединенным кибер-информационным (фьюжн) центром комплексирования.

Чтобы существенно повысить кибербезопасность в Германии еще на этапе разработки ключевых технологий, с конца 2018 года Федеральное министерство обороны и Федеральное министерство внутренних дел начали работать совместно над созданием Агентства инноваций в сфере кибербезопасности. Это агентство будет распределять целевые контракты для выполнения амбициозных исследовательских проектов с высоким новаторским потенциалом. Таким образом, оно сможет прокладывать новые пути для сохранения ведущей роли Германии в технологических инновациях.

Центр кибер инноваций дает Федеральному министерству обороны свой собственный интерфейс между стартап компаниями и Бундесвером.

Федеральное управление информационной безопасности обеспечивает поддержку таким государственным институциям, как германский Бундестаг, по проблемам информационной безопасности. В случае необходимости, оно как можно быстрее распределяет команды реагирования на чрезвычайные компьютерные ситуации для восстановления информационной безопасности. Для Бундесвера эта задача выполняется Службой кибероперациий и информационного обеспечения.

Атрибуция – т.е. идентификация исполнителей – кибернападений входит в сферу ответственности правоохранительных органов и разведывательных служб.

Если Бундесвер сам по себе не является объектом кибератаки, Конституция Германии ограничивает его роль до оказания административного содействия и поддержки в случаях особенно тяжелых инцидентов. Это, однако, не означает, что серьезные нападения на критическую инфраструктуру не могут привести к военному ответу в контексте национальной и коллективной обороны.

Реализация политики

Защита & операции, разведка & воздействия, геопространственная информация

Бундесвер плотно занимается вопросом информационной безопасности с 1990-х. Более 20 лет Бундесвер поддерживает свою собственную организацию по обеспечению ИТ безопасности, которая в настоящее время превращается в комплексную организацию, занимающуюся информационной безопасностью с особым упором на повышение бдительности при использовании ИТ оборудования членами Бундесвера. В ответ на последствия расширяющейся дигитализации, в апреле 2017 была введена в действие новая Служба кибероперациий и информационного обеспечения Германии. Эта основная организационная структура в настоящее время имеет военный и

гражданский личный состав приблизительной численности в 14 500 человек. В ней собраны уже существующие подразделения с соответствующим опытом и расширенной компетентностью.

Спектр задач этого основного организационного компонента очень разнообразен. Одним из фокусов его деятельности является защита и функционирование ИТ системы Бундесвера, как дома, так и в заграничных операциях. Его способности не ограничены до создания требуемых линий связи; он также располагает ситуационными центрами, которые круглосуточно осуществляют мониторинг ИТ систем. Там выявляются и, если необходимо, сдерживаются кибератаки. Кроме того, прежде чем какие-либо ИТ системы или системы с ИТ компонентами будут введены в действие в Бундесвере, они испытываются и получают аккредитацию центрального ведомства на предмет информационной безопасности.

Общая ответственность за информационную безопасность в Бундесвере лежит на Главном офицере по информационной безопасности (ГОИББВ), который также является моим заместителем в качестве Заместителя начальника Службы кибероперациий и информационного обеспечения.

Усиливаются и дальше развиваются способности для ведения разведки и осуществления воздействия в кибер и информационном пространстве. В это входят кибероперации, например инфильтрация в ИТ сети противника и выявление уязвимостей в союзных системах. Ценные разведывательные результаты предоставляет военная разведка, например, радиолокационные изображения, соответствующие определенным требованиям, или изображения высокого разрешения для защиты своих и союзных сил. В число способностей Службы кибероперациий и информационного обеспечения входят средства для ведения электронной войны и осуществления оперативной коммуникации. Оперативная коммуникация занимается такими факторами информации и восприятия, как: что люди на театре военных действий говорят о военных операциях? Имеется ли в обращении ложная информация о Бундесвере? Когда есть ответ на эти вопросы, можно предпринимать контрмеры, если это необходимо.

Сотрудники Геоинформационной службы оказывают содействие всем подразделениям Бундесвера при осуществлении их миссий, предоставляя разнообразную цифровую и аналоговую геопространственную информацию высокого разрешения и с гарантированным качеством.

Объединенный кибер-информационный (фьюжн) центр комплексирования

Сложность киберпространства и информационного пространства делает надежный анализ незаменимым. По этой причине, Служба кибероперациий и информационного обеспечения создала свой собственный ситуационный центр для кибер-информационного домена. Путем комплексирования существующих (частичных) картин всех функциональных областей, имеющих

отношение к кибер-информационной сфере, Объединенный кибер-информационный фьюжн центр создает картину реальной ситуации, которая является основой для выбора возможных курсов действий и использования синергетических эффектов. Аналитики обрабатывают разные типы данных – как структурированные, так и неструктурированные – из разных источников; в будущем они будут использовать также методы искусственного интеллекта и методы обработки больших массивов данных. Например, коррелируя данные ИТ систем Бундесвера с другой информацией военной разведки, а также с информацией из открытых источников в социальных сетях, можно выявить надвигающуюся гибридную угрозу или скоординированную кибератаку. Проведенный таким образом анализ затем можно предоставлять потребителям в Бундесвере и в других государственных ведомствах.

Опыт разработки программного обеспечения в Бундесвере

Служба кибероперацій и информационного обеспечения Бундесвера способна разрабатывать свое собственное программное обеспечение или адаптировать коммерчески доступные программные продукты к требованиям Бундесвера или НАТО. С 1 апреля 2019 года эти способности были собраны и продолжают развиваться в Центре экспертизы в сфере программного обеспечения Бундесвера. Возможности, которые предоставляет такой центр, трудно переоценить. Это позволяет нам дать решающий вклад в дигитализацию Бундесвера – от экипировки спецназа и боевых постов до центров данных Бундесвера. Замечательным примером – одним из многих – является гармонизация К2 информационных систем. Бундесвер гармонизировал существующие К2 информационные системы вооруженных сил, приспособив их к специфике служб. Этот проект, а также последующие проекты, которые надстраивали его результаты, например Информационная сеть военных миссий Германии, позволит Бундесверу обеспечивать большинство необходимых ему для миссий ИТ из центров данных через «частное облако Бундесвера», и для связанных с миссиями и учениями задачами, через «облако миссий». Критически важный вклад в эту сферу делает Центр экспертизы в сфере программного обеспечения Бундесвера.

Запрягая Искусственный интеллект

Работа Центра экспертизы в сфере программного обеспечения Бундесвера уже сделала очевидным, что Служба кибероперацій и информационного обслуживания придает большое значение использованию возможностей, предоставляемые цифровизацией. Это также относится и к использованию искусственного интеллекта (ИИ). Для цифровизации ИИ является квантовым скачком – также, как сборочный конвейер для индустриализации. Слабый ИИ, который в отличие от сильного ИИ, ограничен до решения конкретных проблем пользователя, – станет интегральной частью нашей ежедневной жизни, средством, которое будет помогать нам круглосуточно. У этой технологии имеется огромный потенциал, в частности, когда речь идет о струк-

турировании большого количества данных, поскольку как некий металлоискатель, ИИ может найти пресловутую иголку в стоге сена большого массива данных.

Военное применение, к примеру, эта технология может найти при раннем выявлении кризисов. Для этой цели Федеральное министерство обороны с 2017 года разрабатывает в сотрудничестве с индустрией проект ИИ поддержки для раннего обнаружения кризисов. В число участников проекта входит Университет Бундесвера в Мюнхене. Вышеупомянутый Объединенный кибер-информационный центр комплексирования Службы кибероперацийи информационного обеспечения в будущем также будет использовать инструменты ИИ для того, чтобы ускорить принятие решений и поставить его на солидной основе. Здесь становятся очевидными огромные преимущества ИИ. Он освобождает аналитиков от рутинной работы, так что они могут сосредоточиться на том, что не могут делать машины, т.е. на выводах и на оценке вариантов действий. Здесь мы касаемся вопроса, который я считаю исключительно важным. Решение, что делать с информацией, должно и всегда будет приниматься человеческими существами.

В сферах подготовки, технического обслуживания и логистики в Бундесвере, ИИ в будущем также принесет существенные улучшения. К примеру, Сухопутные силы в настоящее время изучают возможные применения ИИ и технологий машинного обучения и реализуют их в пилотных проектах. Военно-воздушные силы изучают потенциал использования ИИ в процессе планирования Воздушного командования и управления (Воздушный К2) и использование ИИ в планировании миссий. В медицинской сфере, анализ изображений уже массово используется в диагностике.

Однако, не только Бундесвер понимает военный потенциал ИИ; другие страны тоже расширяют исследования в этом направлении. Таким образом, использование ИИ в военных целях становится вопросом стратегической важности.

Цифровые сети на поле боя

Мой структурный элемент отвечает за работу, использование, защиту и дальнейшее развитие ИТ системы Бундесвера. Эта ответственность охватывает весь спектр от коммуникационного офис оборудования, доставка которого находится в руках являющейся федеральной собственностью компании BWI, до систем интерфейса оружейных систем Бундесвера – от системы самолетов Eurofighter до бордовых операционных центров Военно-морского флота и планшетного компьютера солдата пехоты на поле боя. Моя задача состоит в том, чтобы предоставить вооруженным силам требуемые ИТ услуги эффективным и надежным способом. Здесь особое внимание уделяется общей схеме системы, чтобы обеспечить беспрепятственные передачи и оперативную совместимость как в плане вооруженных сил Германии, так и в отношении таких внешних партнеров, как союзные вооруженные силы или другие государственные ведомства.

Служба кибербезопасности и информационного обеспечения играет ключевую роль в цифровизации вооруженных сил: она функционирует как центральный орган вооруженных сил по ИТ проектам. Программа цифровизации сухопутных операций (ЦСО) является замечательным примером ее деятельности. Этот проект направлен не только на замену старых систем радиокоммуникации SEM и TETRAPOL, основанными на IP-протоколе услугами, но и на реализацию цифровой взаимосвязи всех военнослужащих и средств на поле боя в качестве частей мобильной и универсальной, национальной и мультинациональной оперативно совместимой сети. Мы намереваемся обеспечить ее работоспособность в национальных и даже в коллективных оборонных операциях, которые характеризуются частыми перебазированиями и мобильным ведением боевых действий. Модернизация ИТ оборудования десятков тысяч транспортных средств и личного состава является грандиозным проектом, который потребует для осуществления несколько лет. Программа ЦСО является ключом к модернизации системы обеспечения мобильной информации в ходе операций.

Мультинациональный и общегосударственный подход

Мультинациональность уже была упомянута в качестве важного руководящего принципа. Она касается сетевой работы как систем и игроков разных уровней командования на поле боя, так и в очень практическом плане многочисленных учений в рамках НАТО, ЕС и на двусторонней основе. В 2019 году Служба кибербезопасности и информационного обеспечения приняла участие в самом большом в мире международном учении по киберзащите в реальных условиях, учении НАТО *Сдвинутые щиты*. Эксперты Бундесвера по компьютерной криминалистике были в четвертый очередной раз признаны лучшей командой в своей категории.

На военно-стратегическом уровне мы также поддерживаем тесные контакты с нашими партнерами. Поэтому, только на втором году нашего существования нам на год поверили председательство Форума кибер-командующих. Этот орган регулярно собирает кибер-командующих нескольких стран-членов и не-членов НАТО с целью укреплять мультинациональное сотрудничество.

Кроме того, благодаря нашему сотрудничеству с другими национальными институциями, Служба кибербезопасности и информационного обслуживания также дает свой вклад в национальную безопасность и укрепляет архитектуру кибербезопасности Германии. К примеру, у нас сложилось тесное сотрудничество с другими ведомствами из сферы безопасности, как например Федеральным управлением информационной безопасности. По нашему мнению, превращение Национального центра киберреагирования, который подчиняется Службе кибербезопасности и информационного обслуживания, в межведомственную институцию оперативного уровня является важным для способности Германии действовать адекватно в будущем.

Также, мы достигли согласия по первым проектам сотрудничества с деловым сектором и сектором науки, к примеру, с Телекоммуникационной

компанией Германии, с Институтом Фраунгофера связи, обработки информации и эргономики (FKIE) и – наше установленное в самое последнее время сотрудничество, с мая 2019 – с Bitkom, ведущей ассоциацией Германии по информационным технологиям, телекоммуникациям и новым СМИ. На региональном уровне, Служба кибербезопасности и информационного обслуживания является частью Боннского кластера по кибербезопасности, поддерживая связи с компаниями в сфере бизнеса, с образовательными институциями и государственными ведомствами для обмена информацией и передовым опытом. Мы осуществляем это, например, через взаимные стажировки или организацию и поддержку мер по практическому обучению.

Личный состав и материальное обеспечение

Адекватно квалифицированный и мотивированный личный состав во все большей степени становится стратегическим ресурсом. Как и многие организации и компании, Бундесвер сталкивается с проблемой привлечения молодых талантов в сфере кибер и информационных технологий. Из разговоров с потенциальными будущими сотрудниками, мы поняли, что Бундесвер, с его специфическим портфолио задач, определенно является привлекательным работодателем для этой целевой группы. Мы используем это преимущество и предлагаем соответствующие стимулы, например, предоставляя нашим сотрудникам возможности для образования и повышения квалификации. В январе 2018 года, в Университете Бундесвера в Мюнхене была введена международная программа получения степени магистра в области кибербезопасности, которая является уникальной для Германии.

В качестве Начальника Службы кибербезопасности и информационного обслуживания, я выполняю те же функции, что и командующие других видов вооруженных сил, когда речь идет о выработке требований к персоналу для карьерных дорожек, находящихся в сфере моей ответственности, т.е. кибер и информационные технологии, военная разведка, оперативные коммуникации и геоинформационные системы. Это означает, что на мне лежит основная ответственность за формирование этих преимущественно технических карьерных путей. Для этих карьерных полей мы установим целостный подход к вопросам личного состава, подходящий для всех основных организационных сфер и, таким образом, улучшим существующий спектр индивидуальных профессиональных перспектив.

В настоящее время мы также расширяем возможности для более полного учета неформальной кибер и ИТ квалификации потенциальных сотрудников, что позволит нам делать привлекательные предложения таким кандидатам. Кроме того, мы отметили существенный прогресс в вопросе усиления персонала резервистами и сотрудниками, приходящими со стороны. При наличии 800 человек, заинтересованных работой в кибер резерве и более 1400 пользователей платформы кибер сообщества, виртуального форума Бундесвера, у Службы кибербезопасности и информационного обслуживания нет проблем с использованием внешнего опыта. Далее, мы со-

здаем разные гибкие возможности для работы и финансового стимулирования, например, в виде выплаты премий срочно необходимым ИТ специалистам.

Что касается вопросов материального обеспечения, мне хотелось бы и далее улучшать процессы приобретения и поддержки. С учетом ускоренных циклов развития в кибер и ИТ сфере, это единственный способ обеспечить соответствующее оборудование и его поддержку. В сфере обороны уже существуют многочисленные проекты, способствующие модернизации К2 способностям Бундесвера. Выше я уже обрисовал в деталях, как Служба кибербезопасности и информационного обслуживания способствует этому путем цифровизации сухопутных систем.

Международное право

В целом, использование военных киберспособностей подчиняется тем же ограничениям в соответствие с международным и конституционным правом, что относятся к любым другим операциям вооруженных сил Германии. На международном уровне существуют вполне определенные, но юридически не обязательные регуляции о том, как применять существующее международное право к кибероперациям, Таллиннское руководство 2.0.[3] Эти юридические и этические основы должны учитываться при предпринятии любых мер в кибер и информационном пространстве. Итак, хотя основания правовой безопасности установлены, в этой области надо сделать еще многое. Действительно, это бесспорно, – и теперь достигнут консенсус, – что обязывающие международные правила, применяемые к вооруженным конфликтам между государствами, применимы и к кибер и информационной сфере. Поэтому, чтобы дать возможность осуществлять быстрый ответ на атаки, если это необходимо, вопрос о том, как эти правила должны применяться к этой новой сфере, следует рассмотреть во всех подробностях.

Дорога вперед

Вызовы в киберсфере и в информационной сфере, которые были обозначены выше, будут усиливаться как в качественном, так и в количественном отношении. Поэтому адекватная защита является жизненно важной для государства, для экономики и для общества. В Германии это воспринимается как национальная задача, которую следует решать совместно с международными партнерами.

Так видит себя и самый новый организационный элемент структуры Бундесвера. Служба кибербезопасности и информационного обслуживания отвечает за ИТ системы Бундесвера, за разведку, воздействия и геоинформацию. В рутинной работе, операциях и на учениях Служба тесно сотрудничает с другими частями Бундесвера, с союзными вооруженными силами и другими государственными властями.

---

[3] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

Что касается цифровизации в Бундесвере, важно не только перечислять риски, но и использовать органически присущие этому процессу возможности. Это, в основном, относится к техническим аспектам. В то же время, однако, когда речь идет об операциях в кибер и информационном пространстве, необходимо новое мышление. Операции в кибер и информационном пространстве являются независимой средой операций, и они обеспечивают поддержку сухопутных, воздушных и морских миссий в рамках конвенциональных военных операций. Поэтому, чтобы предоставить политикам некинетические варианты действий, такие способности должны быть развернуты по всему спектру операций в кибер и информационном домене.

Государство должно поддерживать свою способность действовать и обеспечивать защиту людей и предоставления основных услуг. В этом способности Бундесвера в кибер и информационном домене могут быть существенным вкладом.

Отказ от ответственности

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

Об авторе

Генерал-лейтенант Людвиг Лайнхос поступил на службу в Бундесвер в 1975 году в качестве офицерского кандидата для Военно-воздушных сил. После обучения по специальности «Электротехника» и получения квалификации дипломированного инженера в Университете Бундесвера в Мюнхене, он прошел подготовку и работал на должностях в области электронной борьбы. С 1988 по 1990 он учился на курсах для штабных офицеров в командно-штабном колледже Бундесвера в Гамбурге.

Его дальнейшая военная карьера отмечена разными назначениями на штабных и командных должностях в Германии и за границей в областях систем командования и управления, электронной разведки, а также планирования и использования ИТ. В качестве генерального менеджера Агентства НАТО по управлению программой воздушного дальнего радиолокационного обнаружения и управления (НАПМА), он отвечал за менеджмент программы организации флота ДРЛоУ НАТО. С 2013 по 2016 он курировал вопросы кибероборонs и стандартизации в сфере ИТ, в том числе и в качестве Директора управления К3 в штаб-квартире НАТО в Брюсселе.

После 2016 года генерал-лейтенант Лайнхос в качестве директора управления по активации Службы кибероперaций и информационного обслуживания Германии задавал курс развития новой службы Бундесвера, и 1 апреля 2017 года стал первым начальником Службы кибероперaций и информационного обслуживания Германии.

Признательность

Том 19 журнала *Connections: The Quarterly Journal* публикуется при поддержке правительства Соединенных Штатов Америки.