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

Яаак Тариен, *Connections QJ* 19, № 1 (2020): 5-7
https://doi.org/10.11610/Connections.rus.19.1.01

Основные моменты политики кибербезопасности

Национальная политика киберзащиты и роль международного сотрудничества

Полковник Яаак Тариен

Директор Центра передового опыта в области совместной киберзащиты НАТО, https://ccdcoe.org/

Дигитализация сделала наши общества уязвимыми к кибер угрозам – от электрических сетей до выборов. То же относится и к вооруженным силам, и киберзащита стала естественной задачей всех организаций, связанных с обороной. Кибер угрозы уже нельзя считать новыми угрозами. Однако, ландшафт кибер угроз меняется быстро, и продолжит меняться быстро и в будущем. Зловредные вирусы, хакеры, взломы и тому подобное все еще являются частями этого ландшафта, но основными проблемами безопасности сейчас являются кибер оружия и кибератаки, происходящие от национальных государств. Злонамеренные игроки учатся быстро друг у друга, и их инструменты быстро распространяются. Как нам следует реагировать на это? Создание более безопасного киберпространства возможно только через сотрудничество. Поскольку в киберпространстве не существует традиционных границ, союзники и партнеры НАТО несут одни и те же ответственности, и имеют одни и те же возможности.

Сотрудничество в сфере кибер обороны, как это очевидно следует из наименования, было основным мотивом для учреждения в 2008 году шестью странами-членами НАТО Центра передового опыта НАТО по совместной кибер обороне (ЦПО СКО НАТО). К сегодняшнему дню, Центр обеспечивается персоналом и финансированием в общей сложности 25 странами. Государствами с полноправным участием в ЦПО СКО НАТО являются Бельгия, Болгария, Чешская Республика, Дания, Эстония, Франция, Германия, Греция, Венгрия, Италия, Латвия, Литва, Нидерланды, Норвегия, Польша, Португалия, Румыния, Словакия, Испания, Турция, Объединенное Королев-

ство и Соединенные Штаты. Австрия, Финляндия и Швеция являются участниками, осуществляющими взносы, статус, который предоставляется странам не-членам НАТО. Центр продолжает привлекать новых членов: в процессе присоединения находятся Япония, Хорватия, Черногория, Словения и Швейцария. Кроме того, о своем намерении присоединиться к Центру заявили Канада, Люксембург и Австралия.

ЦПО СКО НАТО, предназначенный для ведения исследований, подготовки и тренировок, предлагает своим странам-членам разные курсы подготовки на техническом, оперативном и стратегическом уровне. Кроме того, подготовлен курс по Международному праву, применимому к кибер операциям для юрисконсультов. Центр ежегодно проводит учение «красные против синих»: *Сдвинутые щиты* для экспертов по кибербезопасности с целью развития их умений по защите национальных ИТ систем и критической инфраструктуры от атак в реальном времени. *Сдвинутые щиты* также включают стратегический элемент, который касается процесса принятия решения, юридических и коммуникационных аспектов. В учении *Сдвинутые щиты* в 2019 году приняли участие более 1 500 экспертов из 30 стран. *Скрещенные мечи*, другое ежегодное учение, является техническим кибер учением, которое играется одной (красной) стороной, и которое ориентировано на повышение подготовки тестеров проникновения, экспертов по цифровой криминалистике и по ситуационной осведомленности. Ежегодная конференция КиКон – Международная конференция по кибер конфликту – является вкладом Центра в работу более всеохватного сообщества по кибер безопасности. КиКон способствует исследованиям и разработкам по техническим, юридическим, концептуальным, стратегическим и военным аспектам кибер обороны и кибер безопасности. Одним из международно признанных достижений Центра стало «Таллиннское руководство 2.0 по международному праву, применимому к кибер операциям».[1] Таллиннское руководство 2.0 является наиболее комплексным анализом того, как существующее международное право применяется к киберпространству. И наконец, с 2018 года Центр отвечает за идентификацию и координирование решений по образованию и подготовке в сфере кибер обороны для всех структур НАТО. Поскольку ядром Центра является его международный личный состав, кибер эксперты с разнообразным опытом, то наши практические результаты являются практическим подтверждением ценности и полезности международного сотрудничества.

Значение киберпространства для наших обществ и экономик будет и дальше увеличиваться. Киберпространство постоянно трансформируется – связывая все большее число людей и устройств, новые технологии позволяют реализацию новых функциональностей. Но будущее киберпростран-

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

ства находится в наших руках. Рост и развитие возможны только, если обеспечены надежность и безопасность киберпространства и в киберпространстве. Это означает, что наши национальные подходы, стратегии и законы требуют постоянного пересмотра и адаптации. Киберпространство остается вызовом для всех государств по отдельности и вызовом в глобальном масштабе. Предстоят дискуссии о ролях и ответственности разных государственных институций, в том числе и вооруженных сил, дискуссии о том, как наилучшим образом реагировать на этот вызов.

В этом номере «Connections» представлены опыт Австрии, Германии, Израиля, Швейцарии, Объединенного Королевства и США, который может быть полезным другим странам.

Достижение наиболее амбициозной цели – более надежное и безопасное киберпространство в целом – возможно только через международное сотрудничество. Существенную роль в этом играют НАТО, ЕС и другие организации. Да, международное сотрудничество в сфере кибер безопасности является чувствительным и сложным вопросом, и существуют определенные ограничения. Однако, насущной основой для такого сотрудничества являются доверие и способность учиться друг у друга. Если мы добьемся успеха в этом, дверь к дальнейшему сотрудничеству будет открыта. Данный номер журнала «Connections» является еще одним шагом к более широкому открытию этой двери.

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.

Об авторе

Полковник Яаак Тариен с сентября 2018 года является директором Центра передового опыта в области совместной кибер обороны НАТО, находящегося в Эстонии. До поступления в Центр, с августа 2012 по июль 2018, полковник Тариен служил в качестве командующего Военно-воздушных сил Эстонии. Среди прочих назначений, он также занимал должности офицера штаба Верховного союзного командования НАТО по трансформации (СКТ), заместителя Директора Регионального координационного центра наблюдения за воздушным пространством и командира эстонской группы в составе Регионального координационного центра наблюдения за воздушным пространством БАЛТНЕТ в Литве. Полковник Тариен, выпускник Военно-воздушной академии США, получил степень магистра в Командно-штабном колледже Воздушного университета ВВС США. Недавно он так же получил степень магистра в области стратегии управления национальными ресурсами в Университете национальной обороны США.

Признательность

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