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

Лиор Табански, *Connections QJ* 19, № 1 (2020): 51-71
https://doi.org/10.11610/Connections.rus.19.1.05

Национальная политика кибербезопасности

Армия обороны Израиля и национальная кибер оборона

Лиор Табански

Интердисциплинарный исследовательский кибер центра Блаватника, Университет Тель-Авива

Резюме: Кибербезопасность сама по себе не особо новая проблема. Современные возможности использовать уязвимости, однако, делают ее полем вызовов. Это нормально, что соперники используют все новосозданные возможности. Конфликт, в котором отношения противников имеют кибер измерение здесь, чтобы остаться. Соответственно, общества должны создать подходящую организацию для своей защиты от преднамеренных угроз. В этой статье рассматривается подход Израиля, обрисовываются корни и эволюция национальной кибер обороны, преобладающие угрозы, доктринальные вызовы и роль, которую играют виды вооруженных сил в кибер обороне.

Ключевые слова: Кибербезопасность, кибер оборона, стратегия, доктрина, кибер операции, роль Армии обороны Израиля.

Майкл Уорнер, историк Кибер командования Министерства обороны США, очерчивает основные теоретические постановки для субъектов, формирующих политику и для официальных лиц США: компьютеры могут допускать утечку конфиденциальных данных и потому их надо защищать (1960-е); компьютеры могут подвергаться атакам и возможна кража данных (1970-е); мы можем встроить компьютерные атаки в военные арсеналы (1980-е и 1990-е); другие могут делать то же самое с нами – и возможно, уже делают (1990-е).[1] Но новые возможности для использования уязвимостей делают

[1] Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 781-799, https://doi.org/10.1080/02684527.2012.7085.

это сферой вызовов. Это нормально, что соперники используют все ново созданные возможности. Кибер конфликт, означающий, что отношения противников имеют кибер измерения, пришел сюда, чтобы остаться.[2] Соответственно, общества должны придумать и создать подходящие организации для своей защиты от (преднамеренных) угроз. В этой статье сделан обзор корней, угроз и вызовов национальной кибер обороны Израиля.

Стратегия национальной безопасности Израиля и текущая стратегическая среда

Ядро доктрины безопасности Израиля всегда включало:

- Абсолютное численное меньшинство[3]
- Острая нехватка стратегической глубины[4]
- Постоянная региональная нестабильность
- Затянувшийся или неразрешимый арабо-израильский конфликт
- Опора на свои силы в обороне.

С 1990-х по 2010-е израильский стратегический ландшафт сдвинулся от угроз, исходящих от арабских вооруженных сил к угрозам, имевшим корни в нерегулярных или полурегулярных суб-государственных организациях, поддерживаемых Ираном. Иран, который не арабское государство и не сосед Израиля, является потенциальной ядерной проблемой высшей степени и требует отдельного отношения. В отличие от государств, такие организа-

---

2 Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA/London: The University of Georgia Press, 2011).

3 Общее население арабских государств исчисляется миллионами, тогда как Израиль остается на несколько порядков менее многочисленным. В 2017 году Израиль был домом для чуть более 6,5 миллионов евреев по сравнению с около 400 миллионов жителей стран-членов Арабской лиги – и более трети их проживают в странах, граничащих с Израилем.

4 Yaakov Amidror, "The Evolution and Development of the IDF," in *Routledge Handbook on Israeli Security*, ed. Stuart A. Cohen and Aharon Klieman (Routledge, 2018): «С момента своего появления Государству Израиль (и до этого, предтече Израиля Еврейскому Ишуву) приходилось стоять перед лицом экзистенциальной угрозы безопасности – узкого территориального субъекта, опирающегося на Средиземное море, окруженное со всех сторон арабскими врагами, жаждущими его исчезновения. Расстояние от Средиземного моря на Востоке до горной области, нависающей над и доминирующей побережье – известной, как «Западный берег» и населенной преобладающе палестинскими арабами – всего 12 км в самой узкой части (от Нетаньи до Тулкарма); и от Тель-Авива всего в 25 километрах (16 милях) в самой широкой части. Даже если добавить Западный берег к уравнению, самая большое расстояние в ширину страны меньше 60 километров. Израильский экономический, финансовый, технологический и демографический центр сконцентрирован вдоль средиземноморского побережья в узкой полосе длиной всего 100 км между Хайфой и Ашдодом».

ции, как Хезболла, Исламский джихад или Хамас основываются на радикальной исламистской идеологии, отказывая Израилю в праве на существование. Их доктрина сопротивления – *Мукавама* – уверяет своих последователей, что долгая, историческая, сейчас трудная борьба против Израиля в конце концов закончится победой, несмотря на временные препятствия.[5] Организации Хезболла, Исламский джихад или Хамас обещают и заявляют достижение успеха своей аудитории, тогда как арабские государства не смогли победить Израиль. Тем не менее, Израиль односторонним образом вывел свои силы из Южного Ливана в мае 2000, отошел от главных центров палестинского населения на Западном берегу после соглашений из Осло и снова в 2002, и эвакуировал свое гражданское и военное присутствие в Секторе Газа в августе 2005.

Де-факто стратегия безопасности Израиля сейчас стоит на четырех столбах:

I. Раннее предупреждение
II. Решительная победа на поле боя
III. Сдерживание (кумулятивное, не абсолютное)
IV. Оборона тылового «домашнего фронта».

Четвертый – оборона – был добавлен постепенно после уроков иракских ударов баллистическими ракетами 1991 года, палестинского терроризма и массированной ракетной угрозы со стороны Ливана и Сектора Газа. Поддерживаемые Ираном, Хезболла *и* Хамас развернули большую огневую мощь в размере 120 000 ракет, направленных на города Израиля. Иран содействует модернизации их в общем ближнего действия, малой точности арсенала, предоставлением высокоточных ракет средней дальности. Израильский оперативный театр боевых действий стер любые существенные отличия между военным фронтом и гражданским тылом. Армия обороны Израиля (АОИ) во все большей степени инвестирует в приобретение самых последних технологий, чтобы найти способы защитить свой «внутренний фронт». АОИ не может позволить себе поражения даже на тактическом уровне, не говоря уже о затянувшемся тупике в будущих войнах. Если сдерживание или сражение закончатся поражением, ни израильтяне, ни АОИ не будут располагать вторым шансом.

В отличие от вооруженных сил западных государств, киберугрозы не занимают верхние строчки в распорядке дня израильской безопасности просто из-за высокой интенсивности не-кибер угроз, охватывающих диапазон от терроризма до массированного использования неуправляемых боеприпасов и управляемых ракет и иранской ядерной программы. Тем не менее, Израиль одна из самых передовых стран, что касается роли государства в

[5] Efraim Inbar and Eitan Shamir, "'Mowing the Grass': Israel's Strategy for Protracted Intractable Conflict," *Journal of Strategic Studies* 37, no. 1 (2014), https://doi.org/10.1080/01402390.2013.830972.

национальной кибербезопасности. Огромная часть деятельности по обеспечению кибербезопасности осуществляется невоенными организациями.

В следующих разделах представлен сначала гражданский элемент, а затем роли АОИ.

Эволюция Национальной кибер стратегии Израиля

Положения о защите критической инфраструктуры от 2002 года

Несмотря на преобладание гораздо более летальных и существенных некибер угроз национальной безопасности, правительство Израиля осуществляет Защиту критической инфраструктуры (ЗКИ) с 2003 года.

При полном понимании гражданской инфраструктуры и ее кибер уязвимостей, накопленных за годы оборонного опыта, на рубеже веков МАФАТ (Управление по исследованиям и разработкам Министерства обороны) озвучило перед другими департаментами правительства свою озабоченность уязвимостями критической гражданской инфраструктуры. В итоге, тогда правительство поставило Совету национальной безопасности (СНБ) задачу наметить в общих чертах стратегии для того, чтобы справляться с возникающими рисками. Это привело к тому, что 11 декабря 2002 правительство Израиля приняло специальную резолюцию B/84 об «Ответственности за защиту компьютеризированных систем государства Израиль». Израиль создал порядок ЗКИ, который требовал от наблюдаемых организаций нанять на работу специальный персонал по ИТ-безопасности, который будет нести ответственность за реализацию профессиональных указаний государственного ведомства. Государство решило создать новую организацию по ЗКИ *Pe'em* (Национальное агентство информационной безопасности, НАИБ). *Pe'em* имело возможность пользоваться подходящей правовой базой, созданной «Законом о безопасности в государственных органах» 1998 года и Статутом *Шабак*-а (Агентства внутренней безопасности). Контролируемые частные предприятия и государственные коммунальные сооружения несли финансовую ответственность за все операции, за защиту, поддержку, апгрейд, архивирование и восстановление своих критических ИТ систем – включая изменения, расширение и оборудование разрешенных *Pe'em,* – обмениваясь информацией и осуществляя совместную деятельность с регулятором. И наконец, закон определял санкции против должностных лиц контролируемых организаций, которые пренебрегают обязательными для выполнения требованиями, поставленные *Pe'em*.

Такая организация Защиты критической инфраструктуры имела место со времени принятия Резолюции B/84 от 2002. С тех пор государственный и оборонный сектор заботились сами о себе, поскольку израильская полиция занималась строго уголовными случаями киберпреступности. В результате, в конце первого десятилетия 21 века, львиная доля населения – малый и средний бизнес (МСБ), неправительственные организации (НПО) и обыкно-

венные граждане – остались без киберзащиты. С развитием технологий сценарии угроз расширялись, но контрмер не было. В число угроз входили потенциальный срыв гражданских услуг, накапливание небольших инцидентов в МСБ, риски для «спрятанных» или встроенных компьютеров (навигационные устройства или контролеры автомобилей) и разрушение морального духа и устойчивости общества с использованием кибер средств (например, операции по оказанию влияния через социальные медиа). Тем не менее, этой темой занимались только эксперты.

Экспертный обзор в рамках Национальной кибер инициативы

Публичное раскрытие Stuxnet-а в 2010 выстрелило кибербезопасность на самый верх политической повестки по всему миру. Премьер-министр Биньямин Нетаньяху обратился к генерал-майору (в отставке) профессору Исааку Бен-Израилю, который в то время был председателем Национального совета по исследованиям и разработкам в Министерстве науки, с просьбой рассмотреть кибербезопасность и дать рекомендации относительно политики Израиля в этом направлении. Профессор Бен-Израиль принял задачу, и в 2010 году была организована Национальная кибер инициатива с целью:

> сохранить положение Израиля в мире в качестве информационно-технологического центра развития, обеспечить стране способности суперсилы в киберпространстве, гарантировать его финансовую и национальную устойчивость, как демократическое, основанное на знаниях и открытое общество.

Национальная кибер инициатива занялась тремя главными вопросами:

- Как стимулировать и развивать кибер технологии в Израиле для гарантирования его положения как мирового (топ 5) лидера в мире к 2015 году?
- Какие структуры нужны для развития кибер технологии в Израиле?
- Какая организация нужна, чтобы наилучшим образом справляться с рисками и угрозами в киберпространстве?

Таким образом, Национальная кибер инициатива занималась не только национальной безопасностью в тесном смысле. Состав специальной группы отражал широкий взгляд инициативы и ее интегрированный подход. В результате, в течение шести месяцев 80 экспертов – представители оборонного сектора и вооруженных сил, академических кругов, директора по исследованиям и разработкам разных институций и представители соответствующих министерств – сделали систематический обзор проблем и возможностей. Команда была разделена на восемь суб-комитетов, один из которых был засекречен.

Национальная стратегия кибербезопасности Израиля от 2011

Решением No. 3611 от 7 августа 2011 «Развитие национальных способностей в киберпространстве»[6] Правительство принимало рекомендации Национальной кибер инициативы, и это решение является публичной Национальной стратегией кибербезопасности Израиля. Как и все официальные документы высшего уровня, Национальная стратегия кибербезопасности является «большой стратегией», которая декларирует видение и руководящие принципы. От этой большой стратегии были разработаны последующие стратегии для каждого домена.

Главной рекомендацией было создать специальное правительственное агентство, которое будет направлять работу в кибер сфере для публичного сектора и частных субъектов и координировать инструменты политики. Кроме того, документ рекомендовал:

1. создать Национальное кибер бюро (далее Бюро) при администрации премьер-министра;
2. регулировать ответственность за работу с кибер сферой;
3. усовершенствовать оборонительные кибер способности Израиля и содействовать исследованиям и разработкам в киберпространстве и суперкомпьютинге;
4. обеспечить достаточный бюджет для реализации Решения, который предлагается премьер-министром после консультаций с министром финансов и вносится в Правительство для одобрения в течение двух месяцев после принятия этого Решения.

Национальное кибер бюро Израиля (НКБИ)

Чтобы разработать и реализовать большую стратегию, при Администрации премьер-министра (АПМ) было создано Национальное кибер бюро (НКБИ).[7] Рез. 3611 определяет его миссию и роли следующим образом.

Миссия:[8] Бюро функционирует в качестве консультативного органа при Премьер-министре, правительстве и его комиссий, который дает рекомендации относительно национальной политики в кибер сфере и содействует ее осуществлению в соответствие с законом и решениями Правительства.

---

6 Government decision 3611: Promoting national capacity in cyber space (Jerusalem, Israel, PMO Secretariat).

7 Главой НБКИ был назначен доктор Евиатар Матания. Он сформировал организацию и направлял ее работу. Он прослужил два трехлетних срока, оставаясь на этой должности до конца 2018.

8 Миссии, роли и задачи Национального кибер бюро Израиля, представленные в этом разделе, определены в Резолюции правительства No. 3611 от 7 августа 2011 «Развитие национальных способностей в киберпространстве», в наличии на https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Israel_2011_Advancing National Cyberspace Capabilities.pdf.

Роли:

- Консультировать Премьер-министра, правительство и его комиссий в отношении киберпространства. По вопросам иностранных дел и безопасности, консультации, предоставляемые правительству, его комиссиям и министрам будут осуществляться Бюро через механизмы Совета национальной безопасности.
- Консолидировать административную работу правительства и его комиссий, касающуюся киберпространства; осуществлять подготовку для обсуждений в этих органах и последующую реализацию их решений. По вопросам иностранных дел и безопасности консолидация административной работы, подготовки обсуждений и последующее проведение решений будут осуществляться Бюро через механизмы Совета национальной безопасности.
- Давать рекомендации Премьер-министру и правительству относительно национальной кибер политики, определяемой правительством и/или Премьер-министром, реализовывать эту политику и следить за ее выполнением.
- Информировать все соответствующие органы в той степени, в которой это необходимо, относительно дополнительных указаний, касающихся кибер политики, проистекающих из решений Правительства и его комиссий.
- Определять и подтверждать, ежегодно, национальный референтный список угроз, требующих защиту киберпространства.
- Способствовать исследованиям и разработкам в киберпространстве и суперкомпьютинге в профессиональных единицах.
- Помогать работе кибер индустрии в Израиле.
- Формулировать национальную концепцию действий на случай чрезвычайной ситуации в киберпространстве.
- Проводить национальные и международные учения для повышения готовности Государства Израиль для действий в киберпространстве.
- Собирать разведывательную информацию от всех участников разведывательного сообщества, касающуюся кибербезопасности.
- Определять статус национальной ситуации в отношении кибербезопасности на основании информации всех сторон, которых это касается.
- Способствовать и повышать общественную осведомленность об угрозах в киберпространстве и средств для борьбы с ними.
- Формулировать и публиковать предупреждения и информацию для широкой общественности относительно кибер угроз, а также популяризировать хорошие практики превентивного поведения.

- Способствовать формированию национальных планов образования и благоразумного использования киберпространства.
- Способствовать сотрудничеству в киберсфере с параллельными органами за границей.
- Содействовать координации и сотрудничеству между государственными органами, оборонным сообществом, научными кругами, производственными субъектами, фирмами и другими органами, имеющими отношение к кибер области.
- Содействовать усовершенствованию законодательства и регуляции в кибер сфере.
- Служить регулятивным органом в областях, связанных с кибербезопасностью, как указано в Статье I, Дополнение B.
- Выполнять любые другие задачи в кибер сфере, определенные Премьер-министром в соответствие со всеми законами и решениями Правительства.

Задачи:

Руководителю Бюро была поставлена задача представить Премьер-министру в течение 90 дней с момента назначения подробный план, базирующийся на рабочих принципах, сформулированных Председателем Национального совета по исследованиям и разработкам (НСИР), профессором генерал-майором (в отставке) Исааком Бен-Израилем, в том числе:

- обратиться к Совету по высшему образованию (СВО) и Комитету по планированию и бюджетированию (КПБ) и потребовать, чтобы они рассмотрели возможности для создания академического исследовательского центра по киберпространству;
- способствовать созданию национального центра знаний по высокопроизводительным вычислениям. Если центр будет академическим, обратиться к *Малак* и *Ватат*[9] с просьбой изучить этот вопрос;
- создать инфраструктуру для развития кибер технологии, например, создать способности для симуляций и национальную систему аккредитации кибер технологий;
- усовершенствовать экспортные процедуры, имеющие отношение к киберпространству и осуществлять надзор над экспортом в этой сфере;
- разрабатывать инструменты для действий в чрезвычайных ситуациях в киберпространстве;
- развивать национальную кибер оборону;

[9] Смотри специальные разделы ниже.

- разрабатывать решения для определенных проблем кибер обороны;
- разрабатывать местные кибер решения и технологии.

Баланс основных свобод и потребностей безопасности

В июне 2013 Эдвард Сноуден начал публиковать секретные документы, которые он украл, раскрывая множество программ глобального наблюдения, многие осуществляемые АНБ Соединенных Штатов, АДС Австралии, ШКПС Объединенного Королевства, ЦБКК Канады, часто в сотрудничестве с телекоммуникационными компаниями. Эти разведывательные управления собрали огромное количество информации, и Сноуден, в числе многих, утверждал, что эти программы нарушают гражданские права, в частности право на конфиденциальность, и являются нарушением множества местных законов. Очевидно АНБ подключается к серверам основных интернет фирм, включая Facebook, Google, Microsoft и Yahoo, для прослеживания онлайн коммуникаций, используя программу наблюдения, известную под наименованием Prism.

В то время молодое НБКИ занималось наращиванием структуры, тогда как зрелое *Ре'ем* сосредотачивало свое внимание на операциях по ЗКИ. Поскольку *Ре'ем* было подразделением *Шабак,* на заднем плане начал маячить потенциальный риск. Служба безопасности или контрразведывательная организация, которая имеет доступ к сетям других людей для конкретного расследования, может воспользоваться этим доступом в некоторой степени в других целях. Верно, что *Шабак* никогда не злоупотребляло активами для ЗКИ в своих целях. Также верно и то, что *Ре'ем* имеет длинный список успехов и что гражданский надзор над *Шабак*-ом был хорошо развит к 2010 году. Тем не менее, раскрытия Сноудена о АНБ выдвинули противоречие свободы-безопасность на самый верх повестки дня публичных дебатов и политики. Все последующие существенные события в развитии израильской стратегии должны рассматриваться на этом фоне.

Национальная служба кибербезопасности (НСКБ)

Решением израильского правительства 2444 от 15 февраля 2015 была создана Национальная служба кибербезопасности (НСКБ) для защиты израильского гражданского киберпространства.[10] НСКБ была создана параллельно с НБКИ в АПМ. В отличие от агентств для ЗКИ или кибербезопасности в других местах, НСКБ не получила никаких правоохранительных полномочий. Это целенаправленная попытка избежать любое подозрение на подобные АНБ практики, установить доверие и способствовать сотрудничеству со всеми имеющими отношение к кибербезопасности субъектами в обществе. Этот уникальный проект был направлен на снижение противоречия между

[10] Решение было принято после нескольких раундов обширных консультаций, с учетом официальных рекомендаций проф. Бен-Израиля.

основными свободами и безопасностью и на повышение общественного доверия к этой правительственной службе. Следуя той же логике, решение предполагает включение в НСКБ организации для ЗКИ *Ре'ем*. Действительно, *Ре'ем* была переброшена от ИАБ (*Шабак*) в НСКБ в ходе процесса, который занял примерно год.

Служба начала работать в АПМ 1 апреля 2016, 90 дней после того, как господин Буки Кармели был назначен главой Службы. Во время ежегодной Кибернедели, проводимой Интердисциплинарным исследовательским кибер центром Блаватника (ИИКЦ) университета Тель-Авива, в июне 2017 НСКБ провела однодневное мероприятие по своему представлению, на котором перед публикой в 600 человек было представлено ее руководство и ее планы. Все руководители НСКБ представили свои взгляды и идеи. Глава НСКБ, Буки Кармели, использовал аналогию с водоснабжением, чтобы представить свое видение НСКБ:

> Мы (НСКБ) рассматриваем кибербезопасность как общественную систему водоснабжения. Мы занимаемся непрерывностью поставки чистой воды всему обществу. Когда мы обнаруживаем загрязнение, мы не разбираемся кто загрязнил ее, по небрежности или злонамеренно.

В 2017 все кибер технологические деятельности Бюро были интегрированы в Отдел кибер технологий, который является национальной технологической службой для развития кибер способностей и технологий на национальном уровне.

Группа реагирования на чрезвычайные ситуации в компьютерной сфере – Израиль (ГРЧСК-Ил)

Сфокусированная на сотрудничестве, НСКБ разработала концепцию и технологию повышения национальной ситуационной осведомленности и безопасности в киберпространстве. НСКБ создала и работает с новой Национальной группой реагирования на чрезвычайные ситуации в компьютерной сфере (*ГРЧСК-Ил*), которая должна стать центральной публичной точкой контакта для поддержки всех гражданских не-критических секторов. Это несущая колона в долгосрочной работе по обеспечению безопасности гражданского сектора Израиля в целом. Хотя *ГРЧСК-Ил* отрабатывает каналы для работы с чувствительными данными и секретными службами, она остается доступной для каждого гражданина.

ГРЧСК-Ил была спланирована и встроена в CyberSpark комплекс в Бее'ер Шеба и начала работать 1 июля 2014. Промышленный консорциум под руководством израильского оборонного контрактора RAFAEL выиграл тендер и построил базу *ГРЧСК-Ил*.

Национальный кибер-директорат Израиля (НКДИ)

В соответствие с решением 2444 от 2015, НСКБ, оперативный орган кибер защиты и НКБИ, отвечающее за политику и формирование кибер-сил, сов-

местно составили Национальный кибер-директорат, работающий при Администрации премьер-министра, напрямую подчиняясь председателю правительства. Глава Кибер-бюро был назначен главой и Директората и ответственным за одобрение рабочих планов Службы и бюджета Бюро. С созданием НСКБ руководящий принцип отделить строительство сил от ежедневных задач привел к созданию отдельной организации. После двух лет, несмотря на хорошие результаты, концепция изменилась в сторону создания единой структуры с упрощенной иерархией. Для канализирования работы Правительство Израиля решением 3270 от 17 декабря 2017 слило воедино Бюро и Службу в Национальный кибер-директорат, несущий ответственность за все аспекты кибер обороны в гражданской сфере, от формулирования политики и наращивания технологической мощи до оперативной кибер обороны.[11]

Сильное участие частного сектора, НПО и академических кругов

Стратегия полностью выдержана в духе сотрудничества и действительно НКДИ инициировал, финансировал и координировал множество мероприятий, касающихся всей израильской экономики. Одним из примеров является учреждение и со-финансирование Исследовательских кибер центров в большинстве исследовательских университетов Израиля. Эти академические центры передового опыта проводят независимые научные исследования. Другим примером является создание и со-финансирование нескольких стимулирующих инновации программ в партнерстве с Инновационной службой Израиля. Что касается пропаганды кибербезопасности во всем обществе, НКДИ не намеревается вводить какие-то дополнительные регуляции, а наоборот, призывает к кооперативной работе с уже существующими регуляторами.

АОИ: роли и ответственности Национальной кибер обороны

МО и АОИ не считают, что их задачей в кибер сфере является защита всего общества. Сектор обороны защищает в кибер сфере только себя, тогда как НКДИ обслуживает всех остальных. Такое разделение характерно для всех западных демократий.

Кибербезопасность стала существенным риском. Что делает по этому вопросу АОИ? Генерал-майор (в отставке) Амидрор пишет:

> АОИ, как и другие вооруженные силы, очень занята тем, как наилучшим образом интегрировать кибер способности как для оборонительных, так и для наступательных задач. Поскольку ясно, что кибер война

[11] К этому времени, когда доктор Матания закончил свой срок на должности главы Директората, его наследником был назначен господин Игаль Унна, который вступил в должность в начале 2018. Доктор Матания стал профессором и руководителем программы исследований в сфере безопасности Университета Тель-Авива. Смотри https://www.gov.il/he/Departments/policies/dec_3270_2017.

> станет очень важной в следующие годы, и поскольку впереди лежит длинная дорога, АОИ уже инвестирует значительные суммы денег и очень талантливый персонал в эту сферу и принимает участие в комплексном и всеохватном развитии своих кибер способностей. Как организовать новые подразделения, ответственные за кибер проблематику, отношения между наступательными и оборонительными усилиями и количественное отношение между ними остаются большими проблемами.[12]

Имеющиеся публичные источники предполагают, что Компьютерные сетевые операции (КСО) в АОИ имеют следующую организацию.

Предполагаемые операции

6 сентября 2007 года ВВС Израиля успешно бомбили и разрушили строящийся комплекс в Аль-Кибар, вблизи от города Дейр-ез-Зор в восточной Сирии. Здание скрывало строительство графито-водного ядерного реактора: почти точной копии плутониевого реактора в Северной Корее.[13] Нападение на проект сирийского реактора является отголоском дерзкого рейда ВВС Израиля в 1981 году, при котором был уничтожен ядерный реактор *Озирак* в Ираке. Но в этот раз определяющей для оперативного успеха, предположительно, была кибератака: преодоление плотной сирийской противовоздушной обороны. По информации иностранных источников, значительная сирийская противовоздушная оборона не смогла идентифицировать восемь истребителей ВВС Израиля в наблюдаемом воздушном пространстве. Эти источники предполагают, что Израиль инфильтрировал и временно нейтрализовал РЛС и коммуникационные системы сирийской противовоздушной обороны в ходе кибератаки. Эта проведенная 12 лет назад операция показывает размытую границу между электронной борьбой и способностями для ведения кибер-войны. В любом случае, это показывает, что кибератака может играть поддерживающую роль для кинетического удара.

Публичное раскрытие вредоносной программы Stuxnet в июле 2010 и ее последующие анализы раскрыли глаза общественности. Крайне важно то, что Stuxnet показал, что кибератака действительно может стать причиной существенного физического ущерба. Как писали Демчак и Домбровски:

> Метод Stuxnet-а и его успех изменили представление об уязвимости во все более связанных обществах и критических инфраструктурах. Дни кибер-шпионажа через бэкдоры программного обеспечения или предательство доверенных внутренних лиц, вандализм и даже кража вдруг

---

12 Amidror, “The Evolution and Development of the IDF.”

13 Elliott Abrams, *Tested by Zion: The Bush Administration and the Israeli-Palestinian Conflict* (Cambridge University Press, 2013).

> превратились в демонстрированную способность наносить потенциально убийственные удары, вообще не находясь вблизи от цели.[14]

Вредоносная программа постепенно повреждала центрифуги на заводе по обогащению урана Натанц в Иране перепрограммируя программируемые логические контролеры (ПЛК) фирмы Siemens, которые управляли центрифугами, вызывая увеличение оборотов двигателей за пределы безопасного диапазона. Скрытная, упорная атака в защищенной, физически изолированной сети сначала должна была компрометировать оперативную систему Microsoft Windows и затем начать распространяться внутри корпоративной сети для того, чтобы добраться до программируемого логического контролера (ПЛК). К концу 2010 Stuxnet заразил приблизительно 100 000 хостов в десятках странах, 60 процентов из которых были в Иране.[15] Удивительно, но заражение Stuxnet-ом не означало однозначно повреждение. Stuxnet выполняла свою атакующую функцию (ПЛК код, который предположительно изменял скорость вращения центрифуг) только тогда, когда находила специфическую аппаратную и программную конфигурацию. Зараженной системе, которая не отвечала предварительно определенным параметрам, не наносилось никакого ущерба.[16] Таким образом, Stuxnet является высокоточным оружием: кибератака, которая приводит к физическому разрушению только конкретной цели.

К4Р и кибер оборона (Agaf Ha-Tikshuv Vehahagana Bisvivat Reshet)

В июне 2015 АОИ опубликовала решение объединить кибер подразделения К4Р (командование, контроль, компьютеры, коммуникации и разведка) управления Генерального штаба и Военную разведку под единым командованием к 2017 году. Затем АОИ отказалась от этого плана интегрирования оборонительных и наступательных способностей.

В мае 2017 Генеральный штаб АОИ переименовал Службу К4Р (которое было создано в 2003 году) в Службу К4Р и Кибер обороны. Недавно созданный отдел кибер обороны АОИ был включен в состав службы К4Р. Сейчас Служба К4Р отвечает за безопасность сетей в АОИ и продолжает отвечать за Оборону компьютерных сетей (ОКС) и связанную с этим Эксплуатацию компьютерных сетей (ЭКС). Кроме того, К4Р остается центральным игроком в кибербезопасности Израиля, так как служба отвечает за:

- профессиональную подготовку персонала АОИ для должностей, связанных с информационными и коммуникационными технологиями;

---

[14] Chris C. Demchak and Peter Dombrowski, “Rise of a Cybered Westphalian Age,” *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32-61.

[15] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014).

[16] Jon R. Lindsay, “Stuxnet and the Limits of Cyber Warfare,” *Security Studies* 22, no. 3 (2013): 365-404, https://doi.org/10.1080/09636412.2013.816122.

- разработку программного обеспечения для АОИ;
- архитектуру ИКТ систем для АОИ;
- базовые криптографические разработки для АОИ и Израиля в целом.

Служба К4Р и кибер оборона стремится к утверждению видения об единой сети АОИ. Однако, нерешенной проблемой в АОИ остается недостаточный уровень сотрудничества, трения и конфликт интересов между военно-воздушными и сухопутными силами. Тем не менее, хотя в последние несколько лет ИКТ способствовали более тесной коммуникации и координации, это не создает автоматически совместность действий.

Нельзя обвинять только АОИ в отсутствии совместности действий. В деловом секторе не меньше разрозненности и некоординированных действий, чем в любых передовых вооруженных силах. С принятием на вооружение в военных формированиях все большего количества готовых кибер технологий, цифровая брешь между «элитными» и обыкновенными подразделениями увеличивается. Если на это не обращать внимание, такое развитие может начать мешать совместности и координации военных кибер действий в АОИ и других оборонных организациях Израиля.

Эта точка зрения, конечно, сталкивается со значительными проблемами: многие из формирований и служб АОИ разработали и используют самые разнообразные информационно-коммуникационные технологические решения для разных инфраструктур. Наиболее вероятным результатом для этого подхода была бы унификация цифровой инфраструктуры в рамках сухопутных сил АОИ: естественная сфера К4Р.

Военная разведка (Agaf haModi'in – Aman)

Разведывательные организации были пионерами кибер технологий, накапливая большой оперативный опыт, оставаясь на шаг вперед перед гражданскими способностями. Стратегия Израиля отдает приоритетное значение как раннему предупреждению, так и превосходству в качестве. Эти два фактора являются одними из причин того, почему израильские разведывательные организации заработали такую высокую кибер репутацию.

Аман является независимой службой, которая не состоит в составе сухопутных сил, военного флота или военно-воздушных сил. Формирование 8200 *Аман* отвечает за сбор радиоэлектронных разведданных (SIGINT) и за расшифровку кодов. По мнению аналитиков разведки, подразделение 8200 подобно АНБ или британской Штаб-квартире правительственной связи (ШКПС), часто покрывая весь разведывательный цикл. Иностранные источники утверждают, что подразделение 8200 содействовало разработке Stuxnet, Flame, Duqu, и других сложных кибер кампаний для наступления и разведки.

Даже в этом случае Военная разведка остается ответственной за Атаки на компьютерные сети (АКС) и за Эксплуатацию компьютерных сетей (ЭКС).

Израильские Военно-воздушные силы (ИВВС)

Израильские Военно-воздушные силы рассматривают боевые действия как применение передовых высоких технологий для ведения войны. Самолет олицетворяет превосходство передовой технологии.[17] Культура вида вооруженных сил ИВВС основывается на центральном командовании и управлении и на поддерживающую роль коммуникаций [18] и предполагает получение полной картины всего воздушного пространства в реальном времени. Штабы аккуратно планируют каждую воздушную миссию; график времени точен, определен по расстоянию, полетному пути, маневров уклонения, весу полезного груза и количеству топлива. ИВВС создало и управляет свои собственные функции поддержки: логистика; командование, управление, коммуникации, компьютеры (К4); разведка; радиоэлектронная борьба (РЭБ) и специальные силы (подразделение *Шалдаг*) – и все они критически важны для воздушного превосходства. Практически, все в ИВВС сильно зависит от передовых цифровых информационных и коммуникационных технологий. ИВВС имеет свою собственную разведку (*Лахак Моди'ин – Ламдан*). Поскольку ИВВС полностью зависит от цифровых ИКТ, необходимость обеспечить их безопасность является важным соображением при конфигурировании и ведении операций, что способствует высокой кибер зрелости в ИВВС. Кроме того, ИВВС имеет отдельную и более передовую инфраструктуру, чем другие виды вооруженных сил АОИ.

Побочные эффекты оборонных исследований и разработок

В середине 90-х Израиль был государством всеобщего благосостояния с выживающей экономикой и незначительной хай-тек индустрией. Всего через несколько лет, все еще борясь с неотложными проблемами безопасности, Израиль превратился в технологического гиганта с совершенным и инновационном сектором высоких технологий. Сегодня представление израильских хай-тек компаний в Службе автоматизированных котировок Национальной ассоциации дилеров по ценным бумагам (NASDAQ) обгоняет такие экономические и технологические суперсилы, как Британия, Япония и Южная Корея, и уже в течение десятилетия Израиль является одним из ведущих инновационных технопарков в мире. АОИ стала причиной двух побочных эффектов, которые способствовали успеху Израиля в высоких технологиях и кибербезопасности.

С учетом гораздо меньшей территорией и численностью населения Израиля по сравнению с его противниками, израильская стратегия безопасности всегда опиралась на преимущество в качестве, которое включает умения людей, моральное и научно-технологическое превосходство. АОИ воспринимает кибер технологию как важный, универсальный и качественный

---

[17] Allen W. Batteau, "The Anthropology of Aviation and Flight Safety," *Human Organization* 60, no. 3 (Fall 2001), pp. 201-211.

[18] Amidror, "The Evolution and Development of the IDF."

мультипликатор способностей вооруженных сил. Как и в США, несколько родов войск АОИ и невоенные разведывательные организации давно обращали внимание на развитие и использование средств электронной борьбы, сигнальной разведки, криптирования и информационной безопасности, компьютерной и информационной войны. Почти тридцать лет назад несколько заинтересованных субъектов в АОИ уже вложили значительные усилия в радикальные инновации, которые сегодня назвали бы средствами для «кибер войны». Как DARPA в США, Маф'ат (Директорат исследований и разработок Министерства обороны) инициировал и содействовал дерзким инновациям в сфере кибер ИР.

Независимо от того, что требуют разные виды вооруженных сил, Маф'ат может независимо инициировать большие ИР проекты. Параллельно, основные заинтересованные в кибер домене субъекты АОИ – разведка, К4Р, военно-воздушные и специальные силы – располагают потенциалом выполнять и заказные ИР и приобретать разработки, необходимые для обеспечения их миссий.

В дополнение к секретным ИР, в октябре 2012 Маф'ат и НКБИ начали выполнение плана ИР с двойным предназначением, гражданским и оборонным, названным МАСАД.

Побочные эффекты военного человеческого капитала

Швед и Батлер принимают, что процесс социализации военных культивирует новые умения (человеческий капитал), новые социальные сети (социальный капитал) и новые социальные нормы и кодексы поведения (культурный капитал). Эти три эффекты вместе можно назвать «военным капиталом». Призывники абсорбируют военный капитал, или его часть, во время службы и «экспортируют» его в гражданскую сферу, где он хорошо конвертируем, особенно в хай-тек секторе. Например, способность импровизировать очень ценится как умение, необходимое для решения проблем в ненадежной и бедной ресурсами среде, и поэтому поощряется культурой АОИ, хотя и не является частью официального кодекса АОИ.[19]

Израиль сохраняет обязательный призыв на военную службу для тех, кому исполняется 18 лет. АОИ регулярно готовит и усовершенствует подготовку новых призывников, а также кадровых офицеров. Учитывая трехлетнюю обязательную службу для мужчин, можно предположить, что в каждый момент одна треть армии участвует в разных программах подготовки.

[19] Возможно, наиболее организованной и влиятельной группой является ассоциация 8200. Имя 8200 стало маркой, поскольку ее ветераны были авангардом местной хай-тек индустрии и индустрии венчурного капитала. В сравнении с другими военными ветеранами, конвертируемость военного капитала служивших в подразделении 8200 наиболее высокая. Смотри Ori Swed and John Sibley Butler, “Military Capital in the Israeli Hi-Tech Industry,” *Armed Forces & Society* 41, no. 1 (August 2015), https://doi.org/10.1177/0095327X13499562.

АОИ давно разработала сложную систему для оценки потенциала призывников и начала назначать подходящую подготовку и карьерный путь развития для большинства, существенно способствуя увеличению доли экспертов по науке и технологиям в Израиле.[20] После обязательной службы те, кто получил ценную подготовку, с большей вероятностью, чем остальные, становятся резервистами.

Профили израильских хай-тек сотрудников содержат некоторое количество очень высококачественного военного капитала. Более того, рынок труда в хай-тек сфере демонстрирует институциональное предпочтение к тем, кто располагают военным капиталом. Действительно, общая и военная служба в технологических подразделениях воспринимается как преимущество, эквивалентное университетской степени.[21]

Доктринальные вызовы перед АОИ

Инструменты для кибер войны и автономные системы стали первейшим приоритетом для обороны. Какие роли следует АОИ возлагать на кибер способности? Рассмотрим следующий набор вопросов: Должны ли кибер способности поддерживать кинетические способности, должны ли они заменять кинетические удары там, где это возможно, или они должны давать такие результаты, которые сделают кинетическую силу ненужной? Насколько хорошо АОИ будет их использовать. Существенные изменения для АОИ не менее тяжелы, чем для любой другой большой бюрократической организации.

Прозрачность против секретности

Большинство вызовов перед кибербезопасностью очень существенны. Виды вооруженных сил и роды войск АОИ («Зроа» на иврите) подвергаются существенным реорганизациям. Однако, АОИ не может освободиться от привычки скрывать большую часть своей деятельности не только от широкой общественности, но и от компетентных органов и служб. Эти хорошо известные тенденции мешают кооперативным интеллектуальным усилиям как в коммерческих, так и в военных организациях. Следующий обзор был выполнен без доступа к официальным источникам. Однако, критическая оценка очень затруднена, когда нет доступной базы фактов.

В 2010 решение МО США отменить самонавязанное табу на обсуждение наступательных кибер способностей, вероятно, способствовало тому, что в 2012 АОИ заявила, что рассматривает использование наступательных средств кибер войны. В августе 2015 Армия обороны Израиля (АОИ) опубликовала свою первую доктрину обороны, автором которой является Начальник Генерального Штаба АОИ генерал-лейтенант Гади Эйзенкот.

---

[20] Gil Baram and Isaac Ben-Israel, “The Academic Reserve: Israel’s Fast Track to High-Tech Success,” *Israel Studies Review* 34, no. 2 (2019), http://dx.doi.org/10.2139/ssrn3269147.

[21] Swed and Butler, “Military Capital in the Israeli Hi-Tech Industry.”

Публикация рассекреченной версии документа Стратегия АОИ, сформулированной в рамках многолетнего плана «Гидеон», была существенным прогрессом в гражданско-военных отношениях. Хотя Стратегия АОИ не является обязующим документом, она дает в общих линиях точку зрения вооруженных сил на стратегические и оперативные реакции на основные угрозы, с которыми сталкивается Израиль, и ставила перед политическим эшелоном вопрос о более ясных инструкциях. Стратегия АОИ описывала принципы использования вооруженных сил в контекстах, которые являются общими для всех оперативных театров военных действий против полугосударственного врага и в разных для АОИ функциональных ситуациях: рутинная, чрезвычайная и война.

Концептуализация кибер обороны как Мабат

Случаи широкомасштабных насильственных действий от 2002, 2006, 2008-9, 2012 и 2014 года иллюстрируют миссии АОИ в двадцать первом веке. АОИ разработала концепцию «кампании между войнами» (*Мабат – Маараха бейн Милхамот)* для описания военных операций на грани войны, которые АОИ инициирует и проводит с целью противостоять возникающим вражеским угрозам. Позже это слово стало официальным доктринальным термином и было включено в Стратегию от лета 2015. Эти тайные и явные операции охватывают диапазон от удаленного или на месте сбора разведывательной информации и до хирургических рейдов Специальных сил, высокоточных ударов и совместных маневров на батальонном уровне. Сила используется не для достижения политических целей, а для того, чтобы обезвредить способности врага для нанесения ущерба Израилю. К примеру, удары против иранских сил в Сирии и в других местах были направлены против транспортных средств, перевозящих оружие, против ключевых лиц или против сооружений.

Похоже, что концепция *Мабам* можно с успехом применять и к кибербезопасности. Зрелая кибер оборона уже не стремится только к предотвращению наличия брешей. Сегодня для организации эффективных кибер операций используются две модели – кибер убийственная цепочка и защита в глубину. *Мабам* – это стратегия почти рутинного состояния чрезвычайной ситуации, которая не рассчитывает на победу в одном единственном сражении. Подобным образом, зрелая кибер защита воспринимает реальность как продолжающееся, долгосрочное состязание между противниками. Эксперты по передовой кибербезопасности никогда не обещают абсолютную защиту, не говоря о решительной победе. Цель состоит в минимизировании угрозы через оборону в глубину, разведку и упреждающие действия. Концепция *Мабам* также рассчитывает на менее героическую оперативную рутину, а не на решительную победу, которая уничтожит врага.

Рассматривают ли таким образом кибербезопасность АОИ в целом или каждый из заинтересованных субъектов (К4 или разведка), очень неясно.

Концептуализация киберзащиты как воздушное превосходство

Эта общая стратегия, отдающая предпочтение качеству перед количеством, привела к длинному ряду оперативных достижений АОИ против арабских государств, которые осуществляли военную агрессию. В результате этого, Египет и Иордания подписали мирные соглашения, Сирия Асада не сделала ни единого выстрела против Израиля с 1982 года. Эти и другие факторы привели к укреплению воздушного и разведывательного компонента АОИ.

Военно-воздушные силы располагают полным воздушным превосходством и могут действовать против любой цели в воздухе, на земле или на море по всему Ближнему Востоку. ВВСИ стали как длинной стратегической рукой, так и главным исполнителем нанесения точных ударов, вытесняя артиллерию. Это воздушное превосходство, конечно, в основном, зависит от использования ИКТ – кибер технологий – на всех этапах: планирование; логистика; сбор, анализ и распространение разведданных; К2; РЕБ; подавление ПВО.

Какими будут оперативные, стратегические и политические пользы для АОИ, если она будет направлена на обеспечение кибер превосходства? Неизбежно, это приведет к драматическим переменам. Большая часть практики кибербезопасности направлена на минимизацию рисков для существующих способов «делать бизнес». Если ваша теория победы основывается на доминирующем маневре бронетанковых сил, то вам кибербезопасность будет нужна в той мере, в какой она поддерживает действия бронетанковых частей. Если ваша теория победы основывается на манипулировании политическим процессом принятия решений противника и его расчетами инструментами упорных операций по оказанию влияния через социальные медиа, тогда кибербезопасность будет иметь качественно другую роль.

Путь вперед

Для современных развитых стран в целом, и для Израиля в частности, национальные вооруженные силы доказали, что являются наиболее успешными оборонными организациями, которые обеспечивают безопасность в противоборстве с другими государствами. Но могут ли вооруженные силы обезопасить наши общества от иностранных кибер угроз? Рассчитывать на это было бы совсем не обосновано. Расходы на оборону Израиля составляют от 5 до 6 процентов от ВВП – примерно в четыре раза выше, чем в среднем для западных демократий. Какая часть из этих расходов обеспечивает национальную гражданскую кибербезопасность? Стратегия национальной кибербезопасности Израиля принимает разделение ответственности между оборонным и гражданским сектором: резолюция 3611 не касается «специальных органов»: Армии обороны Израиля, израильской полиции, израильского Агентства безопасности (*Шабак*), Института разведки и специальных операций (*Моссад*) и оборонных предприятий (в основном, оборонно-промышленный комплекс). Директорат безопасности оборонных предприятий

(*Малмаб*) остается государственным регулятором по вопросам кибербезопасности в оборонном секторе.

МО и АОИ не возлагают на себя обязанность защищать все общество в кибер сфере. Оборонный сектор защищает сам себя в кибер сфере, а для защиты всех остальных была создана новая национальная гражданская организация. Такое разделение типично для западных демократий. Западные вооруженные силы, в общем, и АОИ, в частности, играют почти незначительную роль в обеспечении национальной кибербезопасности для своих обществ. Западные военные лидеры должны сначала увидеть эту реальность и сформировать позицию по вопросу о желательной роли военных в национальной кибербезопасности. Диапазон возможных вариантов может быть выведен из двух общих стратегий:

- Возложить на военных задачу обеспечивать больше кибербезопасности. Это потребует ребалансирования соотношения между безопасностью и основными свободами так, чтобы вооруженные силы могли действовать во внутреннем гражданском кибер пространстве
- Обеспечить больше кибербезопасности без участия военных. Это потребует урезания конвенциональных оборонных сил для высвобождения ресурсов на кибербезопасность и создание новых гражданских организаций.

Теоретики и руководители обороны должны вложить максимум усилий в разработку эффективной национальной кибербезопасности, что потребует радикальных новаторских изменений в оборонных институциях и в других субъектах. Израиль проводит инновационную политику в сфере кибербезопасности с 2002 года. Хотя Израиль достиг относительно больших успехов в гражданской кибербезопасности, следует ожидать реализации большего количества инновационных решений.

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.

Признательность

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

Об авторе

Доктор Лиор Табански является руководителем отдела научных исследований и разработок Интердисциплинарного исследовательского кибер центра Блаватника, Университета Тель-Авива. Лиор Табански предлагает уникальное понимание кибербезопасности, сочетающее академические исследования по международной безопасности, 15 лет профессиональной ИТ работы и деловой опыт в формулировании кибер стратегий. Книга мистера Табански от 2015 года *Кибербезопасность в Израиле*, написанная в соавторстве с профессором Исааком Бен-Израиль, является первым комплексным отчетом десятилетий политики и операций Израиля, сделанный «внутренним» человеком. Более того, в книге сделан оригинальный анализ роли, которую играют в кибербезопасности большая стратегия и инновации. Докторская диссертация Лиора раскрывает, почему даже самые развитые нации остаются настолько подверженными деструктивным кибератакам по стратегическим внутренним целям, совершаемые иностранными государствами. *E-mail*: cyberacil@gmail.com.