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

Мари Бэзнер, *Connections QJ* 19, № 1 (2020): 73-84
https://doi.org/10.11610/Connections.rus.19.1.06

Национальная политика кибербезопасности

Кибербезопасность в Швейцарии: вызовы и путь вперед для швейцарских Вооруженных сил

Мари Бэзнер

Центр изучения вопросов безопасности, ФТИ Цюрих

Резюме: Политика кибербезопасности Швейцарии направлена на повышение компетентностей и знаний, инвестирование в исследования и обеспечение устойчивости критической инфраструктуры, мониторинг угроз, поддержку инноваций, утверждение стандартов и повышение осведомленности – все в рамках публично-частного, межрегионального и международного сотрудничества. Вооруженные силы оказывают поддержку этой политики путем развития способностей для разведки угроз и атрибуции, готовности предпринимать активные меры в кибер пространстве и обеспечения оперативной готовности в любых обстоятельствах.

Ключевые слова: кибер риски, стратегия кибербезопасности, устойчивость, кризисный менеджмент, охрана правопорядка, кибер защита, кибер операции.

Основные моменты политики

Как и в любой другой европейской стране, значение кибербезопасности в швейцарской политике увеличилось. И хотя работа над швейцарской политикой в сфере кибербезопасности и кибер обороны все еще продолжается, страна уже провела огромную работу по формированию правильной политики, ролей и ответственностей по кибербезопасности.

Опубликованная в 2018 году «Национальная стратегия по защите Швейцарии от кибер рисков» [1] является основным документом, определяющим политику, которым руководствуются швейцарские амбиции и который заменил стратегию от 2012 года.[2] В целом, стратегия ставит семь стратегических целей и устанавливает десять сфер деятельности. Цели можно подытожить следующим образом: подготовка Швейцарии к встрече во всеоружии с рисками завтрашнего дня путем создания компетентностей в сфере кибербезопасности, структур для кризисного менеджмента, повышения устойчивости и содействия международному сотрудничеству.

Стратегия сопровождается планом реализации,[3] который является результатом трехлетних консультаций с основными игроками на ландшафте швейцарской кибербезопасности. Тогда как управление стратегией централизовано, ее осуществление децентрализовано с ясным распределением ролей. План реализации перечисляет конкретные меры осуществления в десяти сферах деятельности, определенных в стратегии 2018 года. Так же уточняются ответственности, даются измеряемые цели и устанавливается график оценки прогресса реализации стратегии.

За написание и применение стратегии, и информирование швейцарского населения и частного сектора о любых новых кибер угрозах отвечает Швейцарский центр учета и анализа обеспечения безопасности информации (MELANI).

Другим важным документом является *План действий по кибер защите 2017* Федерального министерства обороны, гражданской защиты и спорта (МОГЗС). План действий определяет роли МОГЗС, Федеральной разведывательной службы (ФРС) и вооруженных сил на ландшафте швейцарской кибербезопасности. В целом, их роль состоит в защите сетей МОГЗС и критической инфраструктуры от кибер угроз, ведения военных и разведывательных кибер операций и оказание поддержки гражданским критическим инфраструктурам в случае больших кибератак.

Швейцарский политический ландшафт перетерпел существенные изменения за последние несколько лет. В 2016 Федеральный совет опубликовал

---

1 Swiss Federal Council, *National Strategy for the Protection of Switzerland against Cyber Risks (NCS) 2018-2022* (Bern: Federal IT Steering Unit FITSU, April 2018), https://www.isb.admin.ch/dam/isb/en/dokumente/ikt-vorgaben/strategien/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_EN.pdf.

2 Federal Department of Defense, Civil Protection and Sport DDPS, *National Strategy for the Protection of Switzerland against Cyber Risks* (revised), June 2012, https://www.isb.admin.ch/dam/isb/en/dokumente/ikt-vorgaben/strategien/ncs/Strategie%20zum%20Schutz%20der%20Schweiz%20vor%20Cyber-Risiken.pdf.

3 Swiss Federal Council, “Implementation Plan for the 2018-2022 National Strategy for the Protection of Switzerland Against Cyber Risks (NCS),” May 2019, https://www.isb.admin.ch/dam/isb/en/dokumente/themen/NCS/Umsetzungsplan_NCS_2018-2022_EN.pdf.

доклад о политике безопасности Швейцарии,[4] в котором подчеркивались риски, проистекающие из информационных технологий, и изменяющийся характер конфликта с учетом кибер пространства. Швейцарский парламент принял новый закон о разведке, который вошел в силу в 2017,[5] а в 2018 был изменен военный закон, чтобы позволить вооруженным силам иметь свои средства для защиты своих законных сетей и осуществлять наступательные кибер контрмеры. Недавно Федеральный совет учредил Федеральный кибер комитет для управления усиливающейся централизацией сферы кибербезопасности, что необычно для Швейцарии. Как федеральное государство, Швейцария предпочитает давать определенную свободу действий своим 26 кантонам и частному сектору. Кибер комитет также отвечает за осуществление мониторинга реализации национальной стратегии кибербезопасности.

Эти политические события показывают, что швейцарское правительство относится к проблемам кибербезопасности очень серьезно и занимается ими на самом высоком политическом уровне. Федеральный совет также создал Центр компетенций по кибербезопасности, который служит единой точкой контакта по всем вопросам кибербезопасности на национальном уровне. Он также координирует реализацию национальной стратегии. И наконец, последним развитием было назначение делегата по кибербезопасности, который не только направляет стратегию кибербезопасности, но и возглавляет специальный федеральный комитет по кибербезопасности и представляет Швейцарскую Конфедерацию в других комитетах.

Вызовы перед политикой

Национальная стратегия защиты Швейцарии от кибер рисков занимается большим набором проблем кибербезопасности. Она охватывает развитие технических способностей, модернизацию образования, борьбу с киберпреступностью, укрепление кибер способностей вооруженных сил, расширение международного сотрудничества и повышение осведомленности. Хотя стратегия конкретно сфокусирована на кибербезопасности, она также согласована с Политикой национальной безопасности Швейцарии от 2016 года, Стратегией Федерального совета о дигитализации Швейцарии от 2018 года, Национальной стратегией защиты критической инфраструктуры 2018-2022, и интегрирует в себя последние изменения в законе о разведке и законе о вооруженных силах.

---

[4] “Die Sicherheitspolitik der Schweiz: Bericht des Bundesrates,” August 24, 2016, https://www.vbs.admin.ch/de/themen/sicherheitspolitik/sicherheitspolitische-berichte/sicherheitspolitischer-bericht-2016.detail.document.html/vbs-internet/de/documents/sicherheitspolitik/sipolb2016/SIPOL-B-2016-de.pdf.html.

[5] “Federal Act on the Intelligence Service (Intelligence Service Act, IntelSA),” September 25, 2015 (по состоянию на 1 марта 2018) https://www.admin.ch/opc/en/classified-compilation/20120872/index.html.

В целом, стратегия подчеркивает необходимость в развитии публично-частных партнерств и в активном участии частного сектора, с одной стороны, и настаивает на дополняющей роли государства, с другой. Что касается вооруженных сил, стратегия упоминает необходимость не только развития оборонных способностей, но и обеспечения возможности вооруженных сил предпринимать активные меры в киберпространстве. Эти активные меры понимаются как способы и средства для создания помех, предотвращения или замедления действий противника против критической инфраструктуры Швейцарии. Кроме того, стратегия говорит, что Швейцария играет активную роль в формировании кибер норм на международном уровне и сотрудничает с другими странами. И наконец, стратегия подчеркивает значение повышения публичной осведомленности о проблемах кибербезопасности. Стратегия охватывает все эти элементы в десяти сферах деятельности:

1. Создание компетентностей и знаний
    - Мера 1: мониторинг тенденций в технологических инновациях;
    - Мера 2: развитие исследований и образования в киберсфере;
    - Мера 3: установление правовых рамок, которые будут поощрять инновации в сфере кибербезопасности;
2. Ландшафт угроз
    - Мера 4: улучшение и расширение способностей для анализа и представления ландшафта кибер угроз;
3. Менеджмент устойчивости
    - Мера 5: улучшение устойчивости критических инфраструктур;
    - Мера 6: улучшение устойчивости сетей федеральной администрации;
    - Мера 7: улучшение устойчивости кантональных сетей путем обмена информацией и опытом;
4. Стандартизация/регуляция
    - Мера 8: дефинирование и введение минимальных стандартов для повышения сопротивляемости сетей;
    - Мера 9: составление обзора на основе обязанности докладывать о кибер инцидентах;
    - Мера 10: расширение участия Швейцарии в международном управлении Интернета с целью обеспечения развития свободного и демократического Интернета;
    - Мера 11: создание экспертных групп для оценки регуляции в сфере кибербезопасности;
5. Менеджмент инцидентов
    - Мера 12: развитие MELANI как публично-частное партнерство;

- Мера 13: предоставление MELANI услуг для всех типов предприятий;
- Мера 14: развитие коллаборации между швейцарским правительством и другими центрами компетенции;
- Мера 15: создание процесса ясного определения ответственностей при менеджменте кибер инцидентов в рамках федеральной администрации;

6. Кризисный менеджмент
   - Мера 16: интеграция кибер экспертов в ячейки для кризисного менеджмента для стимулирования коллаборации с частным сектором в случае необходимости;
   - Мера 17: организация совместных учений по кризисному менеджменту с интеграцией элементов, связанных с кибербезопасностью в более всеохватных учениях и организация собственно кибер учений;
7. Преследование по закону
   - Мера 18: составление перечня текущих уголовных кибер преступлений в Швейцарии;
   - Мера 19: расширение коллаборации между разными центрами компетенций и национальной сети следователей по делам кибер преступности;
   - Мера 20: развитие образования по охране правопорядка для накопления знаний, касающихся преследования за кибер преступления;
   - Мера 21: модификация существующей структуры федеральных отделов по уголовным делам для создания нового Центрального управления по борьбе с кибер преступностью с целью усиления коллаборации между кантонами по делам кибер преступности;
8. Кибер оборона
   - Мера 22: развитие способностей для разведки угроз и осуществления атрибуции;
   - Мера 24: развитие способностей вооруженных сил для обеспечения их оперативной готовности в любых обстоятельствах;
9. Активное позиционирование Швейцарии в международной политике кибербезопасности
   - Мера 25: участие Швейцарии в ранних дискуссиях международных форумов по кибербезопасности;

- Мера 26: расширение международного сотрудничества, направленного на улучшение способностей и обмена информацией по кибербезопасности;
- Мера 27: установление двухсторонних и многосторонних диалогов по внешней политике безопасности в плане кибербезопасности;

10. Общественное влияние и повышение осведомленности
    - Мера 28: осуществление коммуникационной стратегии для стратегии кибербезопасности;
    - Мера 29: повышение осведомленности общественности о кибер рисках.

Десять сфер деятельности и содержащиеся в них меры направлены, главным образом, на развитие существующих структур и заполнение пробелов, которые были обнаружены в национальной стратегии от 2012 года. Основные отличия стратегий от 2018 и от 2012 касаются трех сфер деятельности. Первое отличие связано с кризисным менеджментом и повышением осведомленности. В стратегии 2018 в число групп, чья кибербезопасность находится под угрозой, включены население, малые и средние предприятия и кантоны, тогда как в стратегии 2012 года внимание было направлено только на операторов критической инфраструктуры. Второе отличие касается стандартизации и регуляции. В стратегии 2018 упоминается изучение возможного обязательства докладывать о кибер инцидентах, оценка и введение минимальных стандартов для ИТ безопасности критической инфраструктуры. Эти новые меры отражают Директиву Европейского Союза о сетевой и информационной безопасности (СИБ). Третье отличие касается кибер обороны. Стратегия 2018 года включает роль и ответственности вооруженных сил, тогда как в первой стратегии они полностью отсутствуют.

Как и Национальная стратегия защиты Швейцарии от кибер рисков, План действий по кибер защите (ПДКЗ) 2017 признает необходимость комплексного подхода к кибербезопасности. ПДКЗ 2017 служит дорожной картой для МОГЗС при расширении его кибер способностей. Документ направлен на повышение внимания к урокам, усвоенным при кибератаке RUAG в 2016,[6] и национальных учений по кибер защите. ПДКЗ 2017 идентифицирует пять основных областей, в которых МОГЗС должно обеспечить прогресс: стратегический менеджмент, развитие оперативных средств, создание механизмов поддержки со стороны структур милиции, улучшение коллаборации с

[6] В январе 2016 швейцарская медиа раскрыла, что технологическая фирма, являющаяся собственностью Швейцарской Конфедерации, стала объектом шпионской кибер кампании, ответственность за которую была атрибутирована на APT группу Turla. Для дополнительной информации об этой кибератаке смотри: “APT Case RUAG,” *GovCERT.ch*, Technical Report, May 23, 2016, https://www.melani.admin.ch/dam/melani/en/dokumente/2016/technical%20report%20ruag.pdf.

высшем образованием и частным сектором и нахождение квалифицированной рабочей силы. В ПДКЗ 2017 указано, что с 2016 МОГЗС уже стало принимать меры по реализации Системы менеджмента информационной безопасности (СМИБ) в соответствии с серией стандартов ISO 27000 и модернизации своих систем и своей сетевой инфраструктуры. ПДКЗ очень прозрачен в отношении ресурсов, которые необходимы для реализации этих целей.

Структуры для реализации политики и общегосударственный контекст

Швейцария является одной из самых федерализованных и децентрализованных стран в мире. Большое число задач оставлено для решения кантонам, включая образование и охрана порядка. Эта децентрализация иногда воспринимается как вызов и/или ограничение для федерального правительства, мешающие ему решать такие новые проблемы, как кибербезопасность. Действительно, прошедшие годы показали, что в сфере кибербезопасности преобладает тенденция сдвига в сторону централизации на федеральном уровне.

Координационная структура. С новой стратегией, Швейцария создала новую общую структуру с Кибер комитетом Федерального совета, уполномоченным по кибербезопасности, и Центром компетенций по кибербезопасности. Все эти новые институции играют роль при координации кибербезопасности на федеральном уровне:

- *Кибер комитет Федерального совета*: Комитет состоит из глав Федерального министерства финансов, МОГЗС и Федерального министерства правосудия и полиции (ФМПП). Комитет заседает четыре раза в году и осуществляет мониторинг реализации национальной стратегии кибербезопасности;
- *Уполномоченный по кибербезопасности*: Федеральный совет отвечает за выбор Уполномоченного по кибербезопасности. Уполномоченный отвечает за формирование повестки дня по вопросам кибербезопасности Швейцарской Конфедерации на федеральном уровне. Уполномоченный возглавляет внутренние комитеты по кибербезопасности и представляет Швейцарию в других комитетах в Швейцарии;
- *Основная кибер группа*: Группа подчиняется Кибер комитету Федерального совета и отвечает за улучшение коллаборации между тремя секторами: кибербезопасность, кибер защита и уголовное преследование. Группа несет ответственность за обеспечение совместной оценки угроз и осуществляет надзор через федеральных субъектов над менеджментом кибер кризисами, касающихся нескольких федеральных департаментов.

Фигура 1: Федеральная организация по кибер рискам.

- *Руководящий комитет по национальной кибербезопасности*: Комитет подчиняется Кибер комитету Федерального совета и гарантирует, что осуществление мер, описанных в стратегии, остается скоординированным. Руководящий комитет по НКБ также помогает предложениями о дальнейшем развитии политики;
- *Центр компетенций по кибербезопасности*: Центр подчиняется Федеральному министерству финансов и включает MELANI. Центр является единой точкой контакта по вопросам кибербезопасности на федеральном уровне и гарантирует скоординированную реализацию стратегии.

Роли и ответственности вооруженных сил: Вооруженные силы являются частью МОГЗС. Их роль состоит в защите и обороне своих собственных сетей и критической инфраструктуры от кибератак, поддержке ФРС при ответе на кибератаки, направленные против гражданской критической инфраструктуры и поддержке способностей в киберпространстве на случай войны. Условия, при которых вооруженные силы оказывают поддержку ФРС при защите от кибератак, очень строги, и вооруженные силы привлекаются только в качестве дополнительной помощи. Главным актором в киберзащите вооруженных сил в рамках МОГЗС является Электронный оперативный центр (ЭОЦ). ЭОЦ отвечает за выполнение вышеупомянутых задач и взаимодействует с ФРС в плане критической инфраструктуры. ЭОЦ состоит из военного и гражданского персонала; военные призывники, работающие в ЭОЦ, подчиняются Бригаде поддержки командования 41. После изменения закона о вооруженных силах сейчас вооруженные силы могут проводить наступательные контрмеры с разрешением Федерального совета.

Роли и ответственности органов охраны правопорядка:

- *Кантональные полицейские силы*: Борьба с киберпреступностью или кибер преступлениями является задачей полицейских сил. Каждый кантон выделяет ресурсы и организует борьбу с киберпреступностью по своему желанию. Кантон Цюрих создал Центр кибербезопасности и является одним из кантонов, который инвестирует наибольшие ресурсы в борьбу с киберпреступностью. С другой стороны, меньшие кантоны располагают ограниченными ресурсами и могут не быть в состоянии создавать такие центры, как центр кантона Цюрих. Кантональные полицейские силы координируют и обмениваются информацией на таких национальных платформах, как Швейцарская конференция начальников кантональной полиции, Конференция директоров кантональных департаментов правосудия и полиции, Швейцарская сеть безопасности и ново созданная Киберборд, чья роль состоит в осуществлении надзора над кибер нарушениями закона в Швейцарии;
- *Федеральная полиция (Федпол)*: Федпол отвечает за борьбу с организованной преступностью, за координацию отношений с иностранными полицейским и силами, за защиту людей и зданий, находящихся в юрисдикции Швейцарской Конфедерации, и за координацию идентификационных процессов (паспорта, удостоверения самоличности, иммиграция). Что касается киберпреступности, Федпол отвечает за расследование только тех преступлений, которые попадают под юрисдикцию Швейцарской Конфедерации (киберпреступления, связанные с областями ответственности, упомянутые выше);
- *Офис Генерального прокурора Швейцарии*: Генеральный прокурор отвечает за привлечение к ответственности в случаях киберпреступлений, которые попадают под юрисдикцию Швейцарской Конфедерации.

Роль и ответственности разведки: Федеральная разведывательная служба (ФРС) отвечает за контрразведку и атрибуцию, оказывает поддержку критической инфраструктуре, которая является объектом кибератак, борется с терроризмом в киберпространстве и проводит кампании повышения осведомленности о кибер шпионаже. До 2017 года ФРС была ограничена до использования только оборонительных мер в киберпространстве. По новому закону, у ФРС имеется правовой базис для принятия наступательных кибер контрмер против инфраструктур, расположенных вне Швейцарии с разрешением главы МОГЗС, который обязан сначала провести консультации с руководителями ФМИД и ФМПП.[7]

[7] Статья 37 «Федерального закона о разведывательной службе», 25 сентября 2015, https://www.admin.ch/opc/fr/classified-compilation/20120872/index.html#a37.

Роль и ответственности Федерального министерства иностранных дел (ФМИД): Отдел политики безопасности Федерального министерства иностранных дел отвечает за такие дипломатические меры, как участие в международных форумах по нормам кибербезопасности, разработке международных договоров по вопросам кибербезопасности и управлению Интернета.

Реализация политики

Международное сотрудничество: Хотя Швейцария является нейтральной страной, она не отказывается от сотрудничества на двухсторонней или многосторонней основе с другими странами. Швейцария не раз показывала, что понимает, что проблемы кибербезопасности нельзя решить в одиночку. Что касается кибербезопасности, Швейцария, в основном, участвует в международном сотрудничестве через свою разведывательную службу, через вооруженные силы и ФМИД. С 2019 года Швейцария также является партнером с финансовым участием Совместного центра передового опыта по кибер обороне (СЦПОКО) НАТО в Таллине. Это партнерство позволяет Швейцарии иметь доступ к знаниям, информации и подготовке, и принимать участие в разных мероприятиях, предлагаемых СЦПОКО.[8] Швейцария уже принимала участие в таких международных учениях, как Сомкнутые щиты, Скрещенные мечи, Кибер коалиция, Кибер буря и Кибер Европа. Швейцария регулярно взаимодействует и обменивается с другими государствами в плане разведки кибер угроз и в плане опыта.

Через ФМИД Швейцария принимает международное участие в разработке международных кибер норм в таких организациях, как ООН и ОБСЕ. Швейцария принимает участие в Правительственной группе экспертов ООН (ПГЭ ООН) и является председателем Открытой рабочей группы (ОРГ). Швейцария хочет давать свой вклад в дискуссиях по соблюдению и применению международного права в киберпространстве и в установлении доверия между государствами по вопросам кибербезопасности. И наконец, Швейцария пропагандирует себя и Женеву в качестве дискуссионной платформы по проблемам кибербезопасности.

Участие частного сектора / НПО / академических кругов: В 2018, МОГЗС организовало Кампус по кибер обороне (Кампус КО), который должен служить центром для исследований и разработок, связывающим вооруженные силы, академические круги и частный сектор. Кампус КО является частью Armasuisse, Федерального управления военных поставок, расположенного в МОГЗС. Кампус КО создает офисы при ФПШ в Лозанне и ШВТШ в Цюрихе. Цель состоит в том, чтобы быть возможно ближе к стартапам и инновациям,

[8] "Participation au Centre d'excellence pour la cyberdéfense en coopération," May 22, 2019, https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-75145.html.

осуществлять мониторинг новых технологий и талантов, вести исследования и готовить талантов.[9] Кампус КО достигнет своей полной производительности к концу 2020.

МОГЗС также взаимодействует с Швейцарской академией инженерных наук (SATW) для мониторинга проектов исследований и разработок по кибербезопасности в Швейцарии. Кроме того, МОГЗС возлагает разработку исследовательских проектов по техническим и нетехническим темам, связанными с кибербезопасностью, институтам высшего образования.

И наконец, МОГЗС оказывает поддержку таким кибер соревнованиям, как 9/12 Стратегический вызов, организуемым Женевским центром политики безопасности (ЖЦПБ), и Швейцарская кибер буря, для пропаганды сферы кибербезопасности и для нахождения талантов.

Призывная армия: В августе 2018 швейцарские вооруженные силы начали осуществлять программу подготовки по кибер обороне для призывников. Программа квалификации имеет долгосрочную задачу подготовить 600 призывников, чтобы они стали специалистами по кибербезопасности, которые будут интегрированы в батальон по кибер обороне.[10]

Путь вперед

Поскольку проблемы кибербезопасности продолжат быть существенным вызовом для государств, Швейцарии следует продолжать изменения и улучшения, которые были инициированы в последние три года. Последние инициативы и политики Швейцарии, касающиеся кибербезопасности, являются новым и пока еще рано их оценивать и замечать их результаты. Время покажет, помогут ли эти меры Швейцарии встретить вызовы кибербезопасности завтрашнего дня. Однако, недавно предпринятые меры останутся важными для Швейцарии в следующие года. Международное сотрудничество останется существенным из-за трансграничного характера кибербезопасности. Эти проблемы не могут быть решены в одиночку, и поэтому Швейцария продолжит двустороннее и многостороннее сотрудничество. Программа подготовки по кибербезопасности регулярно будет поставлять призывников в будущий батальон по кибер обороне. Эти новые специалисты по кибербезопасности будут способствовать созданию способностей и принесут пользу, на первом месте, швейцарским вооруженным силам, как и всему обществу, когда они вернутся к гражданской жизни. В целом, Швейцария должна сохранить импульс и продолжать выполнение своей стратегии и наращивание своих способностей в гражданских и военных институциях.

---

[9] “Cyber-Defence Campus,” https://www.ar.admin.ch/fr/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html.

[10] “Premières expériences dans le domaine de l’instruction en cybernétique,” https://www.vtg.admin.ch/fr/armee.detail.news.html/vtg-internet/verwaltung/2018/18-09/erste-erfahrungen-mit-dem-cyber-lehrgang-der-armee.html.

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

Мари Бэзнер является исследователем в Группе по кибер обороне Центра изучения вопросов безопасности. У нее степень магистра по международной безопасности, полученная в Университете города Бат, Объединенное Королевство, и степень бакалавра по международным отношениям (политология и международное право), полученная в Университете Женевы. До поступления в ЦИВБ, Мари Бэзнер работала в подразделении по тыловой поддержки командования швейцарских Вооруженных сил и в миротворческой миссии швейцарских Вооруженных сил в Косово. Исследования Мари Бэзнер направлены на изучение кибер инцидентов и кибер аспектов современных конфликтов. E-mail: marie.baezner@sipo.gess.ethz.ch.