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

Санджай Гоэль, *Connections QJ* 19, № 1 (2020): 101-111
https://doi.org/10.11610/Connections.rus.19.1.08

Точки зрения практиков и академических кругов

Как улучшенная атрибуция в кибер войне может способствовать деэскалации гонки кибер вооружений

Санджай Гоэль

Центр информационной криминалистики и обеспечения доступности, целостности и безопасности информации штата Нью-Йорк, Университет Олбани, 1400 Вашингтон авеню, Олбани, NY 12222, https://www.albany.edu/cifa/

Резюме: Средства для ведения кибер войны являются критически важным компонентом военных арсеналов национальных государств, и гонка кибер вооружений началась при отсутствии международных соглашений (норм и мер по укреплению доверия), которые ограничивали бы использование инструментов кибер войны. Одним из существенных препятствий на пути достижения консенсуса по кибер нормам и мерам по укреплению доверия является отсутствие прозрачности при разработке кибер оружий и ненадежная атрибуция исполнителей атак. В последнее время намечается определенное улучшение способностей для атрибуции на основе улучшения сбора данных и профилирования известных хакеров и национальных государств разведывательными ведомствами, и это должно дать импульс усилиям по развитию мер по укреплению доверия и кибер норм. В этой статье рассматривается необходимость и проблемы атрибуции, последние новшества, которые приведут к улучшению атрибуции, и коллективная ответственность национальных государств при разрешении этих проблем. Предлагаются несколько инициатив, направленных на уменьшение вероятности возникновения кибер конфликтов, а также предотвращения эскалации кибер конфликтов, как например дефинирование четких процессов для атрибуции, создание нейтральных органов для анализа инцидентов и ограничение масштаба ответной реакции на основе повышения доверия к атрибуции.

Ключевые слова: кибер война, гонка кибер вооружений, атрибуция, укрепление доверия.

Введение

Преобладание и риск кибер атак продолжают увеличиваться параллельно с растущей зависимостью от Интернета наших систем экономического производства, цепочек поставок и распределения, финансов, энергетики, транспорта и другой критической инфраструктуры. Средства кибер войны становятся следующей серьезной угрозой национальной безопасности,[1] которая может воздействовать не только на жизнь и имущество, но и на финансовые рынки.[2] По информации Центра стратегических и международных исследований (ЦСМИ), общее число кибератак против государственных ведомств, оборонных и высокотехнологичных компаний, или экономические преступления с потерями больше одного миллиона долларов увеличилось от 21 в 2014 до 58 в 2017.[3] Этот список ЦСМИ, составленный на основе только открытых источников, показывает тревожную тенденцию увеличения кибератак, ответственность за которые возлагается на покровительствуемые государством группы, действующие против политических и экономических интересов других государств.

В показаниях перед Комитетом по вооруженным силам США в январе 2017 Джеймс Клаппер, бывший директор Национальной разведки США, заявил, что к концу 2016 более 30 государств развивали способности для наступательных кибератак. Далее он высказал мнение, что «распространение кибер способностей в сочетании с новыми военными технологиями увеличит частоту противостояния и дистанционных операций, особенно на начальных этапах конфликта».[4] Политики предупреждают об опасностях кибер конфликтов и превозносят преимущества кибер мира, а государства начинают рассматривать киберпространство как пятый домен для проведения операций, не менее важный, а в будущем возможно и более важный, чем традиционные домены суши, моря, воздуха и космоса. Военные и разведывательные ведомства государств продолжают осуществлять кибер шпионаж и проводить тайные атаки на компьютерные системы и сети, преследуя политические или военные цели как до начала, так и в ходе конфликтов. Имеет место ограниченная прозрачность в плане того, как государства

---

1 Richard A. Clarke and Robert K. Knake, *Cyberwar: The Next Threat to National Security and What to Do About It* (New York, NY: Harper Collins, 2010).

2 Sanjay Goel and Hany A. Shawky, "Estimating the Market Impact of Security Breach Announcements on Firm Values," *Information & Management* 46, no. 7 (October 2009): 404-410, https://doi.org/10.1016/j.im.2009.06.005.

3 Centre for Strategic and International Studies, "Significant Cyber Incidents Since 2006," 2018, по состоянию на 20 июня 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/180425_Significant_Cyber_Events_List.pdf.

4 James R. Clapper, Marcel Lettre, and Michael S. Rogers, "Joint Statement for the Record to the Senate Armed Services Committee 'Foreign Cyber Threats to the United States'," January 5, 2017, по состоянию на 14 июня 2018, https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

собираются использовать свои кибер способности, поскольку только немногие страны опубликовали свои кибер доктрины и стратегии. Например, по оценкам McAfee, глобальной компании, занимающейся программным обеспечением для компьютерной безопасности, в 2007 году более 120 стран работали над созданием кибер команд,[5] а Dévai перечислила 114 стран, которые к 2013 году развивали гражданские и военные кибер способности, кибер политику, кибер доктрины и организации на разных уровнях готовности или разного предназначения.[6] Учитывая, что многие из официально объявленных «оборонительными» кибер способности легко можно применять и в наступательных кибер операциях, а также и факт, что данные, собранные кибер экспертами, часто основаны только на публично доступной информации, не удивительно, что оценки варьируют, и что действительное состояние готовности кибер оружия и кибер способностей в мировом масштабе сложно установить. Эта высокая степень неопределенности, в сочетание с низкой ценой и легкостью приобретения кибер оружий, многочисленностью и расширяющимся выбором объектов воздействия и множеством видов атак, которые могут оставаться незамеченными в течение длительного времени, способствует преобладающему состоянию кибер небезопасности в международном сообществе. Проблема еще больше усугубляется фактом, что нет общепринятой терминологии критически важных кибер понятий (например, «кибер» или «информационная» безопасность) среди ключевых кибер акторов, что отражается на способности наиболее вероятных стратегических противников найти общий язык в качестве предварительного условия для диалога.

Термин кибер война является широким понятием, которое относится к действиям государственных акторов (или других международных организаций с *mala fide* (недобросовестными) намерениями) с использованием хакерских инструментов для достижения военных целей в другом государстве. Инструменты для взлома разнообразны, и в их число могут входить вредоносное программное обеспечение, атаки типа «отказ в обслуживании», социальная инженерия, фейковые новости и злонамеренные инсайдеры, а также инструменты для маскировки личности хакеров или неправильного указания авторства. Цели могут быть тактическими или стратегическими. Тактическими целями могут быть деградация боевых способностей противника или способностей разрабатывать вооружения (например, Stuxnet), или шпионаж для сбора разведданных. Стратегическими целями могут быть использование мягкой силы, пропаганды для оказания влияния

---

[5] Arie J. Schaap, "Cyber Warfare Operations: Development and Use Under International Law," *Air Force Law Review* 64 (2009): 121-173.

[6] Dóra Dévai, "Proliferation of Offensive Cyber Weapons. Strategic Implications and Non-Proliferation Assumptions," *Academic and Applied Research in Military and Public Management Science (AARMS)* 15, no. 1 (2016): 61-73, https://folyoiratok.uni-nke.hu/document/uni-nke-hu/aarms-2016-1-devai.original.pdf.

на общественное мнение, направленное на смену режима или на изменение политического результата выборов, или использование жесткой силы путем внедрения спящих вредоносных программ в системы критической инфраструктуры с целью использовать их во время конфликта.

Граница между конвенциональной и кибер войной становится размытой, поскольку конвенциональные оборонительные и наступательные способности во все большей степени используют Интернет для командования, управления, коммуникаций и разведки, делая информационные и коммуникационные инфраструктуры и сети одновременно мишенями и средствами военных ударов. В то же время Интернет стал коммуникационным хребтом, необходимым для функционирования современных обществ и экономических систем. Поэтому характер и средства вооруженной защиты этих систем тоже должны измениться и стать более гибкими, чтобы соответствовать появляющимся угрозам. Прежде всего, формирующийся механизм кибер защиты любого государства должен быть в состоянии дать национальному политическому руководству ответы на некоторые критические вопросы: Кто является источником кибератаки; откуда она пришла? Кто несет ответственность за нее? Каков рекомендуемый курс действий или ответ?

Атрибуция

Определение авторства кибератак очень важно, особенно для оправдания ответных действий против исполнителей и предотвращения случайной реакции против невинных мишеней. Вся область кибер норм и мер по укреплению доверия сфокусирована на видимости, т.е. способности установить исполнителей атак и узнать силу противника. При отсутствии такой верификации остается сомнение, национальные государства начинают предполагать самое худшее и готовят себя созданием все более могущественных арсеналов для поддержания стратегического равновесия.

Анонимность часто считается ключевым фундаментальным принципом Интернета, порожденным необходимостью защитить идентичность пользователя и отделить действия потребителей от их идентичности.[7] Такая анонимность гарантирует возможность говорить свободно без страха возмездия, что может быть полезно в политических комментариях, при обсуждении спорных вопросов, при задавании личных вопросов, при изучении соперников и при покупке товаров или услуг, не раскрывая персональные предпочтения. Защитники конфиденциальности сделали многое для защиты анонимности пользователей, обеспечивая такие сервисы, как ремейлеры и шифрование, которые еще больше маскируют идентичность пользователей и защищают их от наблюдения со стороны государства. Однако,

[7] Barry M. Leiner et. al, "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review* 39, no. 5 (October 2009): 22-31, https://doi.org/10.1145/1629607.1629613.

хотя анонимность полезна в некоторых контекстах и обстоятельствах, она также скрывает и совершителей преступлений и терроризма в Интернете.[8] Плащ анонимности защищает и позволяет действовать людям, занимающимся отмыванием денег, вымогательством, шпионажем и воровством. Подобным образом акторы, участвующие в кибер войне, используют анонимность в Интернете для ведения наблюдения, зондирования и совершения атак без привлечения внимания к своим действиям. Для гарантирования права людей на конфиденциальность и безопасность нужно обеспечить баланс между анонимностью и безопасностью.[9]

Криминология и атрибуция

Несмотря на присущую Интернету анонимность, пользователи оставляют следы своей деятельности по пути. Эти следы могут дать ценную информацию, которая раскрывает идентичность авторов атак и их возможной мотивации. Целью дигитальной криминологии является сбор этих следов, соединение точек и вывод заключений об инциденте, включая идентификацию исполнителей, определение механизма операции и каталогизации компрометированной или измененной информации. Инструменты, процессы и знания для цифровой криминологии свободно доступны. Тем не менее, анонимность Интернета делает такой анализ затруднительным, особенно в случае кибер войны, когда информация об атаке спрятана за межсетевыми перегородками страны и защищена спонсорами атаки.

Цифровая криминалистика может снять часть анонимности Интернета и сузить поле авторов атак путем складывания этих кусочков информации и создания цепочки свидетельств, которые могут связать исполнителей с инцидентом.[10] Такая цепочка свидетельств может не составить неоспоримое доказательство в суде. Тем не менее, в сочетании с такой дополнительной информацией как юридические, политические, разведывательные и концептуальные соображения, конечная оценка может позволить политикам выработать национальную реакцию на кибератаки. В плане национальной безопасности, как утверждает Хийли, знать, «кому предъявить обвинение», может быть более важным, чем знать «кто сделал это?».[11] Правильный ответ на этот вопрос дает национальным властям возможность оценить ситуацию в ходе развивающегося конфликта и взвесить возможные реакции из

---

[8] Helen L. Armstrong and Patrick J. Forde, “Internet Anonymity Practices in Computer Crime,” *Information Management and Computer Security* 11, no. 5 (2003): 209-215, https://doi.org/10.1108/09685220310500117.

[9] Sanjay Goel, “Anonymity vs. Security: The Right Balance for the Smart Grid,” *Communications of the Association for Information Systems* 36, Article 2 (January 2015): 23-32, https://doi.org/10.17705/1CAIS.03602.

[10] Sanjay Goel, “Cyberwarfare: Connecting the Dots in Cyber Intelligence,” *Communications of the ACM* 54, no. 8 (August 2011): 132-140, DOI: 10.1145/1978542.1978569.

[11] Jason Healey, “Beyond Attribution: Seeking National Responsibility for Cyber Attacks,” *Atlantic Council*, January Issue Brief 2012, https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF.

набора экономических, дипломатических или других средств, находящихся в их распоряжении. Эта многомерная проблема, для решения которой нужна информация из всех наличных источников, включая техническую криминалистику, агентурную и техническую разведку, исторические прецеденты и геополитику, атрибуция атак государственному актору требует по-настоящему национальных усилий и развития соответствующих технических и нетехнических способностей. Именно через эти процессы сбора и обмена информацией, анализа и сотрудничества, осуществляемых на национальном и международном уровнях, цифровая криминалистика становится полезной при операционализации и практическом развитии устойчивого режима мер по укреплению доверия (МУД).

Инструменты и технологии кибератак одинаковы для «кибер войны», «кибер терроризма» и «кибер активизма». Только анализируя акторов, способы действий и мотивацию атак и их предполагаемые или демонстрированные мишени, можно отнести их к одной из трех категорий. В отличие от конвенциональных военных действий, очень сложно отличить являются ли авторами атаки на вебсайт или онлайн кражи данных субъекты в другом государстве, мотивом которых является финансовая выгода, политическая или религиозная идеология, или эти действия были предприняты государственным разведывательным ведомством или военными (или их прокси). Поскольку государства могут осуществлять кибератаки через прокси в других государствах, сложности атрибуции усугубляются и становятся фундаментальными проблемами как во время конфликта, так и в мирное время, когда имеют место международное сотрудничество и верификация соблюдения договоров.

Цифровая криминалистика включает сбор данных, зарегистрированных на разных устройствах, включая компьютеры, маршрутизаторы, промышленные электронные системы управления и мобильные устройства,[12,13,14] выстраивание их в одну временную линию и выведение заключений для определения анатомии атаки/вторжения. Для прослеживания действий лиц или устройств можно использовать разные кусочки соответствующей информации, включая IP-адреса, имена доменов, и метки времени.[15] Эти индивидуальные записи в разных лог-файлах могут быть скорреллированы

[12] Rizwan Ahmed and Rajiv V. Dharaskar, “Mobile Forensics: An Overview, Tools, Future Trends and Challenges from Law Enforcement Perspective,” in *6th International Conference on E-Governance, ICEG, Emerging Technologies in E-Government, M-Government* (2008), 312-23.

[13] Terrence V. Lillard, Clint P. Garrison, Craig A. Schiller, and James Steele, *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data* (Syngress Publishing, 2010).

[14] Michael G. Solomon, K. Rudolph, Ed Tittel, Neil Broom, and Diane Barrett, *Computer Forensics Jumpstart* (Indianapolis, IN: Wiley Publishing Inc., February 2011).

[15] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Boston, MA: Academic Press, May 2011).

по времени для создания цепочки доказательств и демонстрации активности, исходящей от конкретного источника.

Не менее важным измерением цифровой криминалистики является обнаружение вторжения и пост-инцидентный анализ, при котором расследующим нужно понять, как была реализована атака, что было украдено, повреждено или изменено, и как предотвратить повторение подобных атак в будущем.[16] Это требует анализа внутренних лог-файлов акторов, имевших отношение к атаке, и сложение в единую временную цепь событий свидетельств из множества источников. Доказательства можно собирать с твердых дисков, RAM, USB-накопителей, устройств для сохранения данных и сетевых устройств. Фундаментальной проблемой такого анализа является сам объем данных. Кроме того, чтобы делать криминологический анализ данных из прошлого, они должны быть сохранены. Ограничения объема сохраняемых данных, в особенности данных сетевых устройств, которые генерируют огромное количество данных, также ограничивает временные рамки анализа.[17] Другой полезной криминологической технологией является анализ социальных сетей, как и анализ текстов из социальных медиа с целью идентифицировать действия, характерные для кибер войны, пропаганду, вербовку террористов или обмен информацией. Часть этого анализа производится вручную, но большая часть осуществляется с использованием автоматических инструментов, которые могут процеживать огромные объемы текста для того, чтобы выявить данные, анализ которых должен делать человек. Лингвистические инструменты, которые используются для анализа текстов, стали намного более совершенными за последнее десятилетие, они развились от простого подсчета слов до выделения частей речи и ограниченного понимания языка. Эти криминологические инструменты могут способствовать разрешению проблем атрибуции и обеспечивают возможность решения спорных вопросов, связанных с установлением авторства и уклонением от ответственности.

Криминологические методы хорошо отработаны, и имеются в наличии инструменты для быстрого анализа данных и получения заключений. Данные для анализа можно получать от устройств и сетей в организациях и поставщиков интернет услуг (интернет сервис провайдеров – ИСП). Однако, имеются фундаментальные проблемы, связанные с криминологическим анализом и сбором данных, которые пересекают международные границы и выходят за юрисдикцию национального государства. Во-первых, большая часть данных хранится на маршрутизаторах и устройствах ИСП, которые подчиняются местным законам. Данные могут быть разбросаны по многим источникам в сети и их нужно получить до начала анализа. Если данные не

---

[16] N.K. McCarthy, *The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk* (McGraw-Hill Osborne Media, August 2012).

[17] José Camacho, “Visualizing Big Data with Compressed Score Plots: Approach and Research Challenges,” *Chemometrics and Intelligent Laboratory Systems* 135 (July 2014): 110-125, https://doi.org/10.1016/j.chemolab.2014.04.011.

будут взяты непосредственно после инцидента, на них могут быть перезаписаны новые данные. Поэтому криминологической работе могут помешать административные задержки. Кроме того, если в проведении атаки замешано государство, достоверность данных может быть под вопросом. Данные могут быть изменены, адаптированы или полностью подделаны. Во-вторых, получение физического доступа к компьютерам исполнителей атак предполагает такой уровень сотрудничества между странами, который возможен в отношении уголовных преступлений, но будет ограничен или полностью отсутствующим в случае кибер войны. В-третьих, все данные могут быть сфальсифицированы, т.е. в информационных пакетах может быть использован ненастоящий адрес отправителя для того, чтобы скрыть реальные IP-адреса, что делает проблему идентификации еще более трудной. И наконец, замаскировать исполнителей может использование анонимизированных инструментов, что еще более усложняет атрибуцию.

Все эти проблемы делают техническую атрибуцию для международных кибер инцидентов трудной, хотя и не невозможной. Она возможна и драматически улучшилась за последние несколько лет в результате постоянной разведывательной работы. В дополнение к данным, получаемым напрямую от ИСП и организаций, данные можно собирать путем использования «горшочков с медом» и предварительно установленных ответвителей данных в глобальных сетях. Разведывательные ведомства непрерывно осуществляют мониторинг деятельности известных акторов (в том числе национальные государства). Они составляют разведывательные досье, которые можно связывать с информацией, полученной в результате цифровой криминологической работы для получения более определенной атрибуции.

Знания о предшествующих событиях, об инструментах и техниках известных акторов можно использовать для прослеживания источников атак. Не существует автоматизированного процесса анализа; наоборот, аналитики скрупулезно оценивают доказательства и делают вероятностные предположения об определении авторства. Существуют разные уровни атрибуции, с каждым следующим уровнем атрибуция или определение источника (национальное государство, хакерская группа), конкретного устройства (компьютер, использованный для осуществления атаки) и лица, ответственного за совершение атаки, становятся более трудными. Еще более трудно определить спонсора атаки в случаях, когда хакер/группа работают как прокси.

Дискуссия

У цифровой криминологии есть свои ограничения. Эти инструменты работают только в той степени, в которой имеется политическая воля для международного сотрудничества в обмене и анализе информации. Первым важным шагом может стать установление горячих линий и расположение в стратегических местах устройств для сбора стандартной информации, работу которых невозможно искажать. Они могут быть фундаментом для обеспечения криминологического анализа кибер атак и международного

определения случаев использования средств кибер войны. Нужно создать и разместить в нейтральной стране международный орган для мониторинга и оценки кибер конфликтов с участием наблюдателей из воюющих сторон. Такой орган был бы в состоянии быстро требовать доступа к данным из разных источников; длительные процедуры могут замедлять и ограничивать сбор данных, которые могут быть эфемерными. Такой орган будет располагать технической квалификацией для анализа больших объемов данных, определения атрибуции и конфиденциальной работы с разведывательной информацией, не раскрывая ее источники.

Практики цифровой криминологии были разработаны для эффективного сочетания отдельных доказательств в случаях, когда: цифровой след небольшой; имеется физический доступ к устройствам и исполнители атак относительно неопытны в технологиях маскировки. Случай, когда атаки осуществляются хорошо квалифицированными профессиональными хакерами, является весьма редким сценарием. В результате этого, разведывательные ведомства уже адаптировали и масштабировали криминологические процедуры для кибер атак, осуществляемых национальным государством; большинство таких практик все еще не находятся в публичном домене. Нам нужно создать стандартные криминологические процедуры (доступные публично) для расследования трансграничных атак, при которых используются техники маскировки. Кроме того, цифровая криминология постоянно отстает от бурного темпа технологической эволюции как в плане приложений и устройств, так и в плане объема данных.[18] Чтобы стать надежным фактором атрибуции деятельности, связанной с кибер войной, цифровой криминологии в следующие года нужно быть в состоянии бороться с исключительно большими объемами данных, а также с изощренными технологиями маскировки, которые используются в кибер войне. Чтобы мы не сбивались с курса, нам нужен международный криминологический исследовательский институт для изучения и актуализации криминологических методов по мере развития информационной инфраструктуры (например, связанные транспортные средства, вживляемые устройства, автономные автомобили). Нам нужно начать готовить в каждой стране экспертов по лучшим практикам (инструменты и технологии) в сфере цифровой криминологии так, чтобы они смогли вести собственные исследования.

Мы должны понимать, что атрибуция может не всегда быть совершенной из-за преднамеренного введения в заблуждение или из-за ограничений самого анализа. Это иллюстрируется атакой на Sony Pictures Entertainment в ноябре 2014. Хакерская группа, называющая себя «Стражами мира», раскрыла в Интернете конфиденциальные данные Sony, включая личные данные сотрудников, огромные файлы с электронными письмами и паролями, внутренние документы и внутренние коммуникации, невыпущенные

[18] Simson L. Garfinkel, “Digital Forensics Research: The Next 10 Years,” *Digital Investigation* 7, Supplement (August 2010): S64-S73, https://doi.org/10.1016/j.diin.2010.05.009.

еще фильмы и многое другое. Есть две противоположные теории атрибуции: одна предполагает, что за атакой стояло правительство Северной Кореи, учитывая подобие вредоносных программ, которые использовались в предыдущих атаках северокорейцев;[19] другая, на основе лингвистического анализа, предполагает, что атака была проведена русскими.[20] Нет никаких решающих доказательств, поддерживающих одну из теорий, только косвенные свидетельства, основанные на конвенциональной триаде средств, мотивов и возможности. Чтобы решить эту проблему, мы должны опираться на вероятностный подход и дефинировать стандарты атрибуции, основанные на уровнях достоверности атрибуции и на допустимую реакцию для предотвращения непропорционального ответа, эскалирующего в кинетический конфликт.

Демилитаризация киберпространства или мораторий на разработку кибер оружий уже невозможны. Однако, национальные государства должны собраться, чтобы найти общую основу в кибер войне, начиная с мер по укреплению доверия, норм поведения и применимости международного права для снижения вероятности большого катастрофического инцидента. Формальный обмен информации (КГРЧС и на дипломатических уровнях) и создание горячих линий поможет деэскалировать будущие кибер инциденты. Нужно достичь консенсуса в Организации Объединенных Наций и других существующих международных органах, например Организации по сотрудничеству и безопасности в Европе (ОБСЕ), для нахождения путей к созданию консенсуса между национальными государствами по предотвращению кибер конфликтов и по укреплению доверия.

Выводы

Интернет является основной экономической и социальной движущей силой и инструментом распространения знаний с огромными экономическими, политическими и связанными с национальной безопасностью последствиями. Но он также является местом краж данных, шпионажа, фейковых новостей, политического воздействия и пропаганды, как показывают события на Ближнем Востоке, в Южной Азии и в Европе. Атаки, осуществляемые национальными государствами, постоянно разрастаются как в плане частоты, так и в плане изощренности. Такие атаки подрывают влияние Интернета в качестве социального клея и уменьшают его влияние на экономическое процветание. Были сделаны попытки канализировать эскалацию методов ведения кибер войны; однако, очень трудно добиться консенсуса между национальными государствами по механизмам де-эскалации кибер войны. Отсутствие прозрачности в разработке кибер вооружений и атрибуции кибератак является критически важным барьером для принятия мер по

[19] Kim Zetter, “Sony Got Hacked Hard: What We Know and Don’t Know So Far,” *Wired*, March 12, 2014, https://www.wired.com/2014/12/sony-hack-what-we-know.

[20] Zetter, ‘’Sony Got Hacked Hard.”

укреплению доверия. Улучшение сбора данных (разведка) и возможностей криминологического анализа повышают наши способности для атрибуции кибер инцидентов. Добиваясь консенсуса между национальными государствами по протоколам и процедурам атрибуции и по выяснению применимости международного права, мы можем начать достигать консенсуса по МУД и нормам, сделать Интернет более безопасным и позволить ему процветать. В этой работе предложено несколько инициатив, направленных на снижение вероятности кибер конфликта и на предотвращение эскалации кибер конфликтов, например дефинирование четких процессов атрибуции, создание нейтральных органов для анализа инцидентов и ограничения масштаба реакции на основе доверия к атрибуции.

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.

Признательность

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

Об авторе

Смотри стр. 100 настоящего номера,
https://doi.org/10.11610/Connections.rus.19.1.07.