ЛЕТНЯЯ ШКОЛА
по управлению интернетом

Болданова Дарья

Асимметрия возможностей в кибератрибуции и управление международными киберкризисами

Введение и обоснование актуальности выбранной темы

27 июня 2017 года мир столкнулся с одной из самых разрушительных кибератак в истории – вирусом-шифровальщиком NotPetya, который парализовал работу государственных органов и компаний в Украине, а затем распространился на глобальные корпорации, включая Maersk, Merck и FedEx, ущерб составил более 10 млрд долларов США [1]. Уже в феврале следующего года правительства США, Великобритании, Австралии и ряда союзников публично обвинили Россию в организации атаки [2]. Однако Украина, несмотря на то что стала первичной и наиболее пострадавшей стороной, не сделала публичного обвинения, полагаясь на заявления союзников. Это отражает более широкий феномен, когда государства с разным уровнем ресурсов обладают неравной способностью влиять на международный нарратив атрибуции. То есть, атрибуция кибератак является не только техническим, но и политическим процессом, зависящим от распределения возможностей между государствами [3].

Тут также важно различать внутреннюю (техническую и операционную) атрибуцию, когда государство для себя определяет вероятного виновника атаки, и публичную атрибуцию – официальные обвинения на международной арене. В этом эссе основной интерес представляет прежде всего публичная атрибуция как политический процесс, но её анализ невозможен без рассмотрения технического и операционного уровня, которые формируют основу для публичных заявлений.

Из-за сочетания технических, политических и правовых аспектов, каждый из которых сопряжен с неопределенностью, проблема кибератрибуции давно признана одним из ключевых вызовов международной безопасности [4]. False flags, использование прокси-групп и разрыв во времени между атакой и выявлением исполнителей усложняют процесс, а в условиях кризиса сокращённые сроки принятия решений повышают риск ошибочной эскалации [6, с. 155].

Асимметрия возможностей между государствами в киберпространстве усиливает эти риски. Инфраструктурно развитые государства обладают доступом к глобальным разведывательным сетям, высокотехнологичным средствам киберфорензики и влиятельными дипломатическими каналами, тогда как страны с еще несозревшей инфраструктурой вынуждены опираться на внешние оценки или вовсе остаются без поддержки, что создаёт «неравенство в способности влиять на международный нарратив атрибуции» [3, с. 6].

В этом эссе я хочу показать, как асимметрия возможностей в кибератрибуции влияет на управление международными киберкризисами и какие меры могут минимизировать риски эскалации в подобных ситуациях.

Разбор составляющих проблемы

Техническая неопределённость

Атрибуция кибератак представляет собой многоуровневый процесс, включающий технический, операционный и стратегический этапы [3, с. 6]. На техническом уровне проводится анализ цифровых артефактов: IP-адресов, доменных имён, сигнатур вредоносного кода, временных меток, инфраструктуры командных серверов (command-and-

control, C2). Однако такие данные подвержены манипуляциям, атакующие часто используют маршрутизацию через скомпрометированные узлы в третьих странах, VPN-сервисы и анонимизаторы для сокрытия реального происхождения трафика [6, с. 22-24]. Ещё одной проблемой является повторное использование вредоносного кода или его фрагментов, что затрудняет определение авторства: одни и те же программные элементы могут встречаться как в атаках, проводимых государственными группами, так и в операциях киберпреступников [7, с. 46]. Кроме того, существуют false flag операции, когда злоумышленники намеренно оставляют ложные цифровые следы, имитирующие почерк другого актора, с целью ввести в заблуждение расследователей [6, с. 23].

В условиях киберкризиса государства часто вынуждены принимать решения об атрибуции в сжатые сроки, до завершения комплексного расследования, что повышает риск ошибочных обвинений и непреднамеренной эскалации [3, с. 7]. Эта проблема усугубляется тем, что доступ к техническим, разведывательным и аналитическим ресурсам распределён крайне неравномерно, потому способность государств собирать убедительную доказательную базу сильно различается, и многие вынуждены привлекать внешних партнёров или частные компании для поддержки. Особенно остро это проявляется на этапе публичной атрибуции, когда предварительные технические выводы становятся основой для дипломатических обвинений.

Асимметрия возможностей

Государства с более развитой разведывательной инфраструктурой, такие как США или Великобритания, располагают глобальными системами радиоэлектронной разведки (SIGINT), доступом к массивам перехваченных данных и партнёрскими связями с крупнейшими частными компаниями, специализирующимися на киберфорензике (Microsoft, Mandiant, CrowdStrike) [7, с. 50]. Они способны быстро интегрировать разведывательные данные с результатами технического анализа, а также мобилизовать дипломатические каналы для координированного публичного обвинения и формирования международной коалиции [5, с. 32]. В противоположность этому, менее инфраструктурно снаряженные государства часто не имеют доступа к подобным ресурсам и зависят от внешней поддержки как в технической, так и в политической части атрибуции.

Такая зависимость создаёт уязвимость, при которой их инциденты могут быть проигнорированы или недостаточно приоритезированы, если они не соответствуют интересам союзников [3, с. 7]. Обратная сторона асимметрии, государства с глобальным влиянием формируют политически выгодный нарратив атрибуции, особенно в отношении маргинализированных в международной системе государств, таких как Иран, КНДР, Китай и Россия [6, с. 52].

Уязвимость “сильных”

Парадокс кибербезопасности еще заключается в том, что государства с более развитой цифровой инфраструктурой, обладая значительными возможностями по атрибуции атак, одновременно оказываются и более уязвимыми целями. Чем более цифрово-интегрировано общество, тем шире его критическая инфраструктура, подверженная кибератакам: энергетические сети, транспортные системы, финансовые платформы, цепочки поставок [7, с. 53]. Эта уязвимость усиливается взаимозависимостью сетей, ведь атака на одного крупного игрока может вызвать цепной эффект в экономике и безопасности партнёров [5, с. 33]. Иными словами, государства учитывают не только репутационные, но и прямые риски. Публичное обвинение может спровоцировать симметричные или асимметричные ответные кибератаки. Например, в случае с атакой на цепочку поставок SolarWinds в 2020 году, несмотря на приписывание ответственности России, США предприняли ограниченный набор ответных шагов, учитывая риск эскалации

и возможность зеркальных атак на собственные сети [8]. Таким образом, инфраструктурная мощь, обеспечивающая лидерство в киберпространстве, одновременно становится источником стратегической уязвимости.

Рекомендации по решению проблемы

Описанные выше проблемы кибератрибуции проявляются во взаимодействии трёх ключевых акторов: государства-таргета атаки, государств с широким доступом к ресурсам и международной аудитории. Каждый из них действует, исходя не только из собственных интересов, но и из того, как на его шаги отреагируют другие стороны. Такая взаимозависимость превращает атрибуцию в стратегический процесс, который можно сравнить с игрой с неполной информацией: у участников есть разные наборы данных, они по-разному оценивают риски, но их решения напрямую влияют друг на друга.

На этом этапе различие между внутренней и публичной атрибуцией становится особенно заметным, даже если государство способно технически установить источник атаки, оно может колебаться, стоит ли превращать это знание в официальное обвинение. На практике это проявляется так. После киберинцидента государство-объект атаки решает, проводить ли расследование и публиковать ли его результаты. Государств с более широким доступом к ресурсам выбирают между тем, чтобы публично обвинить предполагаемого противника или воздержаться от заявлений. Международная аудитория формирует своё мнение на основе доступных технических данных, дипломатических заявлений и независимых источников информации.

Проблема состоит в том, что у государств-таргетов обычно меньше возможностей собрать убедительные данные, тогда как более ресурсные государства располагают глобальными системами разведки, мощной аналитической базой и дипломатическим влиянием. В таких условиях именно позиции наиболее ресурсных игроков часто оказывают решающее влияние на нарратив, в то время как сигналы других могут теряться на фоне. Однако при наличии независимых механизмов проверки даже небольшие акторы могли бы получить возможность укрепить свою убедительность.

Ситуация начинает меняться, если у государства-таргета появляется возможность собирать более убедительные доказательства либо если действуют механизмы независимой проверки информации. Тогда международная аудитория воспринимает его аргументы более серьёзно, и пространство для произвольных или политически мотивированных обвинений сокращается. Иначе говоря, когда появляются независимые механизмы проверки информации, ресурсные государства уже не могут рассчитывать на то, что их обвинения примут “на веру”. Им приходится подробнее обосновывать свои выводы, а пространство для политически мотивированных заявлений сокращается.

Для ресурсных государств дополнительным сдерживающим фактором служит их собственная уязвимость. Чем более цифрово интегрировано государство, тем выше потенциальный ущерб от ответных кибератак или других мер давления. Осознание этой уязвимости делает ведущие их осторожнее. Они не спешат с публичными обвинениями, особенно если существует риск опровержения или репутационных потерь.

У разных акторов есть собственные стимулы поддерживать развитие прозрачных процедур. Для государств-таргетов – это шанс повысить убедительность своих сигналов и снизить зависимость от ресурсных государств. Для ресурсных государств стимулами являются возможность уменьшить репутационные риски и вероятность ответных атак, если их обвинения окажутся спорными. Для международных организаций и коалиций союзников предоставляется способ укрепить свою роль арбитра и снизить вероятность неконтролируемой эскалации.

Совокупно эти интересы создают основу для реализации следующих шагов:

– снижение издержек расследования для таргетов через финансирование, обучение специалистов и доступ к частным экспертным фирмам,

– повышение качества локальных сигналов посредством совместных лабораторий и обмена аналитическими данными,

– введение стандартов раскрытия и форматов сообщений, ограничивающих стратегические манёвры в интерпретации данных,

– создание многосторонних коалиционных механизмов верификации, повышающих вероятность выявления несоответствий и распределяющих репутационные риски,

– использование публичных метрик точности атрибуции, увеличивающих издержки для ложных заявлений,

– согласование пороговых правил для публичных обвинений, предполагающих минимальный объём проверенных доказательств перед их обнародованием.

Эти меры способны сместить баланс от доминирования политически и инфраструктурно ресурсных игроков к модели, где ключевое значение имеют проверяемые факты и сопоставимые процедуры оценки. Стоит указать, что конкретизация исполнителей, будь то международные организации, региональные объединения, частные фирмы или исследовательские центры, требует более детального политического и институционального анализа, который следует выделить в отдельном исследовании.

Итоговые выводы

Кейс NotPetya показал, что отсутствие у пострадавшей стороны достаточных технических и дипломатических ресурсов для самостоятельной атрибуции создаёт зависимость от внешних акторов и позволяет ресурсным государствам формировать доминирующий нарратив. В 2017 году Украина не выступила с самостоятельным публичным обвинением, полагаясь на заявления США, Великобритании и их союзников, которые и определили восприятие атаки в международном информационном пространстве.

Из предложенных в этом эссе мер сразу несколько могли бы изменить динамику кризиса: снижение издержек расследования и расширение доступа Украины к частным киберфорензик-компаниям повысили бы информативность локальных данных; многосторонняя верификация позволила бы аудитории получить независимое подтверждение выводов; а обязательные стандарты раскрытия обеспечили бы сопоставимость доказательств, представленных разными странами.

Эти механизмы одновременно повышают убедительность сигналов государств с ограниченными ресурсами и сдерживают избыточное доминирование более ресурсных государств. Развитие коалиционных процедур верификации и повышение репутационных издержек за ложные обвинения сокращают пространство для политически мотивированных интерпретаций. Для технологически развитых стран это снижает риск ответных атак на собственную инфраструктуру и повышает устойчивость международной системы к непреднамеренной эскалации.

Таким образом, проблема кибератрибуции заключается не только в технической неопределённости, но и в неравенстве возможностей государств формировать международный нарратив. Меры по институционализации прозрачных процедур способны сместить акцент с политического веса отдельных акторов на проверяемость данных и сопоставимость оценок. Это делает публичную атрибуцию менее зависимой от асимметрии ресурсов и более надёжным инструментом предотвращения эскалации киберкризисов.

Список использованных источников

1. UK and US blame Russia for “malicious” NotPetya cyber-attack [Великобритания и США обвиняют Россию в «злонамеренной» кибератаке NotPetya]. – 2018. – 15 февраля. – URL: https://www.bbc.com/news/uk-43064885 (дата обращения: 14.08.2025).

2. Foreign Office Minister condemns Russia for NotPetya attacks [Министр иностранных дел Великобритании осуждает Россию за атаки NotPetya]. – URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (дата обращения: 14.08.2025).

3. Rid, T., Buchanan, B. Attributing Cyber Attacks [Атрибуция кибератак] // Journal of Strategic Studies [Журнал стратегических исследований]. – 2015. – Т. 38, № 1–2. – С. 4–37.

4. Foulon, M., Meibauer, G. How cyberspace affects international relations: The promise of structural modifiers [Как киберпространство влияет на международные отношения: потенциал структурных модификаторов] // Contemporary Security Policy [Современная политика безопасности]. – 2024. – Т. 45, № 3. – С. 426–458.

5. Maesschalck, S. Gentlemen, you can’t fight in here. Or can you?: How cyberspace operations impact international security [Джентльмены, здесь нельзя драться. Или можно?: как операции в киберпространстве влияют на международную безопасность] // Journal of Cyber Policy [Журнал киберполитики]. – 2024. – Т. 9, № 2. – С. 22-36

6. Maurer, T. Cyber Mercenaries: The State, Hackers, and Power [Кибернаёмники: государство, хакеры и власть]. – Cambridge: Cambridge University Press, 2018. – С. 3–157.

7. Nye, J. S. Jr. Deterrence and Dissuasion in Cyberspace [Сдерживание и разубеждение в киберпространстве] // International Security [Международная безопасность]. – 2017. – Т. 41, № 3. – С. 44–71.

8. Paul, K. SolarWinds hack was work of “at least 1,000 engineers”, tech executives tell Senate [Взлом SolarWinds был работой «по меньшей мере 1000 инженеров», заявили технологические руководители Сенату] // The Guardian [Гардиан]. – 2021. – 24 февраля. – URL: https://www.theguardian.com/technology/2021/feb/24/solarwinds-hack-senate-hearing (дата обращения: 14.08.2025).

9. Li, Y., Yang, Z. Games with incomplete information and uncertain payoff: from the perspective of uncertainty theory [Игры с неполной информацией и неопределённым выигрышем: с точки зрения теории неопределённости] // Soft Computing [Мягкие вычисления]. – 2019. – Т. 23, № 24. – С. 13669-13678