УДК 34

О ПРЕДОТВРАЩЕНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С МОШЕННИЧЕСТВОМ В СФЕРЕ ТЕЛЕКОММУНИКАЦИЙ, С ТОЧКИ ЗРЕНИЯ КРИМИНОЛОГИИ

Чжан Байцюань, *Хэйлунцзянский институт профессиональной подготовки милиции общественной безопасности, Факультет ОРД*

Вслед за непрерывным развитием общества и научно-техническим прогрессом, появляются новые тенденции развития преступной деятельности и новые особенности преступлений, связанных с мошенничеством в сфере телекоммуникаций, что является серьезным вызовом для органов общественной безопасности. Необходимо постоянно изучать и анализировать вопросы расследования таких дел. Исследование подобных видов преступлений неотделимо от криминологии. В данной статье обсуждаются способы предотвращения преступлений, связанных с мошенничеством в сфере телекоммуникаций с точки зрения теории криминологии.

Ключевые слова: преступления, связанные с мошенничеством в сфере телекоммуникаций, криминология, предотвращение преступлений, расследование

Мошенничество в сфере телекоммуникаций является наиболее часто встречающимся и распространенным уголовным преступлением. Подозреваемые в совершении таких преступлений посягают на законные интересы государства, общества и отдельно взятых граждан, нарушают общественный порядок и оказывают влияние на чувство защищенности граждан. В последние годы, вслед за быстрым развитием технологий, популяризации интернета и умных мобильных устройств, подозреваемые в совершении уголовных преступлений также не стоят на месте и повышают свои способности противостоять следствию. Именно из-за возникновения новых особенностей и тенденций, органам общественной безопасности приходится вкладывать больше сил в проведение интеллектуального анализа и суждений, привлекать дополнительные ресурсы и материальные средства для упреждающего выявления преступных действий, изучения организационной структуры преступных группировок, сбора улик, задержания подозреваемых в совершении преступных действий. Это является серьезной проблемой для следственных органов общественной безопасности. Следовательно, с точки зрения борьбы с уголовными преступлениями, связанными

с мошенничеством в сфере телекоммуникаций, будь то с точки зрения экономии судебных издержек или снижения степени ущерба, понесенного потерпевшим, предотвращение преступления намного лучше, чем борьба с ним.

Основным содержанием криминологических исследований всегда выступают причины совершения преступных действий и меры их предупреждения, поэтому при изучении способов борьбы с преступлениями, связанными с мошенничеством в сфере телекоммуникаций, необходимо исследовать их с точки зрения криминологии. Традиционные теории криминологии, такие как теория рационального выбора и теория повседневного поведения могут помочь найти новые идеи по предупреждению преступности и борьбе с ней, основанные на современной ситуации в сфере преступлений, связанных с телекоммуникационным мошенничеством.

1. Особенности преступлений в сфере телекоммуникаций

(1) Преступники демонстрируют профессионализм и способность организовываться в группы

Для того, чтобы диверсифицировать риски и избежать преследований, преступники часто организуют группировки, заранее панируя и координируя свои действия, обеспечивают сбыт краденного сразу после завершения дела. Четкое разделение труда и организационная структура обеспечивают возможность непрерывно и многократно совершать преступные действия. Такая тенденция особенно четко прослеживается в последние годы. Мелкие преступные группировки организуются в профессиональные преступные сообщества, которые имеют четкую структуру, состоящую из информационной группы, технической группы, операционной группы, учебной группы, группы по отмыванию денег, группы, ответственной за тыл и т. д. Что касается способов вербовки преступников, то они тоже изменились, уже не используются родственные или соседские связи. Преступники открыто вербуются в сети интернет как операционные сотрудники, проходят обучение мошенническим навыкам и опыту избежания наказания. Более того, изготавливаются специальные онлайн презентации и справочники по мошенническому искусству.

(2) Хорошая осведомленность преступников способам противодействия расследованию.

Что касается мошенничества, преступниками в основном являются рецидивисты. Кроме того, преступные группы, занимающиеся мошенничеством, обучают друг друга, обмениваются опытом, поэтому у них формируются достаточные хорошие способности противостояния следствию. Во-первых, они используют несоответствие внутренних и зарубежных правовых процедур и совершают противоправные действия дистанционно за рубежом, создавая сложности в расследовании таких дел. Во-вторых, они маскируют преступные действия «законной обложкой» и совершают преступные действия в законной

деятельности. В-третьих, различные подгруппы мошенников не контактируют напрямую, а общаются через конкретного «лидера группы», которого сложно идентифицировать в случае ареста.

(3) Низкая раскрываемость преступлений и низкий уровень возврата краденного имущества.

Низкая раскрываемость и низкий уровень возврата краденного имущества – это быстро нарастающая тенденция, связанная с телекоммуникационным мошенничеством, которую нельзя недооценивать. Имеется ряд разнообразных причин. Прежде всего, преступления, связанные с телекоммуникационным мошенничеством, не имеют определенного места совершения, следов преступления остается очень мало и сотрудникам следствия очень сложно отследить преступников по следам. В части телекоммуникационного мошенничества из-за отсутствия ограничения телекоммуникационного пространства, преступники могут совершать преступления «за тысячи миль». Сетевая информация может передаваться в различные места через серверы, Dock bao и другое оборудование. Поэтому, компании, на которые зарегистрирован сервер и продавцы оборудования, также должны рассматриваться в качестве подозреваемых в оказании помощи преступникам. Кроме того, сотрудникам следствия приходится направляться в различные места для сбора доказательств, различие правовых систем разных регионов становится препятствием и серьезной проблемой для следствия. Кроме того, после совершения мошеннических действий преступник может продавать товары через рынок подержанных товаров, через интернет и сторонние финансовые организации с несовершенными уставами и положениями, подпольные банки и казино. В данных случаях сложно зафиксировать факт получения денег, что затрудняет расследование дела и возвращения краденного имущества. Также нельзя не учитывать, что дел совершается очень много, а возможности следствия не велики, что обуславливается наличием несовершенств надзора и управления в общественной сфере и рядом прочих причин.

(4) Время прямого контакта между подозреваемым и потерпевшим сокращено, вплоть до полного отсутствия контакта.

При совершении мошеннических действий ранее преступники использовали разные методы для достижения личного контакта с потерпевшим, они вступали в диалоги и имели достаточно длительные контакты. Таким образом потерпевшие могли описать внешность, голос и прочие особенности подозреваемого, что помогало в расследовании. Вслед за развитием и распространением телекоммуникационных технологий, преступнику не нужно личного контакта с жертвой для совершения мошеннических действий, либо этот контакт может быть минимальным. Преступления могут совершаться через отправку голосовых сообщений, видео, изображений и прочей электронной информации через сеть.

(5) Криминальные методы постоянно модернизируются, идут в ногу со временем. Посягательства совершаются на определенные группы потерпевших.

Существует множество способов совершения мошеннических действий. С одной стороны, вслед за популяризацией Интернет технологий, преступники также используют эти возможности для создания новых видов мошенничества, вместе с тем традиционные методы мошенничества также постепенно интегрируются с Интернетом. С другой стороны, преступные элементы постоянно следят за горячими темами современности, используют информацию о людях и их особенностях, исследуют политические и социальные вопросы, чтобы определенным образом влиять на определенные группы людей, распространяют ложные слухи и посягают на финансовую собственность граждан. Например, использование национальной политики ликвидации бедности для получения субсидий людьми, которые не попадают под соответствующие критерии. Использование учебных и бытовых потребностей студентов для совершения мошеннических действий, таких как, продажа ложных ответов на экзаменационные билеты, незаконное взимание платы за обучение либо выдача ссуд.

(6) Увеличение количества случаев совершения мошеннических действий в сфере телекоммуникаций.

По причине того, что вложения преступников в совершения деяний невелики, а их прибыль высока, а также учитывая высокую себестоимость проведения расследований таких дел привело к тому, что в последние годы наблюдается увеличение числа случаев мошеннических действий и особенно в сфере телекоммуникаций. Согласно «Данным об уголовных процессах», обнародованным Верховным судом, с 2014 по 2018 год из десяти дел в судебном процессе дела, связанные с мошенническими действиями, стоят на шестом месте. Вместе с тем, статистические данные по преступлениям, связанным с телекоммуникационным мошенничеством за 2018 год, говорят о том, что число таких преступлений составило 810454, на 35,54 % больше по сравнению с аналогичным периодом в прошлом году. Количество раскрытых дел составило 98678, на 7,76 % больше по сравнению с аналогичным периодом прошлого года. Коэффициент раскрываемости составил 12.8 %, ущерб, нанесенный собственности граждан, составил 19,2 млрд юаней. Из вышеприведенных данных очевиден рост преступности, связанной с мошенничеством, что серьезным образом влияет на чувство безопасности людей.

(7) Наличие незарегистрированных преступлений

Поскольку темп жизни людей ускоряется, а условия жизни постепенно улучшаются, многие жертвы не сообщают о совершенном против них преступлении, даже если они знают, что их обманули, сумма, связанная с этим делом, невелика, сто или двести юаней, а иногда и вовсе десятки юаней, например, случаи мошенничества в отношении «размороженных капиталов». Кроме того,

из-за сложности процедуры расследования, после сообщения о совершенном преступлении, потерпевшие не желают связываться с такими сложностями и просто примиряются со своим ущербом. А после того, как к подозреваемому в совершении уголовного преступления были применены принудительные меры, преступления, в которых он признался, не гарантированно охватывают все его деяния, поэтому имеющиеся у нас данные меньше, чем фактическое количество преступлений.

(2) Анализ телекоммуникационного мошенничества с точки зрения теории криминологии

(1) теория рационального выбора

Теория рационального выбора говорит о том, что преступник приблизительно рассчитывает вложения, риски и возможные выгоды, необходимые для совершения преступного деяния, прежде чем принять решение о его совершении. В случае если риски и вложения меньше, чем выгода, исходя из человеческих инстинктов и жажды наживы более вероятно то, что преступник совершит преступление. И наоборот, если риски и вложения выше вероятно полученной прибыли, для преступника это будет сдерживающим фактором в совершении противоправных действий. В определенной степени, распространенность телекоммуникационного мошенничества связано с тем, что выгода от совершения данного деяния выше, чем вложения и риски. Как приводилось ранее в статье, в настоящее время сложность расследования преступлений, связанных с мошенничеством в сфере телекоммуникаций органами общественной безопасности, а также рост затрат и судебных издержек приводят к снижению рисков подозреваемых в совершении уголовных преступлений такого типа. Исследования показали, что существует связь между ростом преступности и риском, связанным с раскрытием преступлений. Повышение риска раскрытия уголовных дел о мошенничестве в сфере телекоммуникаций может сыграть определенную сдерживающую роль. Необходимо отметить, что: во-первых, применение теории рационального выбора основано на предположении, что потенциальные преступники рациональны, и могут рассчитывать возможности совершения преступного деяния, но не каждый преступник полностью полагается на рациональный расчет при принятии решения о совершении преступления. Не учитывается влияние на процесс принятия решения таких факторов, как личностные характеристики. Во-вторых, что касается оценки степени риска, критерии для преступников не единообразны, и что действительно может повлиять на совершение преступного деяния, так это то, что преступник, который намеревается совершить преступление, субъективно чувствует риск быть обнаруженным, а не объективные риски быть обнаруженным. Следовательно, исходя из вышеизложенных аспектов, борьба с преступлениями, связанными с мошенничеством в сфере

телекоммуникаций, должна быть сосредоточена на повышении риска преступного поведения, субъективно ощущаемого потенциальными преступниками.

(3) Теория повседневного выбора

Теория повседневного поведения говорит о том, что для возникновения преступного поведения необходимо три фактора: человек, способный совершить преступное деяние, подходящая цель и отсутствие достаточно эффективного надзора. Все эти факторы должны существовать в одном времени и пространстве. Согласно теории повседневного поведения, изменяя все эти три фактора, можно увеличить или уменьшить вероятность совершения преступного деяния и причиненный вред от него. По причине того, что преступные деяния, связанные с телекоммуникационным мошенничеством выходят за временные и пространственные рамки, пространственно-временные условия теории повседневного поведения могут быть приспособлены к виртуальной личности человека, вероятно способного совершить преступное деяние, к достаточно подходящей виртуальной жертве при недостатке эффективного контроля в телекоммуникационном пространстве. При этом необходимо, чтобы все три фактора существовали в пространстве телекоммуникационной сети для осуществления взаимодействия, виртуальные личности не обязательно должны находиться в одном времени и пространстве. Таким образом, для того, чтобы осуществлять борьбу с мошенничеством в сфере телекоммуникаций, нужно отталкиваться от трех элементов: контроль над созданием виртуальных личностей потенциальных преступников, сокращение целевой группы, которая может стать жертвой преступного деяния, усиление надзора над сетевым пространством и обрыв связи между потенциальными преступниками и целевой группой.

3. Меры борьбы с телекоммуникационным мошенничеством

(1) Увеличение рисков совершения преступного деяния, субъективно воспринимаемых потенциальными участниками

В настоящее время органы правосудия предпринимают ряд мер борьбы с телекоммуникационным мошенничеством. Во-первых, применение судебных толкований и совершенствование соответствующих законов и постановлений: «Заключение Верховного народного суда, Верховной народной прокуратуры и Министерства общественной безопасности по некоторым вопросам, касающихся применения законов при рассмотрении уголовных дел о телекоммуникационном мошенничестве», «Заключение Верховного народного суда, Верховной народной прокуратуры и Министерства общественной безопасности по некоторым вопросам, касающихся применения законов при рассмотрении уголовных дел о телекоммуникационном мошенничестве, (2)» и «Толкование Верховного народного суда, Верховной народной прокуратуры по некоторым вопросам, касающихся применения закона при рассмотрении уголовных дел о незаконном использовании сетевой информации, оказании помощи в совершении

преступных деяний в сетевом пространстве» и прочих заключений и судебных толкований. Расширение инкриминирующих обстоятельств (использовать как основание для возбуждения дела не только количество совершенных деяний, но и объем переданных мошеннических данных), определение отягощающих обстоятельств по результатам преступления и четкая классификация такого преступного деяния как содействие совершению телекоммуникационного мошенничества. Во-вторых, операции «меч в облаке», которые проводятся органами общественной безопасности, также отображают решимость борьбы с телекоммуникационным мошенничеством. В третьих, необходимо скорректировать механизмы преследования преступников за рубежом, нельзя допустить, чтобы укрытие заграницей стало для них лазейкой. Все эти меры объективно повысят риски совершения преступного деяния, что в определенной степени повысит субъективное чувство рисков потенциального преступника. В тоже время необходимо повысить эффективность и сократить время расследования. Чем раньше преступник будет наказан в соответствии с законом, тем сильнее будет сдерживающий эффект для других потенциальных преступников.

(2) Контроль над созданием виртуальной личности преступником

Снизить вероятность совершения преступного деяния посредством контроля над созданием виртуальной личности. С тех пор, как в 2020 году началась «Операция по взломам карт», органы общественной безопасности расправились с бандами по выпуску, получению и продаже банковских и телефонных карт, что внесло вклад в контроль над созданием виртуальной личности потенциальных преступников. Необходимо увеличить масштабы борьбы и усилия. Например, теневой банкинг, онлайн-казино, цифровые валюты и прочие платформы могут быть использованы преступниками для проведения транзакций и отмывания денег. Необходимо увеличить контроль органов общественной безопасности над этими платформами, чтобы пресечь возможность создания виртуальных личностей преступниками.

(3) Уменьшить количество целевых групп, которые являются потенциальными целями мошеннических действий.

Группы, которые являются потенциальными жертвами для совершения мошеннических действий, обусловлены следующими причинами: 1, имеющие ограничения или задержки в получении информации, что создает предпосылку для совершения преступных действий, 2, возникновение неправильных мыслей, а именно жажда легкой наживы или получения чего-то даром, 3, неумение различать добро и зло, доверчивость. Поэтому, для того, чтобы сократить количество групп, потенциально подверженных мошенническим действиям, необходимо способствовать формированию правильного мировоззрения и правильных жизненных ценностей, отказаться от идей легкой наживы, повышать чувство социальной ответственности, воспитывать трудолюбие, научить различать добро

и зло, укреплять управление социальными отраслями, уделять особое внимание вопросам, связанным с обеспечением жизнедеятельности граждан, таких как, получение кредитов и медицинское обслуживание.

(4) Усиление контроля над сетевым пространством.

В сегодняшних условиях развития Больших данных и их внедрения во все сферы жизни, необходимо усилить контроль за сбором, сравнением и использованием огромного числа сетевой информации и тем самым снизить количество случаев телекоммуникационного мошенничества. Как и в случаях предотвращения традиционных контактных преступлений (таких как грабежи, карманные кражи и т. д.), органам общественной безопасности необходимо повышать чувство безопасности у населения, проводить патрулирование и усиливать свои контролирующие функции. Необходимо изучить характеристики ложной информации, используемой мошенниками по форме, содержанию и способам распространения и преобразовать эту информацию в электронные данные, использовать определенные процедуры и алгоритмы для систематизации данной информации, выполнять функции надзора и патрулирования. Следует подчеркнуть, что в процессе сбора и проверки информации следует позаботиться о защите информации, не связанной с преступными действиями.

Список источников

1. Хуан Хэ. Обстановка касательно преступности и общественный контроль над наказанием за преступные деяния. Теология наказания. [J]. Национальное и международное право, 2021, 33 (03): 762–782.
2. Чжао Вэйцзя. Характеристики, причины и управление преступлениями в сфере мошенничества в телекоммуникационных сетях: использование в качестве выборки 569 судебного решения 2017 года [J]. Журнал Университета сельского и лесного хозяйства Фуцзянь (издание по философии и социальным наукам), 2018, 21 (03): 100–105.
3. People's Public Security News, Департамент уголовных расследований национальной общественной безопасности добился блестящих результатов в борьбе с преступлениями, 2020 год [EB / OL],
4. Пан Япенг, Шен Тин. Правовое определение действия по «взлому карт». [Дж.]. Прокурор Китая, 2021 (08): 70–71.
5. Кларк Р. (2000) Криминология ситуационного предупреждения и социальные ценности, Этнические и социальные перспективы ситуационного предупреждения преступности, глава 6, стр. 97–112, под редакцией фон Хирша, А. Гарланда, Д. и Уэйкфилда, А. Оксфорд: Hart Publishing
6. Верховная народная прокуратура, Отчет о работе Верховной народной прокуратуры за 2019 год (Text Record), [EB / OL], https://www.spp.gov.cn/tt/201903/t20190312_411422.shtml

从犯罪学角度浅论电信诈骗犯罪的预防

张百全
黑龙江公安警官职业学院侦查系

摘要：当前随着社会、科学技术不断发展，电信诈骗犯罪呈现出新趋势、新特点，这也对公安机关电信诈骗案件的侦查提出严峻的挑战，需要不断加强对此类案件的分析与研究。对于类案的研究必然离不开犯罪学角度，本文结合犯罪学理论探讨如何对电信诈骗犯罪进行预防。

关键词：电信诈骗 犯罪学 犯罪预防 侦查

诈骗犯罪是一种多发、常见的刑事犯罪，诈骗案件的犯罪嫌疑人侵害的是国家、集体或公民个人的合法财产，扰乱了正常的社会秩序，严重影响人民群众的安全感。近年来，随着科技的迅猛发展，互联网、智能移动设备的普及，犯罪嫌疑人反侦查意识逐渐增强，传统诈骗案件犯罪数量减少，与此同时传统诈骗犯罪手段不断更新，逐步与互联网技术融合，利用网络技术实施诈骗的案件不断上升，并随着时间呈现出新特点。正是由于这些新特点，公安机关在主动发现犯罪侵害行为、查清犯罪团伙组织结构、收集犯罪证据以及抓捕犯罪嫌疑人等方面需要投入更为强力的智能分析研判以及更多警力、物力资源，这对公安机关侦查部门提出严峻的挑战。所以，在控制电信诈骗犯罪案件方面，无论从节约司法成本角度，还是在减少被害者受侵害程度方面，预防远胜于打击。

犯罪原因以及犯罪预防对策一直是犯罪学研究的主要内容，所以在研究如何对电信诈骗犯罪进行控制时，必然要从犯罪学的角度进行探究。传统的犯罪学理论，例如合理选择理论以及日常行为理论都可以根据当前电信诈骗犯罪形势为犯罪预防与控制带来新思路。

一、电信诈骗案件的形势与特点

（一）犯罪行为人呈现专业化、职业化、集团化的特点。

犯罪分子为了分散风险，逃避打击，往往采用结伙作案的方式，事前谋划，案中协同，案后销赃，层级分工明确，组织结构严密，连续多次作案。近年来，这种趋势发展愈发明显，从犯罪小团伙转变为专业的犯罪集团，集团内部可分为信息组、技术组、业务组、培训组、洗钱组、后勤组等。在犯罪人员吸收方面也超越以往以地缘、血缘或亲缘关系为纽带，采取传帮带模式相互传授犯罪手段和经验，以及反侦查经验，当前更是会通过网络平台公开招聘“业务员”，然后培训组制作ppt或者培训手册传授诈骗技巧。

（二）犯罪行为人反侦查意识强。

诈骗案件中犯罪行为人多为惯犯累犯，再加上诈骗犯罪群体互相学习传授手段和经验，所以作案人反侦查意识强：第一他们可以利用国内外法律程序不一，将犯罪过程中的某个环节放在境外进行，为侦查制造困难；第二，他们将犯罪行为打上合法的“外包装”，在合法活动中掺杂诈骗行为；第三，诈骗团伙的各个分组之间不直接联系，而是通过特

定的“小组长”进行联系沟通，如被抓捕，难以指认。不同案件情况，还有其他的反侦查手段，这些手段大大增加了执法机关的侦查成本。

（三）破案率低，追赃少

破案率低、追赃少一直是电信诈骗案件不容忽视的形势变化，其原因是多种多样的。首先诈骗行为没有明显的现场，留下的痕迹较少，侦查人员很难通过痕迹进行追查，而在电信诈骗案件中，由于电信网络技术的实际空间限制小，犯罪行为人可以在“千里之外”实施犯罪行为，通过网络手段，网络信息可以通过多地的服务器、多卡宝等设备进行处理、转换、传导，那么该服务器注册公司、多卡宝销售商家涉嫌帮助网络信息犯罪活动罪等罪名应当被侦查，并且根据情况需要侦查人员到多地获得相应的证据材料，又因为执法程序因国家地域的不同而有所差异，导致侦查机关难以取证。再者，诈骗行为实施后，犯罪行为人可以通过二手市场、网络、规章制度的不健全的第三方金融机构以及地下钱庄、网络赌场等途径进行销赃，这些途径在钱财流入时难有记录，给侦查追赃造成阻碍。除此之外，还有发案多，侦查力量少，社会中一些特殊行业管理、监督机制不健全等原因。

（四）犯罪嫌疑人和被害人直面接触时间减少到没有接触。

在以前的诈骗犯罪案件中，犯罪嫌疑人是通过各种方式和被害人面对面接触、对话沟通实施诈骗行为的，被害人和犯罪嫌疑人接触时间较长，侦查人员可以通过被害人了解犯罪嫌疑人的体貌、行为、口音等信息入手查找犯罪嫌疑人。随着网络电信技术和设备的发展与普及，犯罪分子要实施诈骗行为，没有必要和被害人直接接触或者减少接触，可以通过网络电信手段发送语音、视频、图片、软件、链接等电子信息实施诈骗。

（五）犯罪手段不断更新，紧跟时事热点，受害群体精准化

诈骗方式多种多样，一方面由于互联网技术的普及，犯罪分子也借助互联网浪潮产生出多种诈骗手段，与此同时，传统的诈骗手段逐渐和互联网融合翻新；另一方面，犯罪分子紧跟时事热点，利用当前人民群众信息获得便利这一特点，结合当时的政策、方针或者社会热点问题，挑选出更为关注该热点、政策的群体，编造谎言，诱骗被害人钱财。例如，利用国家扶贫政策，以帮助获得扶贫款为托词，骗取实际上不符合扶贫条件群众的钱财；利用学生求学、考试等学习生活需要，谎称贩卖考试答案、收取学费、发放贷款对学生群体实施诈骗行为。

（六）发案率高，电信诈骗案件占比持续上升。

由于诈骗犯罪案件中犯罪行为人投入少，收益大，侦查成本高，近些年来，诈骗案件高发，特别是电信诈骗案件。根据最高法公布的《平安中国背后的刑事审判数据》，2014年至2018年最高法审理案件前十名罪名中诈骗罪位居第六。同时，根据2018年全国电信网络诈骗案件统计，2018年全国电信诈骗案件立案数为810454件，同比上升35.54%，破案数为98678件，同比上升7.76%，破案率约为12.18%，人民财产

损失高达约192亿元。由此可见，诈骗犯罪态势高涨，严重影响了人民群众的安全感。

（七）存在犯罪黑数

由于人们生活节奏加快，生活条件逐步上升，很多受害人即使知道自己被骗了，也不会报案，因为单个人涉案金额并不多，一两百元，或者就几十块钱，例如民族资产解冻类案件。再者因为，报案后，调查程序繁琐，所以不愿报案，自己认亏。以及犯罪嫌疑人在被采取强制措施后，所交代的罪行并不能保证是他所实施过的全部罪行，所以，目前我们已有的数据比实际的发案量要小。

结合犯罪学理论分析电信诈骗案件

（一）理性选择理论

理性选择理论指的是犯罪行为人在决定是否实施行为之前会粗略的计算实施犯罪行为所需要的投入、承担风险以及可能的获益。如果投入和风险之和小于收益，基于人趋利的本能，预谋实施犯罪的犯罪行为人实施行为的可能性要大于不实施的可能性。反之，如果投入和风险之和大于收益，则会抑制犯罪行为的发生。当前电信诈骗犯罪行为高发的原因在一定程度上可以认为犯罪投入和承担的风险远小于可能的收益，正如上文所述，当前公安机关侦查电信诈骗犯罪的难度和司法资源投入增大，则犯罪嫌疑人承担的风险就会降低。有研究表明犯罪率的发展和犯罪后背发现的风险之间存在联系，提高电信诈骗犯罪案件被发现的风险，则可以对该类案件起到一定的抑制作用。需要强调的是：第一，理性选择理论的应用是基于假设潜在的犯罪行为人都是具备理智的，并在实施犯罪行为的时候能够进行计算，但并不是每一个犯罪行为人，都完全依靠理性计算来决定是否实施犯罪行为，其性格特点等因素对决策过程的影响是忽略不计的；第二，对于风险程度的评估，犯罪行为人的标准不是统一的，并且，对于真正能够影响是否实施犯罪行为的是预谋要实施犯罪的行为人主观感受到被发现的风险，而不是客观实际被发现的风险。所以，基于以上被强调的方面，控制电信诈骗犯罪案件应着重增加潜在犯罪行为人主观感受到的实施犯罪行为的风险。

（二）日常行为理论

日常行为理论指出犯罪行为的发生需要有三个要素：有充分可能性的犯罪行为人，足够合适的目标，以及缺少足够的有效监管力。而且需要三者存在于同一时空。根据日常行为理论的描述，通过改变这三种因素，可以增加或者降低犯罪事件发生的可能性以及被害的可能性。结合实际情况，由于电信诈骗案件突破了时间和空间的限制，那么日常行为理论的时空条件则可以适当调整为有充分可能性的犯罪行为人的虚拟身份、足够合适被害目标的网络身份以及在电信网络空间中缺少有效的监管力，并需要三者都存在电信网络空间且虚拟身份之间可以进行联系交流，而虚拟网络身份落地的现实身份，并不要求处在同一时空。所以控制电信诈骗犯罪案件可以从这三个要素着手：控制潜在的犯罪行为人虚

拟身份的构建、降低可能被害目标群体、增加网络监管力量以及切断潜在犯罪行为人和目标群体的联系。

三、电信诈骗犯罪案件控制措施

（一）增加潜在行为人主观感受实施犯罪的风险

当前，刑事司法机关为打击电信诈骗犯罪多方面、多角度实施措施：首先：例如《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》、《最高人民法院、最高人民检察院、 公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》和《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》等意见、司法解释的施行，完善相应法律法规，扩大入罪条件范围（不仅以涉案数额为依据，还以发布诈骗信息的次数为立案条件）、根据犯罪结果规定加重情节以及明确帮助实施电信诈骗行为的定性；第二，公安机关“云剑行动”的开展，展现出公安机关对电信诈骗重拳出击的态势；第三，调整境外打击模式，不让境外成为犯罪分子实施犯罪行为的温床。这些措施都在客观上提高了犯罪行为人实施犯罪的风险，这对提高潜在犯罪行为人主观感知风险有一定作用。与此同时，一要提高侦查效率，缩短侦查时间，犯罪行为人越快收到法律制裁，则对潜在犯罪行为人震慑效果越强；二要发挥媒体作用，加大宣传成功打击电信诈骗案件的力度，提高震慑效果。

控制犯罪行为人网上虚拟身份的构建

通过控制犯罪行为人虚拟身份的构建，减少有可能性的犯罪行为人。自2020年开始的“断卡行动”，公安机关对于银行卡、电话卡开卡、收卡、贩卡团伙进行打击，就是在控制潜在犯罪行为人虚拟身份构建的行为。在这一方面还要加大力度与范围，例如对于地下钱庄、网络赌场、数字货币等可以利用网络进行交易洗钱的平台，公安机关要增强控制能力和力度，使犯罪嫌疑人不能在此类平台构建虚拟身份，从而进行销赃活动。

减少诈骗行为侵害目标群体

诈骗行为被侵害群体，从其自身来说，存在以下但不仅限于以下所列原因：一、存在获取信息阻塞或延迟，为行骗创造机会；二，存在贪图便宜、不劳而获等不当思想；三，不能明辨是非曲直，轻易相信他人。所以，要减少诈骗行为侵害目标群体，就要引导群众树立正确的人生观、世界观、价值观，摒弃不劳而获的思想，促进社会责任感、艰苦奋斗意识的培养；要提高个人明辨是非能力，能够辩证地看待事物；加强社会行业管理，对于关系群众民生事务要特别注意，特别是贷款、医疗保险等事务，要加强必要信息宣传，拓宽群众获取信息渠道，减少获取信息阻塞、延迟的情况。

增强网络监管力量

在着力发展大数据技术融入各行各业的今天，控制电信诈骗犯罪可以通过增强网络监管力量，利用大数据技术在海量的网络信息中比

对、抓取、阻止可疑信息，并根据情况采取相应防诈措施。正如，过去为了防范传统接触型犯罪（例如抢劫、扒窃等行为），提高公众安全感，公安机关在街面巡逻，增加监管力量。研究电信诈骗案件中虚假信息在形式、内容、传播方法等方面特点，并转化成电子数据模式，利用特定程序、算法对可疑数据进行抓取核查，起到网络巡警的作用。需要强调的是，在信息抓取与核查的过程中，要注意对于不涉及犯罪行为的信息进行保护。

参考文献：

1. 黄河. 犯罪现实与刑罚的社会控制 基于刑罚目的论的反思[J]. 中外法学, 2021, 33(03): 762 - 782.
2. 赵炜佳. 电信网络诈骗犯罪特征、成因与治理——以2017年569份判决书为考察样本[J]. 福建农林大学学报(哲学社会科学版), 2018, 21(03): 100 - 105.
3. 人民公安报，2020年全国公安刑侦部门打击犯罪战果辉煌, [EB/OL], https://www.mps.gov.cn/n2254314/n6409334/c7668153/content.html
4. 潘亚鹏, 沈婷. “断卡”行动中提供银行卡及关联行为的法律定性[J]. 中国检察官, 2021(08): 70 - 71.
5. Clarke, R. (2000) Situational Prevention Criminology, and Social Values, Ethnical and Social Perspectives on Situational Crime Prevention, Chapter 6, pp. 97 - 112, edited by von Hirsch, A. Garland, D. and Wakefield, A. Oxford: Hart Publishing
6. [7]最高人民检察院，2019年最高人民检察院工作报告（文字实录）, [EB/OL], https://www.spp.gov.cn/tt/201903/t20190312_411422.shtml

УДК 34

НЕСООТВЕТСТВИЕ ФИЗИЧЕСКИХ СИЛ ПОТЕРПЕВШЕГО И ПРЕСТУПНИКА КАК КРИТЕРИЙ БЕСПОМОЩНОГО СОСТОЯНИЯ ПРИ УБИЙСТВЕ

А. О. Швейгер, *доцент кафедры уголовного права,* Дальневосточного юридического института МВД России, кандидат юридических наук.

В статье рассматриваются актуальные вопросы, касающиеся оценки несоответствия физических сил потерпевшего и виновного лица при совершении убийства. Автор на основе изучения положений теории уголовного права и правоприменительной практики делает выводы о содержании данного признака и правовой оценки несоответствия физических сил как квалифицирующего обстоятельства.

Ключевые слова: убийство, несоответствие физических сил, беспомощное состояние.