МАНИПУЛЯЦИИ ИНФОРМАЦИЕЙ

Вызов нашим демократиям

Отчет Центра анализа, прогнозирования и стратегии (CAPS, Министерства Европы и иностранных дел) и Института стратегических исследований Военной школы (IRSEM, Министерства вооруженных сил).

Содержание:

ТРЕТЬЯ ЧАСТЬ

ПРЕДИСЛОВИЕ

Наше исследование

Наше исследование является результатом двуступенчатого осознания опасности - экзистенциального - что манипуляции информацией взвешиваются на наших демократиях. Во-первых, неоднократные вмешательства, которые произошли с 2014 года (Украина, Бундестаг, голландский референдум, Брексит, выборы в США) показали, что западные демократии, даже самые большие, не защищены. Затем попытка вмешаться во французские президентские выборы 2017 года с так называемым делом «Макроновой утечки» закончилась интересом Франции и убедила нас в важности изучения предмета.

В сентябре 2017 года мы по собственной инициативе решили создать рабочую группу, объединяющую некоторых членов Центра анализа, прогнозирования и стратегии (ЦАПС) Министерства Европы и иностранных дел и Министерства иностранных дел и Института стратегических исследований Военной школы (IRSEM) Министерства Вооруженных Сил, первоначально для рассмотрения возможности создания межминистерской ячейки для борьбы с манипулированием информацией, но более фундаментально для изучения проблемы, ее причин, ее последствий и ее решений.

Эта рабочая группа должна была быть межведомственной, чтобы реагировать на внутренне междисциплинарный характер манипуляций информацией на стыке международных отношений, военных исследований, разведки, средств массовой информации, социологии и социальной психологии; и кстати, в результате, этот вопрос касается определенного количества администраций.

Эта рабочая группа должна быть сосредоточена на международном, принимая во внимание не только наши собственные интересы, но и транснациональный характер явления, которое разыгрывается в рамках суверенитета и территориальности правовых систем. Хотя некоторые случаи более известны, чем другие, манипуляции информацией универсальны. Они касаются гражданских обществ и правительств большого числа государств не только в Европе и Северной Америке, но и в Азии, на Ближнем Востоке, в Африке и Латинской Америке. Но манипуляции с информацией также многогранны, и каждый случай отличается, потому что предназначен для целевого сообщества.

В частности, мы должны различать экзогенные манипуляции, исходящие из-за пределов целевого государства, и эндогенные манипуляции, происходящие изнутри и, с другой стороны, между теми, которые вызваны государственными субъектами и теми, которые вызваны негосударственными субъектами. Поскольку невозможно было охватить все, и наш аспект находится на пересечении иностранных дел и обороны, мы решили ограничить себя в этом отчете исследованием манипуляций с информацией государственного происхождения и иностранного, то есть вмешательства.

В последние месяцы мы посетили двадцать стран (Австрия, Бельгия, Канада, Дания, Испания, Финляндия, Германия, Италия, Япония, Латвия, Нидерланды, Польша, Россия, Сингапур, Испания,

Швеция, Украина, Великобритания) и три организации (ЕС, НАТО, ОБСЕ). Мы провели около ста интервью с властями (министерствами иностранных дел, обороны и разведывательными службами) и представителями гражданского общества (учеными, аналитическими центрами, ГО, журналистами), чтобы выяснить, каково их восприятие угроз и контрмер. Мы также проводили интервью во Франции с властями, гражданским обществом и частными субъектами и работали с имеющейся научной литературой, обзор которой можно найти в библиографии.

Мы подготовили около пятнадцати внутренних заметок для соответствующих министерств и ведомств, публичную записку* и несколько мероприятий, в том числе серию семинаров в IRSEM по «информационным войнам» и международный симпозиум, организованный CAPS, открытый министром культуры и завершенный выступлением министра Европы и иностранных дел, которые по сей день остаются самым точным официальным выражением по этому вопросу.

* Мод Кессард, Американская общественная дипломатия и российская дезинформация: возвращение информационных войн? IRSEM Research Note, № 54, 30 апреля 2018 года.

В своем выступлении министр отметил этот отчет, который находится в стадии подготовки, что является основным результатом наших исследований. Он хотел бы научиться «извлекать оттуда уроки*». Это то, на что мы надеемся. Однако этот отчет не является и не должен рассматриваться как официальная позиция французского правительства. CAPS и IRSEM пользуются определенной свободой слова в своих министерствах. Наша группа исследователей и дипломатов работала независимо.

Этот отчет также не является окончательной позицией: мы продолжим в будущем изучение предмета в рамках наших компетенций, в частности, чтобы попытаться выявить мутации этого явления, которые будут по-прежнему отмечать жизнь наших демократий в постоянно обновляемых формах.

* «Центр анализа, прогнозирования и стратегии моего министерства с Институтом стратегических исследований Военной школы завершает подготовку отчета, в котором анализируются и передовые практики наших партнеров, исследователей, СМИ и организаций гражданского общества на международном уровне. Я надеюсь, что мы сможем извлекать оттуда уроки» (Жан-Ив Ле Дриан, заключительная речь международной конференции «Гражданские общества, СМИ и государственные органы: демократии, сталкивающиеся с манипулированием информацией», Париж, 4 апреля 2018 года)

КРАТКОЕ ИЗЛОЖЕНИЕ

Манипуляции информацией не являются новым явлением. Их последняя актуальность связана с сочетанием двух факторов: с одной стороны, беспрецедентные возможности быстрого распространения и виртуальности, предлагаемые сетью Интернет и социальными сетями, в сочетании, с другой стороны, с кризисом доверия, который живет в наших демократических странах, и который обесценивает публичную речь, чтобы релятивизировать даже понятие истины.

Американские выборы 2016 и французские выборы 2017 сурово освещают этот феномен, его источники и его последствия. Однако влияние манипуляций информацией, в некоторых случаях на их само существование, иногда ставится под сомнение. Разве мы не находимся в контексте демократических дебатов, излишки которых могут быть исправлены действующим законодательством? Не является ли акцент ряда правительств на «ложных новостях» удобным способом очистить себя или указать пальцем на предполагаемых врагов демократии, в том числе на внешнюю сторону, чтобы укрепить свою собственную политическую позицию? И даже коварным предлогом подвергнуть сомнению общественные свободы и, прежде всего, свободу выражения?

Эти возражения серьезны. Они требуют углубленного изучения, чтобы как можно лучше определить, чем являются и чем не являются манипуляции информацией. В этом отчете предлагается определение проблемы, заменяя более неопределенное и полемическое понятие поддельных новостей на более точное - манипулирования информацией, которое понимается как преднамеренное и массовое распространение ложных или предвзятых новостей для враждебных политических целей. В этом отчете основное внимание уделяется манипулированию информацией государственного происхождения и направленной на ослабление или дестабилизацию демократических дебатов в других государствах.

Из этого определения, наших интервью в 20 странах и обзора, насколько это возможно, из обширной литературы по этому вопросу, этот отчет выстроен следующим образом. Во-первых, он ставит вопрос «почему?» к причинам манипулирования информацией, которые в то же время индивидуальны, связаны с природой человека, таким образом, относятся к психологии и эпистемологии (когнитивные изъяны и кризис знаний) и коллективные, связанные с жизнью в обществе (кризис доверия к институтам, кризис в прессе и разочарование в цифровом мире). Проанализировав каждую из этих причин, мы видим, кто получает от нее выгоду, т. е. кто является субъектом манипуляций информацией, сосредоточивая нас на государствах, которые манипулируют снаружи, т. е. которые вмешиваются.

Затем в этом отчете рассматривается «как?». В нем освещаются отличительные особенности последних кампаний по обработке информации с целью выявления некоторых общих особенностей с точки зрения факторов уязвимости (присутствие меньшинств, внутренних подразделений, внешних подразделений, уязвимой среды для СМИ, оспариваемых учреждений) и средств (разнообразными рычагами и векторами, откалиброванными рассказами, привилегированными местами и механизмами, массовой утечкой документов, фальсификацией документов, избирательными вмешательствами). Мы исследуем другие области манипуляций информацией - другие по отношению к постсоветскому пространству, Европе и Северной Америке, которые являются наиболее известными, а именно Ближний Восток, Африку и Латинскую Америку.

В третьей части, посвященной ответам, мы суммируем контрмеры, принятые всеми участниками: государствами, международными организациями, гражданским обществом и частными субъектами, начиная с исследования «Макроновых утечек», которое остается своеобразным примером недавней истории попыток вмешаться в избирательные кампании, так как эти попытки потерпели неудачу. Поэтому важно понять почему и извлекать из этого уроки.

Наконец, мы пытаемся привлечь внимание к будущим задачам - технологическим задачам, будущим тенденциям российской «информационной войны», возможным сценариям - до принятия 50 рекомендаций, предполагая, что манипуляции информацией будут продолжать представлять собой долгосрочную проблему для наших демократий, к которой они должны обеспечить совместный, либеральный и уважительный ответ основополагающих прав. В качестве постскриптума мы, наконец, предлагаем некоторые ответы на возражения, чтобы предвидеть наиболее распространенные критические замечания.

Информация все чаще рассматривается как общее благо, защита которой относится ко всем гражданам, обеспокоенным качеством публичных дебатов. Прежде всего, гражданское общество должно развивать свою собственную устойчивость. Правительства не только могут и должны поддерживать эти усилия, но они играют ключевую роль, поэтому правительства не могут потерять интерес к угрозе подорвать основы нашей демократии и, в конечном счете, национальной безопасности.

50 РЕКОМЕНДАЦИЙ

I Общие рекомендации

1. Определите и четко разделите термины, как мы пытались сделать во введении. Это должно помочь противостоять широко распространенному релятивизму, что «все является пропагандой» и что все СМИ используют дезинформацию. Что нужно осуждать, так это не

защиту национальных интересов - российские СМИ имеют право защищать российскую точку зрения и даже власть, но осуждать нужно манипуляции информацией. Использование диагноза «DIDI» (deception - дезинформация, intention - замысел, disruption - дезинтеграция, interference – интерференция/воздействие/вмешательство), рекомендованное Шведским MSB и Лундским университетом, могло бы помочь благодаря сетке объективных критериев отличить реальные манипуляции информацией от деятельности доброкачественного влияния*.
*. Джеймс Памментинг и др., Противодействие информационной деятельности, op. cit., стр. 7.

2. Не уменьшайте угрозу, даже если она не ощущается каждый день. Хорошая подготовка к борьбе с манипуляцией информацией обязательно должна основываться на соответствующей оценке угрозы, то есть на постоянной и современной разработке сценариев угроз с учетом изменений в конфликтах и рисков.
*. Правительство Финляндии, Стратегия безопасности для общества. Постановление правительства, Комитет безопасности, 2 ноября 2017 года.

3. Выйдите из краткосрочной перспективы. Информационные операции служат краткосрочным и долгосрочным целям. Краткосрочный термин связан с конкретным событием, как правило, с выборами, вооруженным или социальным конфликтом, стихийным бедствием, убийством (Немцов) или попыткой убийства (Скрипаль), авиакатастрофой (MH17) и т. д. Ложные учетные записи и ложные истории могут быть более очевидными, более жестокими, менее изощренными, потому что они имеют ограниченную жизнь в любом случае и будут либо раскрыты, либо удалены после достижения цели. С другой стороны, долгосрочные операции атакуют идеи, позиции, ослабляют их или сообщества, чтобы усугубить напряженность, которая их разделяет. Это ежедневная работа по подрыву, с актерами более сдержанными, более изощренными и последствиями, которые сложнее оценить. Однако именно эти долгосрочные операции являются наиболее опасными. Они следуют модели эрозии: если вода заканчивает разрушение породы, это вследствие длительности, повторения, постоянства. Поэтому важно выйти из краткосрочного периода, который часто является избирательной призмой (состоящей только из беспокойства по поводу информационных угроз в период выборов), чтобы понять, что борьба идет ежедневно.

4. Укрепляйте устойчивость наших обществ. Манипуляции информацией связаны с разделениями и напряженностью, которые протекают через наши общества. Мы будем эффективно бороться, то есть устойчиво, против этих манипуляций только с политическим желанием укрепить устойчивость наших обществ. С этой точки зрения многое можно узнать от некоторых государств, особенно от Финляндии, которая создала устойчивость к так называемым «гибридным» угрозам настоящей национальной концепцией*.
* Рене Ниберг, Гибридные операции и важность устойчивости: уроки из недавней финской истории», Фонд Карнеги за международный мир, 8 февраля 2018 года.

5. Не отказывайте от Интернета экстремистам. Если теории заговора разрастаются, это также потому, что у них нет противоречий*.
*Romain Badouard, The Disenchantment of the Internet. Дезинформация, слухи и пропаганда, с. 174.
«Пользователи Интернета, которые придерживаются формы научной рациональности, считают общение с «верующими» пустой тратой времени и предпочитают имитировать общение или игнорировать их. Точно так же «прогрессивные» пользователи Интернета не заинтересованы в обсуждении с расистскими, женоненавистническими или гомофобными интернет-пользователями для деконструкции их аргументов. В результате пространство онлайн-дебатов насыщается ложными или агрессивными утверждениями*.
*Фред Икле, «Современный контекст», в «Carned Lord» и «Frank Barnett» (ред.), «Политическая война и психологические операции», Вашингтон, издательство «Национальная оборона», 1989, с. 7.
В то же время, однако, нужно учитывать риск эффекта бумеранга, потому что опровергнуть - повторить. Любая коррекция, таким образом, косвенно увеличивает распространение

ложной информации. Этот эффект распространения неизбежен и должен привести к выбору, то есть опровергать стоит только самые опасные манипуляции

6. Не поддавайтесь соблазну контрпропаганды. Как писал в 1989 году Фред Иклэ, «истина - это лучшее оружие POLWAR [политической войны] и PSYOP [психологической войны] демократий», поскольку «цели демократии могут быть достигнуты только с помощью методов, совместимых с демократией"*. Для демократий лучший ответ на манипуляции информацией остается «убедительным фактическим доказательством, предоставленным в нужное время*».

*Фред Икле, «Современный контекст», в «Carned Lord» и «Frank Barnett» (ред.), «Политическая война и психологические операции», Вашингтон, издательство «Национальная оборона», 1989, с. 7.

*Линда Робинсон и др., Modern Political Warfare, op. cit., p. 232.

7. Не верьте в технологический солюционизм, против которого Евгений Морозов предупреждает нас в своей книге с вызывающим воспоминания названием «Чтобы решить все, нажмите здесь»*. В общем, нет единого решения, ответ должен быть многофакторным (поскольку проблема есть).

* Евгений Морозов, Чтобы решить все, нажмите здесь: аберрация технологического решения, FYP, 2014.

II Рекомендации для государств

8. Имейте легкий след. Первым оплотом против манипулирования информацией в демократическом и либеральном обществе должно оставаться гражданское общество (журналисты, СМИ, цифровые платформы, ГО и т. д.). Поэтому первая рекомендация для государства заключается в том, чтобы сохранить легкий след - не только в соответствии с нашими ценностями, но и ради эффективности: одной из причин проблемы является недоверие к элите. Подход «сверху» имеет свои пределы. Лучше продвигать горизонтальные, совместные подходы, которые включают участие гражданского общества. Это соответствует ожиданиям населения: самый большой опрос по этому вопросу (74 000 опрошенных в 37 странах в 2018 году) показывает, что респонденты считают, что ответственность за борьбу с манипулированием информацией лежит в первую очередь на платформах (71%), а затем только на государствах, особенно в Европе (60%) и Азии (63%), меньше в США (40%) *

* Информационный отчет Института Рейтер 2018, стр. 9.

Необходимо признать пределы чисто правительственного ответа, который всегда будет подозреваться в предвзятости и само пропаганде. Ответ должен быть глобальным. Это известно давно: на контр-пропагандистской конференции в 1952 году начальником отдела информационных исследований, секретным отделом британского министерства иностранных дел, в котором участвовало до 300 человек, ответственных за борьбу с Советским Союзом в Соединенном Королевстве уже заявил: «Мы должны развеять любую идею о том, что основные проблемы и вытекающие из этого действия являются обязанностью правительств и органов, которые они контролируют. Информация, спонсируемая правительством, предвзятые листовки, официальные заявления и любые очевидные попытки повлиять на свободное мнение хуже, чем бесполезны*. "

* Контрпропаганда: базовый анализ. Выдержки из чтения по контрпропаганде, данные начальником отдела информационных исследований в секретной серии чтений о коммунизме, SECRET (18674), № PR 89/45 G, TNA FCO 141/7460, сентябрь 1952 года, размещены на psywar.org, 30 апреля 2012 г.

С этой точки зрения предпочтительнее, чтобы государство организовывало выбор без принуждения к нему*

* Ричард Х. Талер и Касс Р. Санштейн, Nudge: Улучшение решений о здоровье, богатстве и счастье, Yale University Press, 2008.

9. Создайте специальную структуру. Большинство заинтересованных государств уже сделали это. Остальные должны создать национальную структуру для обнаружения и

противодействия манипуляции информацией. Эта структура может иметь различные формы: от простого общения пользователей ресурсов, разбросанных по разным службам, до создания центра со своим персоналом. Существенный вопрос, поскольку он связан с бюрократической борьбой, - это институциональная привязанность: среди существующих некоторые структуры координируются межведомственным или надминистерским органом, а другие - внутри министерства. Характер связи (исполнительная власть или простая роль секретариата) также варьируется. Тем не менее, некоторые константы обеспечивают руководство по ключам к успеху хорошей сети:
a) постоянство: постоянные структуры с четко определенными компетенциями и целями работают лучше, чем специальные инициативы, в которых обязанности часто рассеиваются*;
* Вероника Вичова и Якуб Джанда (ред.), Пражское руководство: как разработать национальную стратегию, используя уроки, извлеченные из борьбы с враждебными подрывными действиями Кремля в Центральной и Восточной Европы, европейские ценности, отчет о Кремле, 30 апреля 2018 года, стр. 3 и 28.
б) переменная геометрия: эти сети, как правило, состоят из ориентированного на безопасность «ядра» (Affaires étrangères – Иностранные дела, Défense - Оборона, Intérieur – Внутренние дела, renseignement - разведка), которое регулярно и, в зависимости от повестки дня, группы распространяется на другие министерства (образование, культура, правосудие) или даже на парламентариев и субъектов гражданского общества;
c) широкий объект: они публично выступают как ведущие борьбу с манипуляцией информацией в целом, даже если на самом деле они часто сосредоточены на России. Теоретически они могут иметь дело с другими государственными субъектами (Китаем, Ираном и т. д.) и негосударственными субъектами (джихадистскими группами). Ряд из них работает над созданием мостов между борьбой против манипуляции информацией и борьбой с радикализацией;
d) состав: сети, в которых работают, объединяют небольшую группу людей с цифровым опытом, которые знают друг друга и доверяют друг другу. Если группа слишком большая или слишком разрозненная иерархически, обсуждение будет менее эффективным. Междисциплинарная команда должна включать специалистов по информационным системам, которые слишком часто ограничиваются разрешением инцидентов и которые должны участвовать в стратегическом мышлении. Наконец, наиболее эффективными группами являются те, которые как минимум содержат определенных штатных людей, полностью посвященных этому предмету;
e) производство: помимо встреч и обмена информацией лучшими сетями являются продуктивные сети. Можно думать о трех типах внутренних публикаций: предупреждающие заметки, периодические анализы и тематические отчеты. Эта структура также может привести к составлению ежегодного отчета об управлении информацией (службы разведки - эстонское КАПО - или даже Вооруженные Силы - литовские - уже это делают);
f) коммуникация: поскольку прозрачность важна для устранения соблазнов заговора, эти сети являются публичными, а иногда и общаются вне. Некоторые из тех, кто подвергается сильнейшему давлению в Центральной и Восточной Европе, включая страны Балтии, не колеблясь, подчеркивают роль вооруженных сил и сил безопасности в этих усилиях, когда другие придерживаются противоположной стратегии придавать большую значимость учреждениям, наиболее близким к гражданскому обществу, для того, чтобы успокоить население. В Канаде наибольшая ответственность в борьбе с дезинформацией лежит на министре демократических институций, поскольку манипулирование информацией угрожает выборам и, следовательно, целостности демократических процессов.
Независимо от институциональной привязанности специализированной структуры, министерство иностранных дел играет важную роль в наблюдении и раннем предупреждении, особенно в отношении манипуляционных кампаний, ориентированных на национальные интересы за рубежом. Дипломатические сети действительно могут быть полезны как для оповещения о текущих кампаниях (информаторы), так и для распространения стратегического сообщения министерства (ораторы).

10. Проанализируйте сеть, чтобы найти сообщества, способствующие распространению. Трудно предвидеть угрозу. Однако ее можно обнаружить, и цель состоит в том, чтобы обнаружить ее как можно скорее. Это требует зондов в сообществах риска (экстремисты, заговорщики, монахини и т.д.). Эти зонды могут быть пассивными учетными записями, которые только слушают, или активными, которые участвуют. Существуют технические решения для прослушивания социальных сетей (DigiMind, AmiSoftware, Linkfluence и т. д.).
Официальные ответы (сайты, страницы, счета) имеют ограниченную эффективность. Подпольные операции (манипуляции манипуляторами) являются рискованными, потому что, если они будут обнаружены (и все труднее гарантировать, что они не будут когда-нибудь

обнаружены), они могут дискредитировать источник и укрепить заговорщиков, тем самым усиливая тех, которые должны были быть ослаблены. Что делать тогда?
Первым шагом будет работа в Интернете, чтобы знать сообщества, распространяющиеся в социальных сетях: выявлять главных действующих лиц (что может означать несколько вещей: наиболее последовательные, наиболее активные, наиболее связанные, наиболее цитируемые и т.д.); определить тип сообщества, его структуру (она централизованная, вертикальная, горизонтальная, племенная и т. д.?) и его дух (является ли оно сплоченным или конкурентным? разница важна, потому что конкурентное сообщество, в котором члены стремятся к признанию их другими, не будет затронуто изъятием одного ключевого члена, другой просто займет его место). Эта работа муравьев важна для понимания распространения сообщений и для того, чтобы предвидеть и действовать.
Мы можем тогда а) идентифицировать учетные записи, дающие старт манипуляциям и, напротив, учетные записи «друзья» или, по крайней мере, нейтральные, рациональные обеспечивать хорошей аудиторией; б) нейтрализовать первых (кибератаки, приостановки) и поддержать последних (например, посредством учебных предложений); с) выявить манипуляции, назвать источник (назвать и пристыдить) и дискредитировать содержание ложных новостей - либо прямо, официально, либо опосредованно через учетные записи «друзья».

11. Лучше общайтесь. Просто реагирование увеличивает риск потерь в информационной войне. Чтобы выиграть ее, вы должны не только обеспечить постоянное присутствие, иметь коммуникационную стратегию, передавать сообщения, опровергать ложную информацию, но и проявлять инициативу в том, чтобы вывести противника из своей зоны комфорта. Если наши службы обнаруживают троллей или неактивных ботов даже до их использования, например, они должны публиковаться публично.
Когда вас атакуют, вы должны общаться. Мы можем осудить нападение, не описывая его, и пусть средства массовой информации выполняют свою работу. Это одна из причин успеха движения Макрона En Marche (против попытки вмешаться во время французской кампании), и это также то, что сделали немцы во время их предвыборной кампании. Проактивность в общении в настоящее время считается лучшей моделью.
Для государств, английский язык которых не является официальным языком, необходимо также более плотно коммуницировать на английском об их доктрине, их национальной стратегии, их опыте.

12. Принимайте законы при необходимости. Государства должны иметь возможность принять следующие меры, если они сочтут это необходимым:
а) принять законодательство против ложных новостей, если его еще не существует, или обновить его в соответствии с цифровым контекстом;
б) в большей степени санкционировать дрейфы СМИ, следуя примеру британского Ofcom (который несколько раз санкционировал RT, что, похоже, было эффективным, то есть сдерживающим), и укрепить законодательство, карающее онлайн-преследования, особенно журналистов;
с) рассмотреть вопрос о регистрации иностранных средств массовой информации в соответствии с американским примером, что не повлияет на их распространение (и, следовательно, не будет цензурой), но будет просто мерой прозрачности: общественность имеет право знать, кто говорит, согласно логике, которая аналогична логике продовольственной безопасности: прослеживаемость информации должна обеспечивать ее качество.

Разработайте нашу правовую систему

«Я решил, что мы разработаем нашу правовую систему для защиты демократической жизни от этих ложных новостей. В скором времени будет представлен закон по этому вопросу. В течение избирательного периода на платформах на все спонсируемые материалы будут налагаться обязательства повышенной прозрачности, чтобы обнародовать личности рекламодателей и тех, кто

их контролирует, а также ограничивать суммы, выделяемые на эти материалы. [...]В случае распространения ложных известий, можно будет привлечь судью посредством нового иска по неотложному вопросу, позволяющего, в случае необходимости, удалить сомнительный контент, разыменовать сайт, закрыть соответствующую учетную запись пользователя или даже заблокировать доступ к веб-сайту. Полномочия регулирующего органа, которые также будут глубоко переосмыслены в течение 2018 года, будут усилены для борьбы с любой попыткой дестабилизации со стороны телевизионных служб, контролируемых или находящихся под влиянием иностранных государств. Это позволит CSA (Высшему совету телерадиовещания) модифицироваться, а именно, отказаться от заключения соглашений с такими службами, принимая во внимание весь контент, публикуемый этими службами, в том числе в Интернете. Это также позволит ему в случае каких-либо действий, которые могут повлиять на результаты голосования, будь то в предвыборный или избирательный период, приостановить или отменить соглашение. [...] Эта новая договоренность будет включать обязанность вмешательства со стороны технических посредников для быстрого устранения любого незаконного контента, доведенного до их сведения».

(Эммануэль Макрон, выступление по случаю приветствия прессы, 4 января 2018 года).

Однако следует проявлять осторожность, чтобы не перерегулировать, то есть сохранить баланс между защитой населения и защитой общественных свобод, который делает наши либеральные демократии. Чрезмерное регулирование - реальная опасность, даже ловушка, поставленная нашими противниками, которым далеко не мешает чрезмерное регулирование, и воспользуются полемикой и делениями, которые она создаст. Мы должны быть внимательны к этому риску непредвиденных последствий.

13. При необходимости проводите парламентские расследования. Общественное расследование, как показывают американские и британские примеры, имеет много преимуществ с точки зрения осведомленности общественности, накопления знаний и даже с точки зрения политики сдерживания.

14. Возложите ответственность на цифровые платформы. Роль социальных сетей в манипуляции информацией хорошо установлена: они стали основными источниками информации и, следовательно, дезинформации для большинства населения (они стали нашими «инфопосредниками»). Несмотря на то, что эти манипуляции дорого им обходятся в плане репутации и что они дали гарантии, недавно приняв ряд мер саморегулирования, их готовность положить конец этим методам является амбивалентной. Поэтому мы должны найти рычаги в европейском масштабе:
a) обязывайте их публиковать происхождение рекламных объявлений - требуя прозрачности, эквивалентной прозрачности, требуемой традиционными средствами массовой информации;
b) поощряйте их к принятию мер по борьбе с манипуляцией информацией на своих сайтах и содействию медиаграмотности и повышению осведомленности общественности.
Законодатель должен найти правильный баланс между возложением ответственности на цифровые платформы в борьбе с ложными новостями и уважением свободы слова.

15. Обменивайтесь информацией с цифровыми платформами. Мы не можем, с одной стороны, ждать, пока платформы будут делать больше, чтобы бороться с манипуляциями, а с другой - не предоставлять им информацию, которая им может понадобиться для продвижения. Сотрудничество между государственным и частным секторами имеет решающее значение и требует совместного использования двухсторонних знаний. Это одна из рекомендаций, сделанных двумя бывшими высокопоставленными должностными лицами администрации Обамы правительству Трампа в рамках подготовки к промежуточным выборам в 2018 году.*
* Джошуа А. Гельцер и Дипаян Гош, «Как Вашингтон может предотвратить вмешательство в промежуточные выборы», «Foreign Affairs», 25 июля 2018 года.

16. Инвестируйте в международное. В последние годы на международной арене в этой теме доминировала та же группа государств Центральной, Восточной и Северной Европы, а также Объединенное Королевство и Соединенные Штаты. Франция и Испания начинают больше присутствовать, потому что на них нападают. Не дожидаясь, чтобы быть в таком же положении, другие должны были бы инвестировать больше. В целом мы можем рекомендовать:

a) больше участвуйте в существующем. Государства, которые могут себе это позволить, должны систематически направлять экспертов по крайней мере в одну из целевых групп ЕС, прежде всего на Восток; способствовать работе Хельсинского европейского центра передового опыта по борьбе с гибридными угрозами (Hybrid CoE); и принимать участие в важных ежегодных встречах (Саммите StratCom в Праге , Рижском диалоге StratCom, Атлантическом совете StratCom в Вашингтоне);

b) объединяйте региональные сообщества. Евроатлантическая арена доминирует, но это не единственное: очень интересные вещи происходят в Азии, где Сингапур выделяется как эталон. Мало того, что власти проявляют инициативу и очень развернуты во вне, о чем свидетельствуют парламентские слушания и тот факт, что Министерство обороны скоро отправит эксперта на поселение в Центр передового опыта НАТО в Риге, но и гражданское общество далеко не позади. Центр повышения квалификации в национальной безопасности (CENS) Школы международных исследований им. С. Раджаратнама (RSIS) организует ежегодный семинар по дезинформации, который является одним из немногих точек встречи между сообществами исследователей и практиков из Европы, Северной Америки, Азии и Африки. Для завсегдатаев евроатлантической арены, которые склонны думать о предмете только через российскую призму, этот плюрализм освежающий. Ситуации, конечно же, очень разные (манипуляции информацией в Индии, Бирме или Индонезии тревожат, но они эндогенны, поскольку достаточно далеки от вмешательства России в Европу и Северную Америку), но поскольку Китай становится более агрессивным в регионе, как показывает австралийский случай, станут более интересными параллели с Россией - и вопрос о том, чему они учатся друг у друга;

c) внедряйте инновации, создавая новые механизмы. Поскольку манипуляции информацией часто являются международными, вопрос о координации имеет важное значение. Например, можно создать международный механизм раннего предупреждения для подключения всех сетей / центров / агентств в странах ЕС и НАТО. Нет необходимости создавать новую сеть: между Целевой группой Восточного стратегического комитета ЕС, Хельсинкским и Рижским центрами передового опыта, хабами, места встреч для национальных команд уже существуют.

Некоторые, особенно в Соединенных Штатах, предлагают создать международную коалицию. В своем докладе за январь 2018 года демократические сенаторы рекомендуют создать «международную коалицию против гибридных угроз», которую возглавит Вашингтон. Они предлагают президенту созвать ежегодный глобальный саммит по гибридным угрозам, смоделированный на саммитах Глобальной коалиции против Даэша или для борьбы с насильственным экстремизмом, которые происходят с 2015 года. Гражданское общество и частные субъекты приняли бы в этом участие.*

*Боб Коркер и др., Асимметричное нападение Путина на демократию в России и Европе: последствия для национальной безопасности США, op. cit., стр. 5.

Два месяца спустя Фрид и Полякова делают аналогичное предложение: создание «антидезинформационной коалиции» со стороны «Соединенных Штатов и ЕС», «общественно-частная группа, которая часто объединяет правительственные и неправительственные организации, в том числе социальные медиа, традиционные СМИ, интернет-провайдеров и гражданское общество*». Идея создания сети, объединяющей неправительственных субъектов, превосходна, но, сформулированная таким образом, она нам кажется проблематичной не только потому, что она забывает Канаду, но и потому, что этот трансатлантический альянс уже существует (НАТО) и что нужно будет объяснить Москве, которая не преминет спросить об этом, почему она тоже не может присоединиться к этой коалиции желающих, о риске казаться более антироссийской, чем анти-дезинформационной. Существующие структуры ЕС или НАТО не поддаются этой критике.

*Дэниел Фрид и Алина Полякова, Демократическая защита от дезинформации, Атлантический совет, 2018, стр. 13-14.
В мае 2018 года бывший вице-президент США Джо Байден, бывший министр обороны США Майкл Чертофф и бывший генеральный секретарь НАТО Андерс Фог Расмуссен, создали Трансатлантическую комиссию за прозрачность выборов. Это новая сторона, которой нужно следовать, хотя еще слишком рано знать, какую роль она сыграет.
Наконец, «Большая семерка» - это естественный форум для обмена передовым опытом и принятия решений об общих подходах к борьбе с манипуляциями информацией. Канада сделала его одним из приоритетов своего председательства в G7 в 2018 году, предложив различные механизмы обмена и совместных действий. Франция, которая займет пост председателя G7 в 2019 году, должна основываться на этих первоначальных результатах для продолжения работы на этом форуме с точки зрения сохранения и защиты демократии.

17. Обучайте взрослых и детей (медиаобразование и критическое мышление).
Грамотность в средствах массовой информации является одной из наиболее консенсуальных рекомендаций, хотя она неравно применяется государствами, о чем свидетельствует рейтинг Института «Открытое общество»*. Однако, если это ограничено школами, как это часто бывает, это также долгосрочная мера, которая вступит в силу только тогда, когда дети станут взрослыми. Необходимо рассматривать медиаобразование и, в более широком смысле, развитие критического духа всего населения во все годы жизни. Обучение подростков и учеников особенно важно, поскольку они в целом более уязвимы для манипуляции информацией по различным причинам (отсутствие контрольных показателей, необходимость утверждать себя, социокультурная среда), и не обязательно вначале получают медиаобразование. Предложить основным учебным модулем в первый год университета (текстовый анализ, изображения и идентификацию источников) это было бы полезно и легко реализовать, по крайней мере, на всех курсах гуманитарных наук.
* Институт «Открытое общество» (София), индекс медиаграмотности 2018 года. См. Marin Lessenki, Common Sense Wanted: Resilience to “Post-Truth” и ее предикторам в индексе информационной грамотности средств массовой информации 2018 года, март 2018 года.
Идея состоит в том, чтобы удостовериться, что, сталкиваясь с информацией, каждый человек ставит под сомнение ее достоверность (аргументы, доказательства) и ее источник (надежность, мотивация). Это медико-санитарная мера - так как в девятнадцатом веке необходимо было научиться мыть руки. Таким образом, можем следовать шведской модели и опубликовывать руководство по компьютерной гигиене для политиков и политических партий. Другими словами, мы должны обучать широкую общественность с раннего возраста, но не только, образованию в изображениях и аудиовизуальных СМИ, а и критическому мышлению и рациональной аргументации. Проверьте надежность информации. Курсы критического мышления и рациональной аргументации распространены в некоторых странах и даже считаются необходимыми предпосылками для университета. Человек учится распознавать паралогизмы и софизмы, ошибочные рассуждения. Эти методы «интеллектуальной самозащиты» должны распространяться*.
*Норманд Байерджон, Petit Cours d’autodéfense intellectuelle, Монреаль, Люкс, 2005.
a) В целом, установленные меры ограничены по меньшей мере двумя факторами: учителя недостаточно подготовлены, и у них недостаточно времени для включения этой деятельности в программу. Правительствам необходимо быть внимательными и находить решения.
b) Часть образования должна заключаться в повышении осведомленности о том, что уже возможно (тролли, боты, дип-фейки и т. д.). В школах учить детей не только деконструировать, но и создавать ложные сведения и теории заговора: это позволит им расшифровывать их (если они в состоянии это сделать, они понимают, что взрослые тоже в состоянии, и, вероятно, лучше). Также научите их использовать изображения Google, например, чтобы проверять происхождение изображения. И научите их не только расшифровывать, но и обсуждать, а точнее, обсуждать онлайн, посредством семинаров, моделирований и т. д.
c) Грамотность в средствах массовой информации должна включать компонент среды для средств массовой информации, особенно бизнес-модель, роль онлайн-рекламы и т. д. Медиаобразование должно также включать технологический аспект, чтобы понять, как функционируют социальные сетевые алгоритмы (персонализация, фильтрация пузырьков).

Сама по себе задача объяснить детям, что большинство взрослых уже испытывает трудности с пониманием.
d) Не ограничивайтесь классами: чтобы повысить их эффективность, уроки аудита информации должны использовать широкий спектр вещательных компаний, включая телевидение, которое, вопреки всему, продолжает доходить до молодых аудиторий. Это могут быть информационные сообщения, предшествующие видео роликам на YouTube, или отправленные платформами в частных сообщениях, например, на Snapchat или в Instagram.
e) Взрослые могут подвергаться воздействию общественных кампаний на специальных мероприятиях и через обучение. Мы можем следовать примеру ГО Baltic Centre for Media Excellence, который готовит журналистов и учителей по всему региону. В гражданской службе, и особенно в наиболее заинтересованных министерствах и ведомствах, обучайте офицеров укреплять «компьютерную гигиену» и приобретать собственный опыт, позволяющий действовать автономно; это предполагает новые способы найма, обучения, партнерства между государственным и частным секторами и мобильность наших агентов для инновационных компаний, которые позволяют приобретать эти новые знания. Структуры, подобные Институту перспективных исследований национальной обороны (IHEDN), могут предложить обучение, посвященное информационным угрозам.
f) Игровой аспект важен, потому что манипуляции информацией часто занимательны, и ответ пропустит часть своей цели, если он будет казаться скучным (см. рекомендацию № 20). С этой точки зрения такие игры, как та, что разработана на Facebook Центром передового опыта НАТО по стратегической коммуникации, могут быть очень полезны, чтобы заинтересовать молодых (и не очень молодых) людей*. Другой пример: сайт Buzzfeed делает еженедельную «Fake News Quiz», которая имеет большой успех.
* «The News Hero» (https://apps.facebook.com/thenewshero).

18. Поддерживайте исследования. Наша иммунная защита от информационной инфекции зависит не только от нашей способности контролировать и анализировать информационное пространство, что означает выделение большего объема ресурсов в рамках разведки, - но и на нашу способность понимать участников, используя информационные манипуляции, начиная с России. Поэтому мы должны поддерживать исследования по России и постсоветским пространствам. Речь идет не о реанимации советологии, а о том, чтобы осознать, что адекватно реагировать можно не только на то, что хорошо известно.
В частности, это означает, что государства должны увеличить финансирование исследований путем проведения тендеров на исследования по заранее определенным темам или даже финансирования докторантов и /или постдокторантов, а также мероприятий (коллоквиумов) и публикаций. Связь с манипуляциями с информацией может быть либо прямой (когда речь идет о предмете исследования), либо косвенной, поскольку она может быть полезной, например, для поддержки связанных проектов в области информатики, социальной психологии или политической науки, которые привнесут детали в головоломку.

19. Маргинализируйте зарубежные пропагандистские органы. Сначала их нужно называть по имени. Едва избранный, президент Франции сделал это в Версале перед Владимиром Путиным, в отрывке, отмеченном во всем мире:
Russia Today и Sputnik были органами влияния во время этой кампании, которые в ряде случаев порождали неправду обо мне и моей кампании. [...] Это было не шуточно, что иностранные СМИ - под каким-либо влиянием, я не знаю, вмешивались в распространение серьезной лжи в контексте демократической кампании. И я ничего к этому не добавлю, ничего [...] Russia Today и Sputnik не вели себя как органы прессы и журналисты, но они вели себя как органы влияния, пропаганды и лживой пропаганды, ни больше, ни меньше*.
*Эммануэль Макрон на совместной пресс-конференции с президентом Владимиром Путиным 29 мая 2017 года в Версале.
В дальнейшем, нужно извлечь из этого выводы, то есть не аккредитовать их и не приглашать их на пресс-конференции, предназначенные для журналистов.

20. Используйте юмор и развлечение. Контрмеры часто подвергаются критике, потому что они не занимательны, потому что манипуляции информацией, как правило, таковы. Многие люди потребляют поддельные новости как нездоровую пищу: зная, что это плохо, но, чтобы

порадовать себя. RT и Sputnik практикуют информационно-развлекательную программу, смесь информации и развлечений, рядом с которой сделанные исправления могут показаться достаточно суровыми. Однако то, что подтверждает многолетний опыт в Европе и Северной Америке, заключается в том, что юмор, сатира, мистификация, издевательство особенно хорошо работают против манипуляций информацией. Гражданское общество это хорошо усвоило: в Литве есть сатирические программы («Derzites tam!»), сатирические награды (премия Путина от европейского экспертного центра), сатирические учетные записи в социальных сетях (Дарт Путин на Twitter, который дает советы, такие как «Не верьте * ничему*, пока Кремль не опровергнет это») и т. д. East StratCom Task Force также демонстрирует юмор на своем веб-сайте EUvsDisinfo и в социальных сетях. Государства не должны больше исключать использование юмора и развлечений для общения в определенных контекстах (Швеция делает это очень хорошо, чтобы очистить некоторые клише на Sweden.ru, например).

21. Помните о наших уязвимостях. Информационные манипуляции используют уязвимости наших демократических обществ. Таким образом, необходимо отображать их, идентифицировать их, понимать их, предвидеть, где будут удары, и пытаться предотвратить их. Способность поставить себя на место наших оппонентов имеет важное значение для лучшего прогнозирования их целей. Для этого мы должны не только лучше изучить их, чтобы понять их (исследования и разведка), но и протестировать наши процедуры с red teams - командами, играющими роль противника, и стремящимися выявить и использовать наши уязвимости.

22. Помните, за что мы боремся. Информационные манипуляции стремятся установить систематическое сомнение в отношении ценностей и принципов сообществ, на которые они нацелены. Лучший способ борьбы с этими манипуляциями - это, прежде всего, знать, что именно мы хотим защитить.

23. Признайте неизбежность переворота и незаконного присвоения наших контрмер. Они будут возвращены противником, иногда в зеркальном эффекте (RT имеет свой FakeCheck на четырех языках, с сайта Министерства иностранных дел России с февраля 2017 года раздел «Публикуемые материалы, содержащие ложную информацию о России», и т. д.), или захвачены им или даже третьими государствами (нелиберальные, использующие сюжетт для принятия законов либертицидов). Поэтому мы должны поддерживать позитивные подходы к распространению качественной информации, которая может свободно циркулировать, вдали от логики фрагментации, которая в настоящее время работает в Интернете.

24. Будьте внимательны к слабым сигналам за пределами российской призмы (других государств, негосударственных субъектов) или против наших интересов за пределами Европы (в частности в Африке и на Ближнем Востоке).

25. Слушайте гражданское общество, включая журналистов. Регулярный и свободный диалог между журналистами и политическими лицами, принимающими решения, может помочь бороться с манипулированием информацией. В Швеции Совет по средствам массовой информации регулярно объединяет представителей средств массовой информации и политиков для выявления проблем и, что важно, для координации их деятельности по проверке фактов*. Бельгийская группа экспертов рекомендует создать «платформу для консультаций», которая охватит все соответствующие заинтересованные стороны (университеты, СМИ, журналистов и школы журналистики, ГО, платформы).
*Эрик Браттберг и Тим Маурер, «Российское вмешательство в выборы: противоборство Европы в поддельных новостях и кибер-атаках», Фонд Карнеги за международный мир, 23 мая 2018 года.

26. Боритесь с другими формами влияния. Манипуляции информацией являются лишь частью сложной системы, они питаются другими видами влияния. Например, в случае с

Россией целевые государства должны также снизить свою энергетическую зависимость от России и бороться с коррупцией и российскими деньгами, которые помогают финансировать операции влияния.

27. Во внешней военной операции развивайте отношения с местным населением. Никогда не забывайте, что «каждое действие проецирует изображение, порождает восприятие противником, местным населением, но также сегодня и отечественной и международной аудиторией. Таким образом, отряд в действии является первым действующим лицом, и речь идет не только о несмертельных действиях*». В рамках расширенного присутствия НАТО в странах Балтии американские военнослужащие в Латвии оказывали услуги русскоязычным общинам (например, резкой древесины), что увеличивало их популярность и помогло ослабить пропаганду антиамериканских СМИ, передаваемых российскими СМИ, которую эти общины потребляют*.
* Бертран Бойер, «Операции в области окружающей среды: новая информационная война», Стефан Тайалят, Амаэле Каттарупце и Дидье Дане (ред.), Cyberdéfense. Politique de l'espace numérique, op. cit., стр. 212.
*. Тодд Хельмус и др., Влияние социальных медиа в России, op. cit., стр. 89.

28. Санкционируйте ответственных за серьезное вмешательство, особенно в избирательный процесс, если правомочия это позволяют - например, посредством экономических санкций и уголовного преследования (специальный прокурор США Роберт Мюллер обвинил 13 россиян и 3 российских объекта в феврале 2018 года, а затем 12 офицеров ГРУ в июле 2018 года).

III. Рекомендации для гражданского общества

29. Понимайте и укрепляйте механизмы цифрового доверия. Информационные манипуляции являются одновременно причиной и симптомом кризиса доверия к цифровому пространству. Эффективная борьба с этими манипуляциями должна в конечном счете способствовать повышению уровня доверия, но в то же время она требует понимания психологических механизмов доверия, с точки зрения пользователей, и поощрения передовой практики, которая его укрепляет. С этой точки зрения полезны кооперативы для установления индексов надежности содержимого.

30. Разрабатывайте проверку фактов, осознавая их ограничения. Поскольку мы склонны игнорировать исправление, особенно если оно ставит под сомнение глубокое убеждение, проверка фактов может быть эффективной для данного лица при двух условиях: с одной стороны, если исправление не является прямым вызовом его видению мира (в противном случае это может даже иметь порочный эффект его укрепления - мы видели это в случае оружия массового уничтожения в Ираке, изменения климата или вакцинации) и с другой стороны, исправление должно объяснить, почему и как была распространена дезинформация*.
* Тодд Хельмус и др., Влияние социальных медиа в России, op. cit., стр. 89.

31. Разработайте простые инструменты, позволяющие гражданам разоблачать манипуляции информацией, например, узнавая, кто скрывается за рекламой (whotargets.me) или обнаруживать видео, которые были подделаны (проект InVID AFP), например.

32. Разработайте нормативные инициативы (рейтинги, индексы, метки), осознавая, что множество конкурирующих стандартов помешают общим усилиям. Поэтому цель должна заключаться в том, чтобы выявить некоторые справочные инструменты вокруг признанных ГО. С этой точки зрения инициатива RSF имеет потенциал.

33. Примите международную норму журналистской этики на совместной основе (путем объединения основных традиционных и онлайн- средств массовой информации). В большинстве основных средств массовой информации есть хартии хорошей редакционной и

этической практики*, которые могли бы совпасть. Мюнхенская хартия 1971 года может служить основой, но она должна быть адаптирована к нынешнему медиа-ландшафту, особенно цифровому.
* См., в частности, AFP от 22 июня 2016 года.

34. Лучше подготавливайте журналистов к риску манипулирования информацией, в школах журналистики и на протяжении всей их карьеры. Как укрыть массивную утечку данных (leak), обнаружить ложный профиль или отреагировать на экстремистский контент? Существуют конкретные ответы*, которые могут стать предметом обучения и подготовки
* Например, Хайди Творек, «Ответственная отчетность в эпоху безответственной информации», «Альянс за обеспечение демократии» (GMF) Краткая информация 2018, № 009, март 2018, стр. 4.

35. Повышайте доверие к журналистике за счет повышения прозрачности. The Trust Project*, консорциум, включающий The Economist, The Globe and Mail, Repubblica и The Washington Post, рекомендует выявлять финансирование (аналогично, веб-сайт The Conversation требует от исследователей, которые там публикуются, выявления потенциальных конфликтов интересов, общая практика в научных журналах), профили журналистов, обоснование их опыта, различие между мнением, анализом или спонсируемым контентом, каким образом происходит доступ к источникам, почему журналист предпочел преследовать одну гипотезу, а не другую и т. д. Идея состоит в том, что читатели хотят знать, как работают журналисты, как они узнают, что они узнают: эта прозрачность в отношении журналистских практик, методов и процедур может способствовать укреплению доверия.
*Thetrustproject.org

36. Разрабатывайте инструменты борьбы против троллинга, такие как Jigsaw Perspective, который используя самообучаемость, идентифицирует подстрекательные комментарии, которые затем могут быть изолированы, приостановлены до публикации, а потом подвергнуты модерированию. The New York Times использует этот инструмент на своем сайте. Другой метод - публиковать списки учетных записей, идентифицированных как тролли.

37. Используйте искусственный интеллект и автоматическую обработку языка при обнаружении манипуляций и проверке фактов. Изобретение ложных или предвзятых новостей таково, что журналистов, аналитиков и исследователей никогда не будет достаточно, чтобы найти и обработать их. Программное обеспечение для обнаружения, такое как Storyzy, постоянно усовершенствуется и увеличивается в числе. Что касается проверки фактов, то программное обеспечение может автоматически сравнивать нового правонарушителя со всеми теми, кто уже был «деметифицирован», а не для того, чтобы делать работу впустую, но это предполагает доступ к общим базам данных - отсюда и важность сетей верификаторов. Автоматическая проверка экономит время, но по-прежнему требует, чтобы человек в конце процесса проверял.

38. Разрабатывайте анкеты и опросники для оценки чувствительности населения к манипулированию информацией. Точные и регулярные данные повысят эффективность контрмер, которые будут их учитывать.

39. Развивайте плюрализм посредством инструментов, способствующих разнообразию информации, чтобы обойти явление «фильтрующих пузырьков»: множество проектов, включая NewsDNA Гентского Университета, должны позволить гражданам регулировать степень разнообразия новостей, которые они потребляют*.
* Александр Алафилиппе и др., Доклад Бельгийской группы экспертов по ложной информации и дезинформации, op. cit., стр. 9.

40. Переосмыслите экономическую модель журналистики с целью сочетать сохранение свободы слова, свободную конкуренцию на рынке и борьбу с манипулированием информацией.

41. Поощряйте исследователей вмешиваться в публичные дебаты. Псевдо-наука распространена, потому что она занимает плацдарм, слишком часто оставляемый вакантным истинными учеными: плацдарм распространения научного знания (или популяризация). Слишком многие исследователи отказываются от этой деятельности, учитывая, что воздействие средств массовой информации представляет собой этическое отклонение и тормоз в их карьере. Однако в этом контексте заклинивания и путаницы, социальная ответственность ученых никогда не была более высокой: они должны сделать результаты своей работы доступными для неспециалистов и таким образом занять общественные дебаты. Следовательно, высшие учебные заведения должны организовывать учебные курсы по типу media training в этой исследовательской деятельности, которая отвечает специфическим «кодам». Кроме того, исследовательская деятельность должна быть более оценена в карьере и должна быть основным критерием оценки, чтобы побудить ученых к практическим упражнениям.

IV. Рекомендации для частных действующих лиц

42. Переосмыслите статус платформ: используйте платформы под слово и оказывайте сильное политическое давление, чтобы вовлечь их в требуемые поведенческие кодексы, чтобы гарантировать, для того чтобы их афишируемые миссии воплощались на рабочем уровне (алгоритмы, модерация, усилия полиции в сетях и т. д.). Необходимо задать вопрос об антимонопольном регулировании, упомянутом в рамках группы экспертов, созданной Европейской комиссией (см. выше).

43. Требуйте новый контракт с пользователями на основе новых цифровых прав. Технические условия должны быть переработаны, чтобы сделать их понятными для всех и четко указывающими о доступе и использовании персональных данных. Важно предоставить пользователям Интернета больший контроль над будущим своих данных (можно придумать систему включенных опций, платную систему, обеспечивающую одну или несколько из следующих функций: конфиденциальность данных, блокирование рекламы, отслеживание персональных данных).

44. Наложите высокий уровень прозрачности. После скандала в Cambridge Analytica общих призывов к большей прозрачности уже недостаточно. Пользователи должны знать о кампаниях, которые на них нацелены, и о причинах этого таргетинга. Политическая реклама, связанная с эксплуатацией больших данных, должна подлежать определенному регулированию с учетом целей и задач, которые она представляет для наших демократий. В этом контексте была упомянута идея общественного медиатора, который имел бы доступ к алгоритмам под прикрытием обязательства строго соблюдать конфиденциальность.

45. Повысить себестоимость манипулирования информацией при защите уязвимых отдельных лиц и движений. Необходимо начать более систематическую борьбу с агентами манипуляции, начиная с концепции threat actor, возникшего из области кибербезопасности. Эта концепция помогает идентифицировать цепочку команд и инфраструктур, общих для разных операций. Вместо того, чтобы одно за другим подвергать цензуре проблемные содержания (whack-a-mole approach), платформы проводят расследование, чтобы идентифицировать враждебного актора и подвергнуть цензуре все его демонстрации, по модели закрытия всех страниц Facebook, связанных с IRA. Информаторы и организации, на которых нацелена кампания по манипулированию информацией, должны быть в свою очередь заранее предупреждены с помощью специальных систем обнаружения и использовать процедуры защиты (hotline), чтобы они могли защитить себя.

46. Оценивайте и высоко оплачивайте качественную журналистику. Нынешняя система перестала быть гибкой, цифровые платформы захватили большую часть рекламных доходов, ранее выделявшихся для финансирования средств массовой информации, в то же время всасывая их основной контент, не оплачивая его им. Необходимо подумать о новых способах перераспределения информационной ценности платформ в сторону качества СМИ.

47. Вносите финансовую поддержку на платформы качественной журналистики, например, путем финансирования инструментов проверки фактов.

48. Вносите вклад в финансирование платформ по независимым исследованиям: эксперты согласны с необходимостью доступа к данным платформы для измерения воздействия кампаний по манипулированию информацией, понимания модальности их вируса и оценки влияния мер по борьбе с дезинформацией. Платформы должны способствовать финансированию этих исследовательских усилий, не налагая скрытых условий на ориентацию исследования или политическое позиционирование исследователей по отношению к спонсорам.

49. Размышляйте о создании безопасных зон: учитывая асимметрию информации, проблемы, возникающие перед демократией посредством онлайн-дезинформации, не могут быть выполнены без сотрудничества с цифровыми платформами, что подразумевает воссоздание условий для конструктивного диалога. Следовательно, необходимо придумать создание мест обмена, где права интеллектуальной собственности платформ будут гарантированы в обмен на более легкий доступ к их данным, программному обеспечению и алгоритмам. Эти места должны способствовать развитию сотрудничества между исследователями, гражданским обществом и цифровыми платформами. Это предполагает, в частности, в продолжение дела Cambridge Analytica, предварительное создание основы для этических исследований, смоделированных по протоколам доступа врачей к записям пациентов.

50. Исследуйте методы перенаправления, чтобы те, кто искал ложные новости, наталкивались на демистификацию (debunking). Google Redirect, например, продемонстрировал бы снижение привлекательности Daesh, выявляя потенциальных новобранцев (исходя из их истории поиска) и разоблачая их видео на YouTube, демистифицирующем Daesh. Идея заключается в применении этого метода к другим манипуляциям информацией*.

***** Тодд Хельмус и др., Влияние социальных медиа в России, op. cit., стр. 77.