IPG
Международная
политика и общество

Открытый фланг Европы

Выборы в Европарламент находятся под угрозой кибератак со стороны правых сил, но ЕС не предпринимает достаточных защитных мер

Мориц Фесслер | 06.02.2019

Ни одна дезинформационная кампания не обходится без фирменной хакерской толстовки

Читайте также эту статью на немецком языке

Нет причин сомневаться в том, что выборы в Европейский парламент (ЕП) станут целью хакерских атак, дезинформационных кампаний и попыток манипулирования в социальных сетях: ретроспективный взгляд позволяет четко реконструировать, что со времен президентских выборов в США в 2016 году любое крупное политическое событие в Европе сопровождается попытками манипулирования в киберпространстве. Начиная с референдума о выходе Великобритании из ЕС, продолжая президентскими выборами во Франции и заканчивая неоднозначным народным голосованием по поводу независимости Каталонии – в течение всего этого периода разным аналитическим центрам, неправительственным организациям и государственным деятелям удавалось фиксировать попытки и реальное осуществление дезинформационных кампаний и кибератак в разных уголках Европы. В декабре прошлого года в Бельгии даже распалась правительственная коалиция из-за разногласий вокруг миграционного пакта ООН, которые в значительной мере были раскручены ультраправыми движениями через социальные сети. Потому нет ничего удивительного в том, что, согласно данным одного из последних опросов Евробарометра, три четверти всех европейцев обеспокоены дезинформацией в Сети.

Главы европейских государств и правительств – в качестве реакции на современные угрозы из киберпространства – придали огромное значение данной теме в декларации Европейского совета, принятой в октябре 2018 года. Вскоре после этого Европейская комиссия представила новый план

действий, в котором содержатся конкретные предложения по обеспечению безопасности выборов. В действительности же принятые (и не принятые) до сего дня меры недооценивают характер общеевропейских выборов, которые сегодня угрожают превратиться в пиршество для агрессоров из виртуального закулисья. При этом три основных фактора на порядок усиливают реальный размах кибератак в рамках общеевропейских выборов по сравнению с национальными волеизъявлениями избирателей и придают особый резонанс нынешним дискуссиям о теневых сторонах цифровой демократии в контексте ЕС.

Фрагментированная структура национальных мер безопасности в сочетании со сравнительно долгой длительностью голосования открывает широкий диапазон возможностей для атак из виртуального пространства

Одно из важнейших первоочередных различий обнаруживается уже при взгляде на партийно-политическую ситуацию на европейском континенте. Правее центральной точки политического спектра с нарастающей интенсивностью формируются евроскептические партии, заявленная цель которых состоит в ослаблении ЕС. Именно эти силы уже используют в рамках национальных выборов и референдумов социальные медиа в качестве ключевого инструмента манипуляции общественным мнением и не брезгуют при этом даже целенаправленными дезинформационными кампаниями и фейковыми новостями, как это, к примеру, имело место в рамках избирательной борьбы за кресла в бундестаге. Особое значение приобретает сетевое сходство антиевропейских сил в свете актуальных объединительных устремлений в правом лагере, в рамках которых лидер итальянских правых популистов Сальвини добивается создания альянса между самыми разнообразными евроскептическими партиями. Если бы такому союзу действительно посчастливилось состояться, то за счет этого в масштабах всей Европы возникла бы агрессивная ось в виртуальном пространстве. Тогда бы – в отличие от национальных выборов – результаты самых разных национальных и националистических кампаний в киберпространстве слились бы в конце мая в единый итог выборов, который мог бы поспособствовать значительному расширению присутствия в ЕП объединенных антиевропейских сил.

Во время выборов в Европейский парламент наряду с национальными действующими лицами особое значение для процессов в киберпространстве вполне может приобрести некий внеевропейский игрок. Россия в недавнем прошлом неоднократно пыталась оказывать влияние на выборы в Европе – как посредством фейковых новостей, так и посредством целенаправленного использования ботов в социальных сетях, а также знаменитой фабрики троллей из Санкт-Петербурга. При этом данное намерение Кремля демонстрирует коварное совпадение интересов с текущими целями антиевропейских сил: длительная дестабилизация Европейского союза как единого целого. Как следствие, Москва оказывает в том числе и финансовую поддержку евроскептическим партиям по всей Европе. Упомянутая принципиальная разница между волеизъявлениями избирателей на национальном уровне и выборами в Европейский парламент приобретет впоследствии взрывоопасный характер, поскольку за счет этого ключевые фигуры виртуального пространства больше не будут использовать выборы в мае 2019 года только для классического определения курса за или против той или иной политической повестки дня (например, за или против повышения размеров минимальной зарплаты), а подадут их под соусом выбора за или против ЕС как единого целого – немыслимый процесс на национальном уровне.

Более того, в рамках выборов в ЕП этот мрачный сценарий потенциальных угроз наталкивается на все еще слабо консолидированную линию обороны, которая представляет собой второе базовое

отличие от национальных выборов. Ключевой аспект при этом заключается в характере грядущих выборов: вместо одного тура голосования выборы в Европейский парламент охватывают более длительный временной отрезок с 23 до 26 мая и одновременно проходят в формате национальных выборов в 27 (или 28) государствах – членах ЕС. Тем самым на плечи каждого из этих государств – членов ЕС ложится в том числе и ответственность за защиту избирательной инфраструктуры от кибератак, однако их меры предосторожности воплощаются в жизнь с разной интенсивностью. Эта фрагментированная структура национальных мер безопасности в сочетании со сравнительно долгой длительностью голосования открывает широкий диапазон возможностей для атак из виртуального пространства. Осознавая свое бессилие в этом отношении, европейский комиссар по вопросам юстиции, защиты прав потребителей и гендерного равенства назвала лоскутным ковриком те меры, которые государства – члены ЕС приняли на текущий момент. При этом мало хорошего сулит и тот факт, что даже в Германии во время выборов в бундестаг в 2017 году удалось провести хакерскую атаку на главный программный комплекс, который передавал результаты выборов председателю Федеральной избирательной комиссии.

Если государства – члены ЕС не проявят ответственного отношения к защите выборов, то Союзу придется заплатить за это высокую цену

Третий и последний решающий фактор проистекает из результатов будущих выборов. Если, с одной стороны, дезинформационные кампании или автоматизированное распространение фейковых новостей в социальных медиа будут иметь успешный результат, то антиевропейские силы смогут заполучить приз в виде колоссального количества мандатов и тем самым ощутимо ограничить дееспособность ЕС. Если, с другой стороны, окажется успешной кибератака на избирательную инфраструктуру лишь в одном отдельно взятом государстве – члене ЕС, то можно будет открыто поставить под сомнение результат выборов в целом, а также итоговую легитимность нового Европейского парламента. В обоих случаях была бы оказана медвежья услуга необходимому сегодня усилению позиций парламента и дальнейшей демократизации ЕС.

В конечном итоге в дискуссиях на тему правильного обхождения с виртуальными угрозами в отношении ЕС дает о себе знать фатальный дисбаланс: если государства – члены ЕС не проявят ответственного отношения к защите выборов, то Союзу придется заплатить за это высокую цену. И эта цена вполне может оказаться неоправданно высокой в свете сложившейся ныне ситуации в Европе, когда споры о политическом курсе ЕС все больше и больше отягощаются дебатами о его выживании.