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

Й.М. Паску & Н.-С. Винтила,
Connections QJ 19, № 3 (2020): 64-77
https://doi.org/10.11610/Connections.rus.19.3.04

Рецензированная статья

Повышение устойчивости политических институтов и процессов: рамка анализа

Йоан Мирча Паску и Николае-Серджиу Винтила

Резюме: Обычные, а также нетипичные угрозы и уязвимости, как правило, подрывают основные принципы и механизмы функционирования демократических обществ. В этой статье исследуются внутренние слабости и операции иностранного вмешательства, направленные на манипулирование электоратом, и таким образом, на уменьшение гарантированного законом политического участия и ставящие под сомнение саму сущность демократии. В центре внимания данного анализа – манипуляции и дезинформация, в основном через средства массовой информации и платформы социальных сетей. Это увеличивает риск подрыва общественного доверия и доверия к демократическим институтам и процессам. Основная теза заключается в том, что демократические институты и процессы можно и нужно сделать более устойчивыми. В статье представлена рамка для анализа устойчивости политических институтов и процессов и исследуются текущие инициативы, в том числе ЕС и НАТО, по укреплению устойчивости.

Ключевые слова: устойчивость, демократическая устойчивость, дезинформация, компьютерная пропаганда, постправда, острая сила, демократия, операции иностранного влияния.

> *Сама демократия подвергается ударам со стороны иностранных правительств и внутренних угроз, так что демократические институты не смогут процветать, если наука о социальных данных не задействует наши существующие знания и теории о политике, общественном мнении и политической коммуникации. Эти угрозы актуальны и требуют неотложных действий и, если их не понять и не предпринять оперативных мер, они еще больше подорвут европейские демократии.*[1]

[1] Samuel C.Woolley and Philip N. Howard, eds., *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, Oxford Studies in

«Конец истории», о котором три десятилетия назад объявил Фрэнсис Фукуяма,[2] определенно наступил. Это отрезвляющее время для мечты о неизбежном продвижении либеральной демократии. Аналитики, либералы и соперники сходятся во мнении, что демократия «находится в состоянии рецессии»,[3] «отступает», что международный либеральный порядок, основанный на правилах, как минимум разрушается, если не полностью исчезает.

Наша рабочая гипотеза и основной аргумент этой статьи заключается в том, что демократические институты и процессы можно и нужно сделать более устойчивыми как к экстремальным политическим событиям и кризисам, так *и* к «нормальным чрезвычайным ситуациям». В статье анализируется политическая устойчивость, то есть сохранение демократии и ее чистоты. Мы сосредоточимся на ограниченном числе проблем, в частности, *на манипулировании электоратом* – принуждении кого-либо голосовать против его или ее первоначального намерения, – таким образом *уменьшая гарантированное законом участие в политической жизни и подрывая общественное доверие к демократическим институтам и процессам*. В центре внимания данного анализа – манипуляции и дезинформация, осуществляемые в основном через средства массовой информации и социальные сетевые платформы.

Повышение устойчивости демократических институтов и процессов – это тема, которая приобретает все большее значение в связи с тем, что проблемы возникают не только из-за *растущей хрупкости либеральной демократии* и из-за внутриполитических субъектов, но часто возникают в результате *операций по внешнеполитическому влиянию* и даже операций, осуществляемых при поддержке государств против стран-членов НАТО и ЕС (все чаще включающие кибершпионаж, прямое вмешательство в избирательные процессы, сканирование уязвимости критически важной инфраструктуры, подрывные атаки, а также пропагандистские и дезинформационные кампании[4]). Эти операции представляют собой *серьезную угрозу безопасности наших обществ*.[5]

Digital Politics (Oxford: Oxford University Press, 2018), c. 245. https://doi.org/10.1093/oso/9780190931407.001.0001.

2 Francis Fukuyama, “The End of History?” *The National Interest*, no. 16 (Summer 1989): 3-18.

3 Larry Diamond, “The Democratic Rollback. The Resurgence of the Predatory State,” *Foreign Affairs* 87, no. 2 (March/April 2008): 36-48.

4 Patryk Pawlak, “Horizontal Issues,” in *After the EU Global Strategy – Building Resilience*, ed. Florence Gaub and Nicu Popescu (Paris: European Union, Institute for Security Studies, 2017), 17, https://www.iss.europa.eu/sites/default/files/EUISSFiles/After_EU_Global_Strategy._Resilience.pdf.

5 Julian King, “Democracy Is under Threat from the Malicious Use of Technology. The EU Is Fighting Back,” *The Guardian*, July 28, 2018, www.theguardian.com/commentisfree/2018/jul/28/democracy-threatened-malicious-technology-eu-fighting-back.

Доверие к политическим институтам и процессам, в частности к участию в выборах, является ключевым показателем жизнеспособности и легитимности демократии. Его следует рассматривать во взаимосвязи с другими критическими вызовами и угрозами для устоявшихся и новых демократий, такими как злоупотребление исполнительной властью, коррупция и захват государства политическими элитами, рост авторитаризма и популизма,[6] которые могут усугубляться прямым вмешательством со стороны недемократических иностранных держав. Это вмешательство проистекает из конкуренции между основными международными демократическими и авторитарными игроками в результате сдвига в сторону многополярного распределения власти в глобальной системе.

Подрыв доверия и манипулирование общественным мнением преимущественно использовались во внутренней политике внутренними акторами и лишь впоследствии применялись в силовой игре в международных отношениях.

Сегодня две основные взаимосвязанные тенденции безоговорочно требуют оценки того, насколько подорваны демократические институты. Не менее необходимым и неотложным является осуществление мер по противодействию угрозам и повышению устойчивости демократических институтов и процессов.

Первая тенденция заключается в переплетении между технологиями, социальными и политическими злонамеренными действиями. Общепризнано, что социальные сети и новые электронные средства распространения и автоматизация сообщений позволяют общаться со скоростью света. Хотя Интернет обладает огромным демократическим потенциалом, информация и технологии для распространения могут быть и часто *используются в качестве оружия* для достижения политических целей, в основном направленных на подрыв консолидированных демократий. Такая политическая стратегия, использующая компьютерные средства, тесно связана с преднамеренным генерированием и использованием дезинформации, направленной против политических противников, демократических процессов и институтов как таковых, в невиданном до сих пор масштабе и охвате. (Еще в 2014 году Всемирный экономический форум определил быстрое распространение дезинформации в Интернете как одну из 10 основных опасностей для общества).[7]

Вторая важная тенденция – *экспоненциальный рост операций иностранного влияния*, вмешивающихся в фундаментальные политические

---

[6] Timothy D. Sisk, “Democracy’s Resilience in a Changing World,” in *The Global State of Democracy: Exploring Democracy’s Resilience* (Stockholm: International IDEA, 2017), 34-61, https://iknowpolitics.org/sites/default/files/idea-gsod-2017-report-en.pdf.

[7] World Economic Forum, “Top 10 Trends of 2014,” in *Outlook on the Global Agenda 2014*, http://reports.weforum.org/outlook-14/top-ten-trends-category-page/10-the-rapid-spread-of-misinformation-online. Для более детального анализа см. Wooley and Howard, eds., *Computational Propaganda*, 168.

процессы и подрывающих их – от выборов до широкого спектра «гибридных атак», направленных на подрыв демократии. «Гибридные угрозы» определяются как скоординированные и синхронизированные действия, которые преднамеренно нацелены на демократические государства и институциональные уязвимости политическими, экономическими, военными, гражданскими и информационными средствами.[8]

Операции по внешнему влиянию со стороны автократических держав, понимаемые как проявления «острой силы»,[9] широко и согласованно используют, в частности, вышеупомянутые технологические инструменты. В этом контексте действия, спонсируемые Российской Федерацией, представляют собой наиболее тревожные и хорошо задокументированные случаи операций по иностранному влиянию.[10]

Крайне важно понимать, как демократические процессы и институты могут подвергаться атакам как со стороны внутренних политических субъектов, так и со стороны иностранных соперников и противников, подрывая доверие людей к демократии посредством политических манипуляций с использованием новых коммуникационных технологий. Для этого нам нужно сделать краткое введение в последние достижения в области информационных технологий и специфику *компьютерной пропаганды*, чрезвычайно мощного нового инструмента коммуникации, используемого против демократических субъектов и институтов во всем мире. Могущественные и часто анонимные политические деятели использовали компьютерные методы пропаганды, чтобы вмешиваться в общенациональные выборы, совершать

---

[8] The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE, “Hybrid Threats,” https://www.hybridcoe.fi/hybrid-threats.

[9] Christopher Walker and Jessica Ludwig, “The Meaning of Sharp Power: How Authoritarian States Project Influence,” *Foreign Affairs*, November 16, 2017, www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power. По словам Уолкера и Людвига: «Усилия авторитарного влияния являются «острыми» в том смысле, что они пробивают, прокалывают или проникают в политическую и информационную среду в целевых странах. В новой безжалостной конкуренции, которая происходит между автократическими и демократическими государствами, острые силовые методы репрессивных режимов следует рассматривать как острие их кинжала. Эти режимы не обязательно стремятся «завоевать сердца и умы», что является общей системой отсчета для усилий по применению «мягкой силы», но они, несомненно, стремятся манипулировать своей целевой аудиторией, искажая информацию, которая доходит до нее».

[10] По заключению Национального совета разведки США в 2017 году, усилия России (по оказанию влияния на президентские выборы в США в 2016 году) представляют собой последнее выражение давнего желания Москвы подорвать возглавляемый США либерально-демократический порядок, но эта деятельность продемонстрировала значительную эскалацию прямого влияния, уровня активности и объема усилий по сравнению с предыдущими операциями. См. National Intelligence Council, “Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution,” January 6, 2017, www.dni.gov/files/documents/ICA_2017_01.pdf.

политические атаки, распространять дезинформацию, подвергать цензуре и нападать на журналистов, а также создавать фальшивые тенденции.

Этот анализ выполнен *с точки зрения политологии*, но очевидно, что технические данные должны быть представлены более широкой аудитории за пределами ограниченного пространства специалистов по информационным технологиям. Лица, принимающие решения, и общественное мнение, должны учитывать, что «уже сейчас скоординированные усилия сеют хаос во многих политических системах по всему миру. Некоторые вооруженные силы и спецслужбы используют социальные сети в качестве каналов для подрыва демократических процессов и полного свержения демократических институтов».[11] Специалисты по компьютерной пропаганде предупреждают, что описание явления только с технической точки зрения (как набор переменных, моделей, кодов и алгоритмов) создаст иллюзию «непредвзятости и неизбежности» пропаганды, и предлагают дополнять техническое описание социальными и политическими оценками, которые так же будут представлять вредные и сомнительные намерения и действия субъектов, использующих инструмент компьютерной пропаганды.

По словам Вули и Ховарда, «компьютерная пропаганда – это термин, который четко описывает это новое явление – и возникающую область исследований – цифровой дезинформации и манипуляции».[12] *Компьютерная пропаганда – это на самом деле политическая стратегия, основанная на расширенном использовании компьютерных технологий.* Подробное исследование показало, что платформы социальных сетей являются «средством проведения манипулятивных кампаний по дезинформации». «Компьютерная пропаганда, таким образом, является частью набора сомнительных политических практик, которые включают цифровой астротурфинг,[13] спонсируемый государством троллинг [14] и новые формы *онлайн-войны*, из-

[11] Wooley and Howard, eds., *Computational Propaganda*, 3.

[12] Wooley and Howard, eds., *Computational Propaganda*, 4.

[13] *Астротурфинг* – это процесс для обеспечения победы на выборах или законодательного урегулирования какого-то недовольства, помогающий политическим деятелям найти и мобилизовать симпатизирующую публику с помощью Интернета. Эта стратегия кампании может использоваться для создания имиджа общественного согласия там, где его нет, или для создания ложного впечатления о популярности кандидата или идеи публичной политики – см. Howard (2005), цитировано в Wooley and Howard, eds., *Computational Propaganda*.

[14] Согласно Urban Dictionary, троллинг – это «преднамеренный акт (тролля – существительное или прилагательное), когда он делает случайные непрошенные и/или противоречивые комментарии на различных интернет-форумах с намерением вызвать эмоциональную реакцию у ничего не подозревающих читателей, чтобы вовлечь их в драку или спор». Tech Policy, “State-sponsored trolling is rampant throughout the world – including the US,” *MIT Technology Review,* July 19, 2018*,* https://www.technologyreview.com/f/611694/state-sponsored-trolling-is-rampant-throughout-the-world-including-in-the-us/. Спонсируемый государством троллинг: «Используя фальшивые аккаунты, боты и скоординированные атаки легионов

вестные, как PsyOps (психологические операции) или InfoOps (информационные операции), конечной целью которых является манипулирование информацией в Интернете с целью изменить мнение людей и, в конечном итоге, их поведение». Автоматизация, масштабируемость и анонимность – отличительные черты компьютерной пропаганды.[15] Основанные на обработке данных методы и инструменты, такие как автоматизация (боты – *автоматическое программное обеспечение, созданное для имитации реальных пользователей-людей*) и алгоритмы (код для принятия решений), позволяют небольшим группам участников широко распространять очень специфичную, а иногда и оскорбительную и ложную информацию в основные онлайн-среды.[16]

Использование «больших баз данных» [17] для политической кампании и, зачастую, манипулирования электоратом – еще одна серьезная проблема для функционирования демократии. Специализированные компании по анализу данных собирают информацию об идентичностях, убеждениях и привычках потенциальных избирателей, на которые впоследствии можно направить конкретные сообщения, предназначенные для влияния и изменения их политических решений.

Скандал с данными Facebook / Cambridge Analytica, связанный с кампанией Leave.EU во время референдума в июне 2016 года в Великобритании, и предвыборная кампания Трампа вызвали самый интенсивный парламентский и общественный контроль, а также юридические меры реагирования на риски использования профилирования избирателей и незаконного сбора информации об их личных данных. Профили 87 миллионов пользователей Facebook были взломаны, чтобы выявить их подсознательные предубежде-

последователей, государства крайне затрудняют нахождения различия между общественным мнением и мнениями спонсируемыми троллями».

[15] Wooley and Howard, eds., *Computational Propaganda*, 7.

[16] По словам Вули и Ховарда, «использование ботов в злонамеренных целях, включая подрыв демократических институтов, вызывает особую озабоченность, поскольку – согласно последним данным, боты генерируют почти половину всего веб-трафика – огромную долю», Wooley and Howard, eds., *Computational Propaganda*, 8

[17] Этот термин связан с определением, данным в 2001 году отраслевым аналитиком Дугом Лэйни, который описал «3V»: объем, разнообразие и скорость [volume, variety, velocity], как ключевые «проблемы управления данными». Согласно Оксфордскому словарю английского языка, большие данные - это «данные очень большого размера, обычно в той степени, в которой манипуляции с ними и управление ими создают серьезные логистические проблемы». Наборы данных, подлежащие анализу, слишком велики или сложны, чтобы их можно было обрабатывать с помощью традиционного прикладного программного обеспечения для обработки данных. Наиболее актуальным для использования больших данных в цифровых кампаниях было использование прогнозной аналитики, анализа поведения пользователей или некоторых других методов расширенного анализа данных, извлекающих полезную стоимость из данных.

ния, и это вызвало беспокойство по поводу манипулирования их политическими решениями. Аналитики согласны с тем, что трудно оценить, в какой степени использование в кампаниях наборов данных, созданных Cambridge Analytica для микротаргетинга – индивидуализированного направления политических посланий, – повлияло на общественное мнение и повлияло на результаты голосований 2016 года в Великобритании и Соединенных штатах. Необходимость более строгого надзора за использованием платформ социальных сетей политическими кампаниями во время избирательного процесса была немедленно признана, и сейчас демократические правительства инициируют ответные меры законодательного и нормативного характера.

> *Использование онлайн фейковых новостей и дезинформации в качестве оружия создает серьезную угрозу безопасности наших обществ. Подрыв пользующихся доверием каналов для распространения пагубного и вызывающего разногласия контента требует ясного ответа, основанного на повышенной прозрачности, отслеживаемости и подотчетности. Интернет-платформы должны играть жизненно важную роль в противодействии злоупотреблению их инфраструктурой со стороны враждебных субъектов и в обеспечении безопасности своих пользователей и общества.*
>
> Комиссар ЕС по безопасности Джулиан Кинг [18]

В *Сообщении Европейской комиссии о борьбе с дезинформацией* [19] в Интернете, дезинформация определяется как «заведомо ложная или вводящая в заблуждение информация, которая создается, представляется и распространяется с целью получения экономической выгоды или намеренного обмана общественности, и в любом случае для причинения общественного вреда». В нем уточняется, что это определение исключает публикации об ошибках, сатиру и пародию, пристрастные новости и комментарии или незаконный контент. В сообщении проводится различие между заведомо ложными новостями и вводящей в заблуждение информацией.

Доверие к демократическим институтам также может быть подорвано *политическими кампаниями*, основанными на ложных/фейковых новостях, распространяемых через более традиционные средства массовой информации, а также широко распространяемых через платформы социальных

[18] EU Commission, “Tackling Online Disinformation: Commission Proposes an EU-wide Code of Practice,” April 26, 2018, https://europa.eu/rapid/press-release_IP-18-3370_en.htm.

[19] European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Tackling Online Disinformation: A European Approach, Shaping Europe’s Digital Future, Brussels, April 26, 2018, https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach.

сетей. Это особенно беспокоит, поскольку до недавнего времени политическое представительство в основном осуществлялось через выборных представителей, таких как члены парламента, а теперь граждане выражают свое мнение напрямую, будучи более уязвимыми для таких кампаний.

Наше понимание сегодняшних угроз и уязвимостей демократических политических систем должно учитывать разрушительное использование фейковых, сенсационных и других форм «мусорной информации» в сложные политические моменты за последние несколько лет. О'Коннор точно синтезирует этот феномен: «Мы живем в эпоху дезинформации – эпоху спекуляции, маркетинга и откровенной лжи. Конечно, ложь вряд ли является чем-то новым, но преднамеренное распространение ложной или вводящей в заблуждение информации резко увеличилось в прошлом веке, чему способствовали как новые технологии распространения информации – радио, телевидение, Интернет, – так и возросшая изощренность тех, кто вводит нас в заблуждение».[20]

Основная цель кампаний по дезинформации – создать эмоциональную среду для принятия решений, которая заменит разум и суждения, основанные на фактах, в качестве рабочего метода.

Более того, текущие интеллектуальные дебаты об «обществе постправды» показывают, что некоторые политические стратеги открыто принимают вызов самой истине «как стратегию политического подчинения реальности». «Таким образом, в идее постправды поражает не только то, что истина подвергается сомнению, но и то, что она подвергается сомнению как механизм утверждения политического господства».[21] Мы рискуем оказаться в параллельных реальностях, где будет сложно определить какая из них истинна.

Важным примером операций по иностранному влиянию являются все более хорошо задокументированные попытки России «подорвать единство, дестабилизировать демократии и подорвать доверие к демократическим институтам». Эта модель повторялась в ЕС: от операций влияния в преддверии референдума 2016 года в Нидерландах по Соглашению об ассоциации между ЕС и Украиной; продолжающиеся кибератаки с целью дальнейшего снижения доверия после голосования в Великобритании за выход из ЕС; пропаганда в СМИ, связанных с Кремлем, поляризующих вопросов во время выборов в Германии в 2017 году; и прокремлевские боты, участвующие в скоординированной «стратегии подрыва» в отношение Каталонии в 2017 году, наряду с поддерживаемыми Кремлем новостными платформами».[22] В *Докладе о расследовании вмешательства России в*

---

[20] Cailin O'Connor and James Owen Weatherall, *The Misinformation Age: How False Beliefs Spread* (New Haven, CT: Yale University Press, 2019), 11.

[21] Lee McIntyre, *Post-Truth* (Cambridge, MA: MIT Press, 2018), Chapter 1, Kindle Edition.

[22] Naja Bentzen, "Foreign Influence Operations in the EU," *European Parliamentary Research Service Briefing*, July 2018, http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf.

президентские выборы 2016 года специальный советник Роберт С. Мюллер пришел к выводу, что «российское правительство вмешивалось в президентские выборы 2016 года радикально и систематически».[23]

Согласно *Резолюции Европейского парламента о стратегической коммуникации ЕС для противодействия пропаганде против него со стороны третьих сторон*: «Стратегическая коммуникация России является частью более крупной подрывной кампании, направленной на ослабление сотрудничества в рамках ЕС и его суверенитета, политической независимости и территориальной целостности Союза и его государств-членов». Европейский парламент «призывает правительства государств-членов проявлять бдительность в отношении российских информационных операций на европейской территории и активизировать совместное использование потенциала и усилия контрразведки, направленные на противодействие таким операциям».[24]

Спектр угроз и действий, подрывающих демократические институты и процессы, шире, чем это кратко представлено в документе. Как на национальном, так и на межправительственном уровне растет консенсус в отношении того, что *повышение демократической устойчивости* может подготовить более эффективные меры реагирования на удары и стрессовые ситуации, в том числе те, которые создаются и распространяются с помощью компьютерных средств.

Понятие «устойчивость» широко используется в различных областях, от биологии и экологии до реагирования на стихийные бедствия, развития, гуманитарной помощи, демократии, внешней политики, общества в целом, критических инфраструктур, кибербезопасности и т.д. Таким образом, в последние два десятилетия это понятие воспринималось большинством аналитиков как «модное слово», которое, тем не менее, сохраняет практическую полезность в применении к контекстно-зависимой рамке.

В самом простом определении под устойчивостью понимается *способность абсорбировать и повторно восстанавливаться от любого типа стресса или ударов*. Определения становятся более сложными, но не всегда более убедительными, когда термин связан с конкретной системой или целью, которую необходимо достичь. Не вступая в дебаты о полезности этого термина, мы можем согласиться с Райнардом [25] в том, что любой конкретный подход должен прояснить следующие пять центральных вопросов:

---

[23] U.S. Department of Justice, Special Counsel Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, Volume 1 (Washington, D.C., March 2019), https://cdn.cnn.com/cnn/2019/images/04/18/mueller-report-searchable.pdf.

[24] European Parliament, "EU Strategic Communication to Counteract Anti-EU Propaganda by Third Parties, European Parliament Resolution of 23 November 2016 on EU Strategic Communication to Counteract Propaganda against It by Third Parties (2016/2030(INI))," www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.pdf.

[25] Mark Rhinard, "Horizontal Issues," in *After the EU Global Strategy*, 25-27.

(1) *что такое устойчивость*? – соответственно, значимость широкого и обширного или узкого определения; (2) *кто (или что) должен быть устойчивым?* – имеются в виду приоритеты, установленные различными академическими дисциплинами для устойчивого человека, сообщества, государства или общества в целом; (3) *когда мы можем ожидать проявления устойчивости?*, т.е. устойчивость можно понимать либо как способность «возвращаться в норму», имеющую место после наступления экстремального события, либо как «противодействующую устойчивость», имеющую место до того, как нарушение действительно произойдет, и в лучшем случае, даже не допустить этого; (4) *при каких событиях мы надеемся проявлять устойчивость?* – кризисы, которые выходят за рамки воображаемого («черные лебеди») [26] или имеются в виду «обычные чрезвычайные ситуации», когда устойчивые системы абсорбируют эти проблемы и адаптируются к ним, предотвращая их ухудшение; и, наконец, (5) *можно ли проектировать устойчивость*, делая упор на эффективность разработанной публичной политики для повышения устойчивости.[27]

Международный институт демократии и помощи в проведении выборов (IDEA) изучает решения для создания *демократической устойчивости*: способность демократических идеалов, институтов и процессов выживать и процветать при столкновении с вызовами и кризисами, которые они могут создать.[28]

Согласно определению IDEA, «устойчивость относится к свойствам политической системы, позволяющим справляться, выживать и восстанавливаться после сложных проблем и кризисов, представляющие собой стрессы или напряжение, которые могут привести к системному провалу».[29] По словам Сиска, «главными *качествами устойчивых социальных систем* являются: 1) *Гибкость*: способность выдерживать стресс или давление; 2) *Восстановление*: способность преодолевать проблемы или кризисы; 3) *Адаптация*: способность к изменению системы в ответ на стресс; и 4) *Инновации:* способность изменяться таким образом, чтобы более эффективно или действенно решать проблемы или кризисы».[30]

Создание устойчивости государства и общества, а также устойчивости демократических институтов и процессов, взаимосвязаны и должны разрабатываться скоординировано. Это также верно для политик, которые реа-

---

[26] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, 2nd ed., (New York: Random House, 2010).

[27] Rhinard, “Horizontal Issues,” 27.

[28] Sisk, “Democracy’s Resilience in a Changing World.”

[29] Timothy D. Sisk, “Democracy and Resilience: Conceptual Approaches and Considerations,” Background Paper (Stockholm: International Institute for Democracy and Electoral Assistance, 2017), 5, https://www.idea.int/gsod-2017/files/IDEA-GSOD-2017-BACKGROUND-PAPER-RESILIENCE.pdf.

[30] Sisk, *Democracy and Resilience*, 5.

гируют на конкретные проблемы на уровне подсистем, тем самым обеспечивая устойчивость критических инфраструктур, соответственно устойчивость к кибератакам, энергетическим проблемам или изменению климата, среди прочих, которые должны быть скоординированы и интегрированы в общие усилия по повышению устойчивости государства и общества.[31] Аналитики считают, что демократия может укреплять и способствовать устойчивости сообществ, общества и государства. Демократические системы при определенных условиях становятся более гибкими и способны адаптироваться к изменениям и принимать инновации. Поэтому крайне важно обеспечить и укрепить демократическую устойчивость.

Формирование устойчивости должно зависеть от контекста, поскольку не существует универсальных решений для различных проблем, уязвимостей и угроз, и для усиления способности социальных систем справляться с любыми стрессами и потрясениями и восстанавливаться после них.

Таким образом, необходимы конкретные меры по формированию устойчивости, чтобы реагировать на каждый из вызовов, подрывающих демократические институты и процессы. Политика по расширению демократического участия, реагированию на кампании дезинформации, противодействию гибридным угрозам, повышению киберустойчивости и устойчивости инфраструктуры и т.д. должна быть скоординирована на национальном и межправительственном уровнях. ЕС и НАТО разрабатывают и реализуют комплексные меры по повышению устойчивости на уровне своих государств-членов, а также в тесном сотрудничестве между ЕС и НАТО, чему способствует укрепление стратегического партнерства, как это определено в двух совместных декларациях, одобренных в Варшаве в июне 2016 и в Брюсселе в мае 2018.[32]

Повышение устойчивости – *ключевой элемент коллективной защиты* Североатлантического альянса.[33] Повышение устойчивости государства и

---

[31] Некоторые авторы считают устойчивость формой *управляемости*. По словам Джозефа, устойчивость, несмотря на то, что про нее говорят, что она связана с работой систем, на практике ближе к форме управления, которая подчеркивает индивидуальную ответственность. Тем не менее, если повышение устойчивости понимается просто как хорошее управление, полезность этого термина сомнительна. См. Jonathan Joseph, “Resilience as Embedded Neoliberalism: A Governmentality Approach,” *Resilience: International Policies, Practices and Discourses* 1, no. 1 (2013), 38-52, https://doi.org/10.1080/21693293.2013.765741.

[32] “Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of NATO,” Warsaw, July 8, 2016, https://www.consilium.europa.eu/media/24293/signed-copy-nato-eu-declaration-8-july-en.pdf; и “Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization,” Brussels, July 10, 2018, www.nato.int/cps/en/natohq/official_texts_156626.htm.

[33] Официальный текст НАТО, “Commitment to Enhance Resilience Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 8-9 July 2016,” https://www.nato.int/cps/en/natohq/official_texts_1331

общества является ключевым для подхода ЕС к безопасности государств-членов и Союза, особенно в отношениях с партнерами на Юге и Востоке, как это представлено в Глобальной стратегии ЕС в области внешней политики и безопасности.[34] ЕС принял *ключевые документы по устойчивости*, в том числе по противодействию дезинформации.[35] Очень актуальной инициативой в этом контексте является предназначенный для саморегулирования Кодекс в отношении дезинформации, согласованный в сентябре 2018 года представителями онлайн-платформ, ведущих социальных сетей и рекламной индустрии, которые согласились бороться с распространением онлайн-дезинформации и фейковых новостей.[36]

Значительное количество согласованных действий, реализуемых совместно ЕС и НАТО, сосредоточено на повышении устойчивости, в частности, на противодействии гибридным угрозам, анализе и скоординированной стратегической коммуникации для выявления дезинформации и распространения правдоподобного нарратива, на киберзащите и т.д.[37] Также стоит упомянуть о деятельности Центра передового опыта НАТО STRATCOM и Европейского центра передового опыта по противодействию гибридным

80.htm. Относительно анализа см.: Jamie Shea, "Resilience: A Core Element of Collective Defence," *NATO Review*, March 30, 2016, www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm. Соответствующий обзор обязательств НАТО по обеспечению устойчивости на национальном уровне в Madeleine Moon, "NATO's National Resilience Obligations," *RUSI Commentary*, March 15, 2019, https://www.rusi.org/commentary/NATOs-National-Resilience-Obligations.

[34] «ЕС будет способствовать устойчивости своих демократий и будет придерживаться ценностей, которые вдохновили его создание и развитие. К ним относятся уважение и поощрение прав человека, основных свобод и верховенства закона. Они включают справедливость, солидарность, равенство, недискриминацию, плюрализм и уважение к разнообразию. Последовательная внутренняя жизнь в соответствии с нашими ценностями будет определять наш внешний авторитет и влияние». "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy," June 2016, 15, и "State and Societal Resilience to Our East and South," 23-28, https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

[35] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication to the European Parliament and the Council. A Strategic Approach to Resilience in the EU's External Action," June 7, 2017, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52017JC0021; European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Tackling Online Disinformation: A European Approach," Brussels, April 26, 2018, https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach.

[36] European Commission, "Code of Practice on Disinformation," September 26, 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

[37] EEAS, "EU-NATO Cooperation – Factsheets," June 17, 2020, https://eeas.europa.eu/headquarters/headquarters-homepage/28286/eu-nato-cooperation-factsheet_en.

угрозам, действующих в качестве нейтрального посредника между ЕС и НАТО путем организации стратегических дискуссий и учений.[38]

Международные организации – как межправительственные, так и неправительственные, такие как ОЭСР, различные агентства ООН и IDEA International – предложили конкретные рамки для построения и укрепления государственной, социальной и демократической устойчивости. Сравнительный анализ этих инициатив на уровне демократических государств, ЕС и НАТО и других международных организаций, а также государственно-частных инициатив по реализации конкретных политик устойчивости, выходит далеко за рамки данной статьи.

Тем не менее, стоит упомянуть о некоторых мерах *по восстановлению доверия к демократическим институтам*, борьбе с дезинформацией и фальшивыми новостями, а также против компьютерной пропаганды. По сути, существует потребность в прочном базовом политическом образовании граждан и электората, а также в действиях по противодействию иностранному вмешательству и конкретным мерам наблюдения до начала голосования. «Постоянное развитие критического мышления и цифровых компетенций, особенно у молодых людей, имеет решающее значение для повышения устойчивости нашего общества к дезинформации».[39] Меры, предложенные Национальным демократическим институтом США, могут передать передовой опыт противодействия дезинформации в политике, особенно на выборах, соответственно путем проведения исследований уязвимости и устойчивости к дезинформации; мониторинг дезинформации и компьютерной пропаганды на выборах; усиление приверженности политических партий обеспечению достоверности информации; помощь платформам социальных сетей и техническим компаниям в «создании конфигураций для демократии»; обмен инструментами для обнаружения и устранения дезинформации и восстановления доверия к институтам и процессам посредством демократических инноваций.[40]

Развитие демократии в глобальном масштабе в новейшей истории имело свои приливы и отливы, но мы верим, что демократическая форма правления докажет свою привлекательность и устойчивость, несмотря на нынешние серьезные проблемы. В конце концов, это новая и более высокая форма вековой битвы за завоевание умов и сердец. Устоявшиеся демократии все больше осознают новые вызовы и начали существенную правовую и нормативную работу по повышению устойчивости демократических институтов и процессов. Вызовы и угрозы, представленные в статье, указывают на долгосрочную тенденцию, эволюцию которой трудно предсказать.

---

[38] European Centre of Excellence for Countering Hybrid Threats, “Functions of Hybrid CoE,” https://www.hybridcoe.fi/.

[39] European Commission, “Tackling Online Disinformation.”

[40] National Democratic Institute, “Info/tegrity. An NDI Initiative to Protect the Integrity of Political Information,” https://www.ndi.org/infotegrity.

Нормативно-правовая база реагирования на эти вызовы должна быть скоординирована и постоянно адаптирована к быстро меняющейся среде угроз.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами авторов и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Благодарность

Журнал *Connections: The Quarterly Journal*, Vol. 19, 2020 издается при поддержке правительства США.

Об авторах

Д-р **Йоан Мирча Пашку** – профессор международных отношений Национальной школы политических и административных исследований (с 1990 года). Он был вице-президентом Европейского парламента (ноябрь 2014 - июль 2019 г.), заместителем председателя Комитета по иностранным делам Европейского парламента (2007-2017 гг.). Был министром обороны Румынии (2000-2004 гг.), внес значительный вклад в принятие Румынии в НАТО. Советник президента, руководитель отдела внешней политики Администрации президента Румынии (1990-1992), вице-президент Фронта национального спасения (1990-1992), государственный секретарь, заместитель министра обороны (1993-1996), председатель Комитета по обороне, общественному порядку и национальной безопасности Палаты депутатов румынского парламента (1996–2000 годы), член румынского парламента (1996–2007 годы), вице-президент Социал-демократической партии (1997–2006 годы). Декан факультета международных отношений Национальной школы политических и административных исследований (1990–1996 годы). Заведующий кафедрой международных отношений Национальной школы политических и административных исследований (2004–2009 годы).
E-mail: puiu.pascu@gmail.com

Д-р **Николае-Серджиу Винтила** в настоящее время работает политическим аналитиком в Европейской парламентской исследовательской службе Европейского парламента. Он был советником по политике профессора Йоана Мирчи Паску, депутата Европарламента, вице-президента Европейского парламента, в период с 2009 по 2019 год. С 2001 по 2009 год он занимал руководящие должности в Министерстве обороны Румынии. Доктор Винтила был исследователем в Румынской академии (1990–1997), а с 1990 года он является лектором и доцентом в области международных отношений и ведет курсы в основном для аспирантов в Национальной школе политических исследований и государственного управления в Бухаресте и Люксембургском университете. Он пишет от своего имени.
E-mail: nicolae-sergiu.vintila@ext.uni.lu