DOI: https://doi.org/10.37547/supsci-ojhpl-05-05-43 Pages: 388-396

Oriental Journal of History, Politics and Law

ORIENTAL JOURNAL OF HISTORY, POLITICS AND LAW

journal homepage:
https://www.supportscience.uz/index.php/ojhpl

INFORMATION ATTACKS ON TRANSNATIONAL CORPORATIONS AS A NEW FORM OF HYBRID WARFARE

Takhmina Mamadaliyeva
Lecturer
Tashkent State Transport University
Tashkent, Uzbekistan
E-mail: mishel.96@bk.ru

ABOUT ARTICLE

Key words: information attacks, transnational corporations, cyber threats, hybrid warfare, sanctions, digital sovereignty, international security.

Received: 19.05.25
Accepted: 21.05.25
Published: 23.05.25

Abstract: This article analyzes information attacks on transnational corporations (TNCs) as a key element of modern hybrid warfare. Using case studies involving companies such as Huawei, TikTok, and Microsoft, it explores the linkage between media campaigns, legal pressure, and the imposition of economic sanctions. Special attention is given to the broader consequences of such attacks on international relations, global supply chains, and the investment climate.

TRANSMILLIY KORPORATSIYALARGA QARSHI AXBOROT HUJUMLARI — GIBRID URUSHNING YANGI SHAKLI SIFATIDA

Taxmina Mamadaliyeva
O‘qituvchi
Toshkent Davlat Transport Universiteti
Toshkent, O‘zbekiston
E-mail: mishel.96@bk.ru

MAQOLA HAQIDA

Kalit so‘zlar: axborot hujumlari, transmilliy korporatsiyalar, kiberxavflar, gibrid urush, sanksiyalar, raqamli suverenitet, xalqaro xavfsizlik.

Annotatsiya: Ushbu maqola transmilliy korporatsiyalarga (TMK) qarshi axborot hujumlarini zamonaviy gibrid urushning muhim elementi sifatida tahlil qiladi. Huawei, TikTok va Microsoft kabi kompaniyalar bilan bog‘liq voqealar asosida axborot kampaniyalari, huquqiy bosim va iqtisodiy sanksiyalar o‘rtasidagi o‘zaro bog‘liqlik ochib beriladi. Shuningdek, bu hujumlarning xalqaro munosabatlar, global ta'minot zanjirlari va

investitsiya muhiti uchun oqibatlari ko‘rib chiqiladi.

ИНФОРМАЦИОННЫЕ АТАКИ НА ТРАНСНАЦИОНАЛЬНЫЕ КОРПОРАЦИИ КАК НОВАЯ ФОРМА ГИБРИДНОЙ ВОЙНЫ

Тахмина Мамадалиева
Преподователь
Ташкентский государственный университет путей сообщения
Ташкент, Узбекистан
E-mail: mishel.96@bk.ru

О СТАТЬЕ

Ключевые слова: информационные атаки, транснациональные корпорации, киберугрозы, гибридная война, санкции, цифровой суверенитет, международная безопасность.

Аннотация: Статья посвящена анализу информационных атак на транснациональные корпорации как элемента современной гибридной войны. Рассматриваются кейсы воздействия на такие компании, как Huawei, TikTok и Microsoft, а также прослеживается взаимосвязь между информационными кампаниями, юридическим давлением и введением экономических санкций. Особое внимание уделено влиянию подобных атак на международные отношения, глобальные цепочки поставок и инвестиционный климат.

ВВЕДЕНИЕ

В условиях глобализации и углубляющейся взаимозависимости государств, транснациональные корпорации (ТНК) становятся не только экономическими субъектами, но и важными фигурантами глобальной политической конфигурации. Их масштаб, ресурсы и степень влияния на рынки и цепочки поставок приравнивают крупнейшие ТНК к негосударственным геоэкономическим акторам, способным влиять на международные процессы. Эта растущая значимость делает их уязвимыми в условиях нарастающей конкуренции в киберпространстве, где информационные атаки становятся инструментом гибридных стратегий влияния со стороны государств и иных сил.

Кибератаки против ТНК часто являются частью более широких стратегий – например, попыток ограничить присутствие определённой корпорации на стратегических рынках, получить доступ к чувствительной информации или нанести ущерб критически важной инфраструктуре. Известны случаи, когда информационные вбросы и цифровые саботажи координировались с кампаниями по дискредитации компаний в медиа, с последующим падением их котировок на фондовых рынках и снижением инвестиционной привлекательности. Это подтверждает тот факт, что гибридные воздействия на ТНК не

ограничиваются лишь киберпространством, а охватывают финансовую, информационную и правовую сферы.

Особую тревогу вызывает то, что отсутствие единых международных норм поведения в киберпространстве затрудняет защиту ТНК от подобного рода атак. В результате корпорации оказываются в зоне правовой неопределённости, где они вынуждены самостоятельно выстраивать стратегии киберустойчивости, вкладывая значительные средства в цифровую безопасность и корпоративную разведку. Однако даже при наличии продвинутых систем защиты, растёт вероятность того, что ТНК будут всё чаще становиться мишенями геополитических конфликтов, особенно в высокотехнологичных секторах — энергетике, телекоммуникациях, фармацевтике, ВПК. Это создаёт дополнительные риски для глобальной экономической стабильности. Потери ТНК, перебои в поставках, утечка данных и подрыв доверия к брендам могут иметь домино-эффект, затрагивая смежные отрасли, транснациональные альянсы и финансовые системы. Более того, постоянная угроза кибердестабилизации влияет на инвестиционное поведение и доверие к международным рынкам, провоцируя возрастание протекционистских тенденций и цифрового суверенитета.

Целью настоящей статьи является анализ способов применения информационных атак и киберугроз в отношении транснациональных корпораций (ТНК), а также выявление взаимосвязей между этими действиями, экономическими санкциями и стратегическими интересами в сфере международной политики.

В условиях трансформации глобальной архитектуры безопасности и нарастающей цифровой конфронтации, информационные воздействия становятся неотъемлемой частью внешнеполитических инструментов. Настоящее исследование направлено также на переосмысление роли ТНК в условиях роста транснациональных рисков. Особое внимание уделяется взаимосвязи между цифровыми угрозами и геоэкономической конкуренцией, а также влиянию этих процессов на глобальное распределение власти и доверие к мировым институтам.

Методологическая основа исследования строится на междисциплинарном подходе, сочетающем качественные и количественные методы анализа, что позволяет всесторонне осмыслить природу информационно-киберугроз в отношении транснациональных корпораций. Для достижения поставленных целей статьи применяются контент-анализ, дискурс-анализ. Также, задействуются элементы политико-экономического анализа, включающие оценку влияния информационных атак и киберугроз на глобальные экономические процессы, трансформацию внешнеполитических стратегий и изменение конфигурации международной экономической стабильности.

Результаты

В рамках исследования были проанализированы резонансные кейсы, демонстрирующие, каким образом транснациональные корпорации становятся объектами информационного давления и кибератак, тесно увязанных с геополитическими интересами государств. Были рассмотрены примеры (Huawei, TikTok, Microsoft) которые позволили зафиксировать устойчивую стратегию воздействия, при которой цифровые угрозы используются в комплексе с политическим и экономическим инструментарием.

Одним из наиболее показательных кейсов выступает китайская корпорация Huawei, оказавшаяся в эпицентре международных обвинений в шпионаже и нарушении норм национальной безопасности. В первую очередь, речь идёт о действиях Соединённых Штатов, инициировавших масштабную кампанию, включающую как санкции и запрет на использование оборудования Huawei в проектах 5G, так и систематические информационные атаки. Через утечки данных, судебные иски и давление на союзников в рамках альянсов типа Five Eyes формируется устойчивый нарратив угрозы, встраивающий технологическую корпорацию в дискурс о цифровом суверенитете и зависимости от Китая. Для синергетического эффекта репутационного давления, информационные публикации СМИ сопровождались официальными заявлениями.

Другим значимым примером является TikTok, платформа китайского происхождения, оказавшаяся под пристальным вниманием американских и европейских регуляторов. В риторике официальных лиц TikTok представляется как потенциальный инструмент влияния, способный собирать персональные данные и вмешиваться в информационное поведение граждан. Угрозы о запрете приложения в США сопровождались не только юридическими инициативами, но и активной информационной кампанией в публичном пространстве, целью которой было подорвать доверие к платформе как к нейтральному цифровому сервису. В следствии чего, эта ситуация демонстрирует, что информационная атака может существовать как автономный инструмент давления, усиливающий санкционные меры и способный мобилизовать общественное мнение в нужном направлении.

Microsoft. Хакерская атака через уязвимость в системе SolarWinds, затронувшая десятки правительственных и корпоративных структур, выявила уязвимость даже крупнейших технологических корпораций перед координированными кибероперациями. Расследование инцидента было сопровождено масштабным информационным освещением, где акцент делался на недостаточную защищённость облачных сервисов и потенциальные угрозы от внешнего вмешательства в критическую цифровую инфраструктуру. Это стало поводом для корректировки стратегий информационной безопасности как со стороны

частных компаний, так и государственных структур, включая формирование новых стандартов взаимодействия в условиях киберрисков.

Все рассмотренные кейсы свидетельствуют о наличии чётко структурированных целей информационно-кибервоздействий. Во-первых, такие атаки нацелены на подрыв доверия к транснациональным корпорациям, как в глазах потребителей, так и в рамках государственно-политических структур. Во-вторых, они способствуют созданию атмосферы нестабильности и политического давления, особенно в контексте гибридных конфликтов, где границы между экономическим и информационным противостоянием размыты. В-третьих, за такими действиями нередко стоит стратегическое стремление получить преимущество на международной арене, используя контроль над цифровыми технологиями как ресурс власти в новой геоэкономической реальности.

Транснациональные корпорации, оказавшиеся в фокусе таких атак, интенсифицируют инвестиции в кибербезопасность, внедряют механизмы оперативного реагирования на утечки и атаки, а также усиливают публичные коммуникации, направленные на восстановление репутации и укрепление доверия. Государства, в свою очередь, прибегают к комплексному инструментарию, включая санкции, ужесточение нормативной базы и собственные информационные кампании. Сращивание кибер и информационного воздействия с политико-правовыми механизмами давления усиливает транснациональный характер конфликта.

Анализ выявляет, что подобные инциденты получают широкий международный отклик, вовлекая не только непосредственных участников, но и страны-наблюдатели, обеспокоенные нарушением норм международной цифровой безопасности. Реакция государств остаётся неоднородной: в то время как одни государства поддерживают ограничительные меры, другие занимают более нейтральную или прагматичную позицию, исходя из собственных экономических интересов и технологических зависимостей.

Представленные результаты демонстрируют, что информационные и кибератаки против транснациональных корпораций являются не эпизодическими, а системными проявлениями гибридной конфронтации, отражающими всё более тесную взаимосвязь между технологией, безопасностью и международной политикой.

Анализ собранных кейсов и материалов позволяет выявить чёткую структурную взаимосвязь между информационными атаками на транснациональные корпорации (ТНК) и последующим введением юридических и экономических санкций. Подобная взаимосвязь проявляется не как случайное совпадение, а как поэтапная стратегия эскалации давления, встраиваемая в контекст гибридной внешней политики.

На начальном этапе формируется репутационный нарратив, направленный на подрыв доверия к корпорации. Это достигается путём информационных кампаний, в которых транслируются обвинения в нарушениях — шпионаже, сборе данных, подрывной деятельности — с активным использованием медиаресурсов, официальных заявлений и докладов аффилированных аналитических структур. Нередко источниками становятся прокси-акторы, действующие от имени государства либо через косвенные каналы — НКО, экспертов, информационные платформы. Подобные атаки на репутацию создают негативный образ компании как «угрозы национальной безопасности» или «инструмента влияния враждебного государства».

Следующим этапом, логически вытекающим из сформированной общественно-политической атмосферы, становится юридическое давление. Основанием служат уже распространённые информационные материалы, которые начинают рассматриваться как предварительные основания для запуска проверок, возбуждения судебных процессов или пересмотра лицензионных соглашений.

Завершающим этапом становится введение экономических санкций, которые представлены как необходимая мера реагирования на выявленные угрозы. Санкции включают замораживание активов, запреты на экспорт и импорт, ограничения на участие в государственных тендерах, ограничения на доступ к технологиям и финансовым инструментам.

Репутационная атака становится ключевым элементом, формирующим социальное и политическое обоснование для всех последующих шагов. Пример Huawei наглядно иллюстрирует этот механизм: от публикаций в западных СМИ и отчётов о якобы возможной передаче данных китайским спецслужбам, через запуск уголовных дел и антимонопольных расследований в ряде стран, к санкциям со стороны США и ограничению доступа к критически важным компонентам, таким как полупроводники и программное обеспечение. Аналогично развивалась ситуация с TikTok, когда информационная кампания предшествовала законодательным инициативам и угрозам о полном запрете деятельности в США.

Исследование показало, что современные информационные и кибератаки, направленные против транснациональных корпораций, всё чаще выходят за рамки экономической конкуренции и приобретают выраженный геополитический характер. Они становятся катализаторами политической напряжённости и инструментом перераспределения влияния в международной системе. Эти процессы оказывают многоуровневое воздействие – от трансформации дипломатических отношений до трансформации глобального инвестиционного климата.

Противостояние между ключевыми акторами мировой политики – США, Китаем и Европейским союзом – усугубляется в условиях киберугроз, направленных на корпорации, выступающие как технологические символы государств. Атаки на Huawei, TikTok или Microsoft сопровождаются обвинениями в нарушении цифрового суверенитета и правовых норм, что усиливает атмосферу взаимного недоверия. Экономическое давление на ТНК посредством информационных атак и санкций оказывает непосредственное влияние на устойчивость глобальных цепочек поставок. Так, санкции в отношении Huawei повлияли не только на китайский рынок, но и на ряд европейских производителей компонентов и телекоммуникационного оборудования.

Инвестиционная привлекательность также оказывается под угрозой. Неопределённость, связанная с киберугрозами, ухудшает прогнозируемость бизнес-среды и повышает риски для инвесторов. Это приводит к замедлению инновационного развития. Усиление давления в сфере цифровой безопасности трансформирует логику инвестиционного планирования, смещая фокус с эффективности на защищённость.

В ответ на возрастающие риски транснациональные корпорации реализуют многоуровневые стратегии адаптации. Среди ключевых мер является снижение зависимости от определённых регионов и поиск более нейтральных юрисдикций для операционной деятельности. Это позволяет минимизировать последствия санкций и политических рисков, а также повысить гибкость в условиях быстро меняющейся глобальной повестки. В ряде случаев компании принимают решение о стратегическом уходе с национальных рынков, где воздействие со стороны государства становится экономически и репутационно недопустимым. Такие действия влияют на географическую конфигурацию глобального бизнеса, усиливая сегментацию мировой экономики.

Особую роль в эволюции данной проблематики играет концепт цифрового суверенитета, получивший широкое распространение как на уровне ЕС, так и в Китае, России, Индии. Государства стремятся взять под контроль цифровую инфраструктуру, развивая собственные технологические экосистемы, ограничивая влияние иностранных платформ и навязывая локализацию данных. В результате формируется тренд на фрагментацию глобального цифрового рынка, подрывающий универсальность интернета и открытость цифровых инноваций.

Информационные и кибератаки против ТНК оказывают многослойное воздействие на международные отношения и глобальную экономику. Они становятся частью структурной трансформации мировой политико-экономической системы, усиливая конфронтацию между центрами силы, провоцируя рост цифрового протекционизма и создавая новые вызовы для глобального бизнеса.

Информационные атаки на транснациональные корпорации в современных условиях становятся неотъемлемым элементом гибридной конфронтации, где цифровое давление и репутационные удары служат продолжением политико-экономической борьбы между государствами. В условиях нарастающей взаимозависимости и технологической уязвимости, обеспечение устойчивости транснациональных корпораций к информационно-киберугрозам становится задачей не только бизнеса, но и международной политики. Необходим пересмотр существующих подходов. Но, для начала, в настоящее время особо важно разработать унифицированные международные правовые нормы. В перспективе только синтез усилий частного сектора, государственных институтов и международных организаций способен сформировать более сбалансированную и безопасную цифровую среду.

Литература

1. Ukraine war: Hackers are hitting Western companies with disinformation, sabotage campaigns. *CNBC*. 14 June 2023. https://www.cnbc.com/2023/06/14/ukraine-war-hackers-are-hitting-western-companies-with-disinformation.html

2. "Global cybersecurity rules urgently needed to tackle growing threats – UN." Reuters, 27 October 2022. https://www.reuters.com/world/global-cybersecurity-rules-urgently-needed-tackle-growing-threats-un-2022-10-27/

3. "The top cybersecurity threats for global businesses in 2023." World Economic Forum, January 2023. https://www.weforum.org/agenda/2023/01/cybersecurity-threats-global-businesses-2023/

4. "Huawei: Why the US is targeting China's tech giant." BBC News, 30 January 2020. https://www.bbc.com/news/technology-51312294

5. Triolo, P., Allison, K., & Brown, E. (2020). Huawei and the Global Battle Over 5G. Eurasia Group White Paper.

6. Thompson, N., & Warner, B. (2021). The TikTok Threat: How the US Government Is Using National Security to Redefine Digital Sovereignty. International Journal of Communication, 15, 2234–2256.

7. Sanger, D. E. (2021). The SolarWinds Hack: The Fallout and the Future of Cyberwar. The New York Times.

8. Feldstein, S. (2019). The Global Expansion of AI Surveillance. Carnegie Endowment for International Peace.

9. "Cybersecurity strategy and transformation." *PwC Global*. https://www.pwc.com/gx/en/issues/cybersecurity/cybersecurity-strategy-transformation.html

10. "Significant Cyber Incidents in 2023." Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/significant-cyber-incidents-2023

11. The geopolitics of cybersecurity." Brookings Institution. https://www.brookings.edu/articles/the-geopolitics-of-cybersecurity/

12. Klimburg, A. (2017). The Darkening Web: The War for Cyberspace. Penguin Press.

13. Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. International Journal of Law and Information Technology, 19(3), 187–223.

14. Pawlak, P. (2020). Cybersecurity and Geopolitics: The Rise of Digital Sovereignty. European Union Institute for Security Studies.

15. Gertz, G. (2020). Huawei and the US-China Tech Cold War. Foreign Policy Research Institute.

16. Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.

17. Pohle, J., & Thiel, T. (2020). Digital Sovereignty. Internet Policy Review, 9(4), 1–17.