

Природа международной конфликтности в социодинамике цифровой трансформации

Н. Н. Левчук,

главный научный сотрудник, доктор политических наук,

Научно-исследовательский институт Вооруженных Сил Республики Беларусь;

Д. А. Войсковой,

заместитель начальника отдела,

581-й Главный центр анализа и прогноза Вооруженных Сил Республики Беларусь

В статье на основе анализа социодинамики цифровой трансформации раскрывается природа международной конфликтности. В качестве системообразующей основы такой конфликтности представлена тенденция систематических попыток формирования международных отношений в русле американской модели глобального доминирования. Анализируется использование политических технологий цветных революций и других дестабилизирующих стратегий в парадигме цифровой трансформации. Разработан типовой алгоритм развязывания вооруженного конфликта и войны, отражающих высшую степень проявления международной конфликтности.

Ключевые слова: международная конфликтность; глобальная политика; цифровая трансформация; киберфизические системы.

The article, based on an analysis of the sociodynamics of digital transformation, reveals the nature of international conflict. As a system-forming basis for such conflict, the tendency of systematic attempts to form international relations in line with the American model of global dominance is presented. The use of political technologies of color revolutions and other destabilizing strategies in the paradigm of digital transformation is analyzed. A typical algorithm for unleashing armed conflict and war has been developed, reflecting the highest degree of manifestation of international conflict.

Keywords: international conflict; global politics; digital transformation; cyberphysical systems.

В решении проблемы, сформулированной в настоящей статье, следует исходить из того, что международная конфликтность характеризуется противоборством государств, коалиций стран, а также политических сил внутри них. Социодинамика цифровой трансформации предопределяет формы и способы реализации потенциала международной конфликтности, а ее природа реализуется на основе объективно существующих взаимосвязанных процессов международных отношений. На наш взгляд, политическую природу международной конфликтности характеризует типовой алгоритм развязывания войны или вооруженного конфликта, разработанный авторами настоящей статьи, а существенной характеристикой природы международной конфликтности является потребность в устранении силовыми инструментами диспропорций источников экономического роста между военно-политическими союзами и геополитическими центрами силы с применением технологий нового технологического уклада, интегрированных на основе цифрового управляющего контура.

Первый шаг алгоритма – насаждение при помощи биржевых и иных инструментов глобального или регионального финансового и экономического кризиса. *Второй шаг* – консолидация при помощи средств социальной инженерии на этнической и социокультурной почве протестных ресурсов, способных стать движущей силой массовых беспорядков и возникновения вооруженного конфликта. *Третий шаг* – создание политических условий для возникновения массовых беспорядков, конструирование и актуализация шокового события-драйвера (террористический акт и др.), как правило, связанного с убийствами людей, с целью создания почвы для развязывания внутреннего вооруженного конфликта. *Четвертый шаг* – мятеж: социально-политическая дестабилизация, провоцирование массовых беспорядков. *Пятый шаг* – наращивание и реализация конфликтного потенциала пропагандистскими и политическими средствами до такого уровня напряженности, когда реализованный провокационный инцидент или серия инцидентов превращаются

в военный (внутренний вооруженный) конфликт. *Шестой шаг* – внешнее вмешательство (война).

В современных условиях средой возникновения и развития политического конфликта выступает информационная сфера, в которой находят воплощение как общественные противоречия, так и борьба за ресурсы, а также любые конфликтные взаимоотношения [1] между ее субъектами. Типовым условием его возникновения в Беларуси является дестабилизация извне социально-политической обстановки, а под информационной сферой подразумевается область деятельности людей, связанная с созданием, преобразованием и потреблением информации. Эта сфера под воздействием непрерывного процесса цифровой трансформации проявляет себя как киберфизическая среда взаимодействия политических субъектов.

В глобальном контексте цифровые технологии реализуются в виде санкционного инструментария геополитического противоборства, как в случае с решением ЕС об отключении нескольких белорусских банков от платформы передачи финансовых сообщений SWIFT, ограничением доступа к высоким технологиям. Сегодня цифровые блокчейн-системы форматируют взаимодействие международных экономических блоков, а технологические платформы предопределяют границы политических союзов. В широком обиходе противоборствующих сторон на разных уровнях политического конфликта находится применение киберсаботажа, а контуры нового «железного занавеса», выстраиваемого коллективным Западом в ходе объявленной им тотальной санкционной войны, имеют цифровые очертания.

Когнитивная среда политического конфликта обеспечивается существованием глобальной информационной инфраструктуры, имеющей сетевой характер и играющей стратегическую роль в нарастании потенциала конфликтности между геополитическими центрами силы. Но киберфизический характер взаимодействия в ней в большей степени выявляет эволюция современных промышленных систем. В данном контексте вызовы четвертой промышленной революции вторгаются в область политических трансформаций и реализуются посредством применения сетевого инструментария геополитического противоборства.

Поступательное созревание технологических условий четвертой промышленной революции обуславливает интеграцию в среду информационной сферы киберфизических систем (КФС) [2], образуемых в процессе цифровизации. Формат и основные направления развития таких систем задают инновационные промышленные практики, реализуемые в цифровой концепции «Индустрия 4.0» (рис. 1) и «умной фабрике» [3] как ее технологическом ядре. В более широкой трактовке КФС – это «умные» сети электроснабжения, «умные» дома, «умные» города. В операционном отношении КФС составляют датчики, оборудование и информационные системы, охватывающие как отдельные объекты, так и комплексы объектов. КФС как сетевая

система может включать интернет вещей, промышленный интернет, «умные» энергетические сети, системы больших данных, системы облачных и туманных вычислений, системы дополненной реальности.



Рис. 1. Индустрия 4.0 [3]: киберфизическая система

На уровне функционирования человеко-машинных систем КФС становятся объектами воздействия в войнах нового поколения, которые синтезируют определенный спектр вызовов и угроз, комплексно воздействующих на среду безопасности [4]. Как показывает международный опыт, через информационное пространство фактически происходит вмешательство во внутренние дела государства, преднамеренная дискредитация его конституционных основ, побуждение к гражданскому неповиновению [5]. А это и есть политический конфликт, который в крайнем проявлении представляет собой войну, сопровождаемую увеличением объема передаваемой информации, ростом требований к системам разведки и управления, сокращением циклов управления войсковыми формированиями [6]. При этом сами по себе средства ведения и обеспечения вооруженной борьбы являются сложными автоматизированными устройствами, связанными между собой по сетевому принципу, которые тоже могут быть идентифицированы как КФС.

В грубом приближении КФС – это усложненный интернет вещей, сам по себе рассматриваемый в качестве КФС. Его возникновение, реализующее возможность телекоммуникационной связи между физическими объектами, находящимися в непосредственном пользовании человека, за последние десятилетия существенно расширило перечень объектов для возможных кибератак. В Беларуси мониторинг и противодействие подобным инцидентам осуществляются на системной основе, функционирует Национальный центр реагирования на компьютерные инциденты [7].

Эволюция КФС позволила деструктивным силам в Беларуси впервые опробовать новую системную стратегию цветной революции. Она была основана на технологии «разрозненного майдана», когда «народные» выступления были организованы не только на одной из крупных площадей столицы, но и во всех областных и крупных районных центрах. Перед началом акций протеста проводилось целенаправленное информационное воздействие на население с исполь-

зованием социальных сетей, мессенджеров и телеграм-каналов. Расшатывание обстановки накануне выборов, координация действий деструктивных сил в ходе массовых беспорядков осуществлялись объединенным оппозиционным штабом.

Одним из координирующих хабов был получивший скандальную известность деструктивный телеграм-канал с польской «пропиской». Накануне выборов там были размещены практические рекомендации («памятка протестующим») по силовому захвату власти в стране. В «памятке» содержался порядок действий при подготовке к участию в уличных беспорядках (одежда, экипировка и амуниция, телефоны правозащитных организаций); порядок действий при использовании личного автотранспорта в ходе беспорядков; порядок действий при использовании правоохранительными органами специальных средств; порядок передачи команд (сигналов) в ходе столкновений при отсутствии или неустойчивой работе сети Интернет. Особое внимание отводилось обучению тактике действий протестующих при противостоянии с правоохранительными органами – «боевые» построения и перестроения, рассредоточение, отступление, быстрое перемещение и сбор во вновь назначенной точке, возведение и удержание баррикад, порядок применения самодельных взрывных устройств (средств поражения), вывод из строя специальной техники правоохранительных органов, занятие и перекрытие основных транспортных артерий и создание транспортного коллапса.

Эти и другие протестные действия предполагают сетевую координацию, которая на уровне современных технических средств осуществима даже при полной блокировке доступа к сети Интернет в локализованных местах городского пространства. Функционирование человеко-машинных систем, имея соизмерительный потенциал технологического обновления в виде «шлакового» выброса социально-политического процесса, реализуется на уровне применения дестабилизационных технологий.

Онтологический «разлом» политического конфликта здесь пролегает по линии противоборства сети, бросающей вызов государственной иерархии, которая парадоксально использует ее же механизмы для ответного противодействия. В процессе цифровой трансформации «глобальный социум», содержащий внутри своего контура заряды многих политических конфликтов, проявляет себя в функциональной среде нового качества, обусловленного киберфизическим симбиозом. Это происходит в социодинамике цифровой трансформации, реализующей техносотциальную природу международной конфликтности в процессе формирования нового технологического уклада.

Как следует из разработанного авторами алгоритма, природа международной конфликтности в процессе возникновения и нарастания реализуется через внутрисоциальный конфликт и лишь на окончательных стадиях его развития выходит на международный уровень. То есть, на наш взгляд, международ-

ная конфликтность содержит внутрисоциальную дестабилизационную природу, в которой воплощены внешние противоречия, возникающие в процессе столкновения геополитических центров силы с их экономическими и социокультурными интересами.

Доктор политических наук Е. Г. Пономарева замечает, что уже на подготовительной стадии белорусских протестов были апробированы основные технологии дестабилизации: массовые протестные акции с применением цепок и провоцированием ОМОН, пикеты солидарности различных уровней, флешмобы, челленджи (жанр интернет-роликов, в которых блогер выполняет задание на видеокамеру) [8]. Уровень координации протестов свидетельствует о нарастании «социальной тесноты» сетевого взаимодействия. И здесь необходимо уточнение понятия КФС, преодоление бытующего стереотипа о ее сугубо промышленной интерпретации, связанной с внедрением вычислительных ресурсов в физические сущности любого типа.

Такая модель не самодостаточна без человеческого разума как ее априорного сущностного признака, а значит, к физическим и программным компонентам КФС добавляются мыслительные и поведенческие алгоритмы, формализуемые на уровне новейших технологий в виде искусственного интеллекта. Цифровая эволюция информационной сферы привела к формированию киберфизической среды массовой коммуникации, предполагающей, кроме прочего, ее артикуляцию в формате политического конфликта – типичное поведение человека в нем рассматривается, как правило, в симбиозе с техносферой.

Список использованных источников

1. Бурдые, П. О символической власти / П. Бурдые // Социология социального пространства. – М.: Ин-т эксперимент. социологии; СПб.: Алетейя, 2007. – С. 87–96.
2. Казарин, О. В. Классификация угроз безопасности для киберфизических систем / О. В. Казарин // Комплексная защита информации: материалы XXIV науч.-практ. конф., Витебск, 21–23 мая 2019 г. – Витебск, 2019. – С. 59–63.
3. Современные концепции развития цифровой экономики [Электронный ресурс] // Ростех. – 2016. – Режим доступа: <http://ar2016.rostec.ru/digital-current/>. – Дата доступа: 29.10.2019.
4. Слипченко, В. И. Войны шестого поколения: оружие и военное искусство будущего / В. И. Слипченко. – М.: Вече, 2002. – 384 с.
5. Арчаков, В. Концепция информационной безопасности Республики Беларусь – взгляд в будущее / В. Арчаков, О. Макаров, А. Баньковский // Беларус. думка. – 2019. – № 3. – С. 24–31.
6. Смирнов, И. Противоборство в киберпространстве по взглядам военно-политического руководства ведущих зарубежных государств / И. Смирнов, Г. Алексеев // Зарубеж. воен. обозрение. – 2017. – № 6. – С. 8–14.
7. Целевая атака на транспортно-логистическую сферу // Национальный центр реагирования на компьютерные инциденты [Электронный ресурс]. – 2021. – Режим доступа: <https://cert.by/?p=1919>. – Дата доступа: 29.12.2021.
8. Пономарева, Е. Г. Протестное движение в Беларуси: эволюция, технологии, символы / Е. Г. Пономарева // Обозреватель – Observer. – 2021. – № 2. – С. 5–28.