



Инновации и технологии в русско-украинской войне

Имре Порколаб,¹ Иштван Локотош,² Ференц Давид³

¹ *Институт исследования оборонных инноваций, Будапешт, Венгрия, <https://defenseinnovation.hu>*

² *Университет Иштвана Сечени, Дьёр, Венгрия, <https://www.uni.sze.hu>*

³ *Институт передачи технологий, Национальная лаборатория совместных технологий, Будапешт, Венгрия, <https://www.techtra.hu>*

Аннотация: Технологии и инновации оказали существенное влияние на русско-украинскую войну, повлияв не только на вооружённый конфликт, но и на восстановление отвоеванных территорий и возобновление услуг. Мало кто верил, что Украина выстоит, когда в феврале 2022 года началось российское вторжение. В этой статье мы рассмотрим, как Украина благодаря своей способности использовать технологические достижения и применять инновационные решения добилась относительных успехов, отражая российскую агрессию. Мы сосредоточимся на фундаментальных различиях на ранних этапах войны, уделяя особое внимание умелому внедрению Украиной новых передовых западных продуктов и технологий двойного назначения.

Ключевые слова: Русско-украинская война, оборонные инновации, технологии двойного назначения

Вступление

Технологии и инновации оказали существенное влияние на русско-украинскую войну, повлияв не только на вооружённый конфликт, но и на восстановление отвоеванных территорий и возобновление услуг.¹ Когда в фев-

¹ Jason McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine," *TechInformed*, February 24, 2023, по состоянию на 4 мая 2023, <https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/>.

рале 2022 года началось полномасштабное российское наступление, мало кто верил, что Украина выстоит. Поскольку у России была армия, в два раза превосходящая украинскую, и оборонный бюджет, почти в десять раз превышающий её, преобладало мнение, что Киев падёт в течение недели-двух.² Однако в ход событий вмешался один фактор: технологии, и, соответственно, инновационная мощь нации.³ Инновационная мощь означает способность изобретать, адаптировать и внедрять новые технологии.⁴ Её значение состоит в том, как новые революционные технологии⁵ и связанные с ними открытия меняют наши теории геополитического определения нации.⁶

Украина добилась успеха, отражая российское вторжение, благодаря способности внедрять технологические инновации и применять инновационные решения. Украина не только остановила наступление на Киев в феврале 2022 года, но и устояла, когда военные действия в апреле переместились на Донбасс, где знание ситуации, открытая местность и более короткие пути снабжения были на стороне России. В сентябре 2022 года Украина вернула себе часть оккупированных территорий в ходе контрнаступления под Харьковом. Эти события резко контрастировали с эффективностью России в военных кампаниях в Крыму и Восточной Украине в 2014 году и её операцией в Сирии в 2015 году.

² Faine Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China," *Foreign Policy*, February 16, 2023, по состоянию на 10 июня 2023, <https://foreignpolicy.com/2023/02/16/ukraine-russia-war-drone-warfare-china/>; Nan Tian et al., "Trends in World Military Expenditure, 2022," SIPRI Fact Sheet, April 2023, 9-11, https://www.sipri.org/sites/default/files/2023-04/2304_fs_milex_2022.pdf.

³ По иной формулировке схожего содержания, это синергия между «прорывными» технологическими решениями и человеческими возможностями. См. также Zdzisław Śliwa, "The Synergy Between Technology and Soldiers in Warfare – The Russian Armed Forces Image During the War in Ukraine," *Wiedza Obronna* 281, no. 4. (2022): 53-69, <https://doi.org/10.34752/2022-d281>.

⁴ Eric Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," *Foreign Affairs* (March-April 2023): 40, <https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics>; См. также: Śliwa, "The Synergy Between Technology and Soldiers in Warfare," 55.

⁵ Новые, революционные и прорывные технологические инновации и области науки охватывают передовые вычислительные решения, науку о данных, искусственный интеллект, автономные транспортные средства и робототехнику, гиперзвуковые технологии, космические системы, биотехнологии и многое другое. См., например, Njall Trausti Fridbertsson, "Technological Innovation for Future Warfare," NATO Science and Technology Committee, Sub-Committee on Technology Trends and Security, 5-8, по состоянию на 20 марта 2023, <https://www.nato-pa.int/document/2022-future-warfare-report-fridbertsson-025-stctts>; Kelley M. Saylor, "Emerging Military Technologies: Background and Issues for Congress," Congressional Research Service Report R46458, updated February 22, 2024, 2, <https://sgp.fas.org/crs/natsec/R46458.pdf>.

⁶ Amy Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," *Foreign Affairs* 102, no. 1 (January-February, 2023): 54-70, 56-57, www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart.

Основное отличие на этом начальном этапе войны заключалось в том, что Украина более изобретательно использовала в операциях передовые западные продукты и технологии, в основном двойного назначения.⁷ Россия же, казалось, либо не может, либо не хочет широко применять свои технологические инновации на украинском театре военных действий.⁸ Разумеется, к официальным отчётам Украины об успешном внедрении следует относиться с долей скептицизма.⁹ На украинском ТВД¹⁰ продолжает доминировать обычная военная техника, но Киеву выгодно показать успехи современных систем вооружений, чтобы сохранить постоянную поддержку США и европейских союзников. По информации из открытых источников сложно определить, было ли использование конкретных технологических инноваций массовым или спорадическим.¹¹

Умелое применение украинскими военными современных систем вооружений и новых технологических решений удивило не только их противников, но и партнёров и союзников. Тем не менее, несмотря на сложность этих технологических инноваций и систем вооружения, маловероятно, что они определяют окончательный исход войны. По нашей оценке, роль обычных вооружений в русско-украинском конфликте останется ключевой, и нельзя утверждать, что война такого рода может иметь окончательный финал. Воюющие стороны часто стремятся превратить технологическое превосходство на поле боя в стратегическую победу. Обладание нужными технологиями имеет важное значение для эффективности, но наличие высоко-

⁷ Термин «двойного назначения» относится к технологическим решениям, которые служат как гражданским, так и военным целям. Парадокс возникает из-за того, что многие продукты и технологии изначально имеют множественное применение, однако их отличие заключается в изначальной разработке для конкретного гражданского и коммерческого использования. См. также Giulio Perani, *Military Technologies and Commercial Applications: Public Policies in NATO Countries*, NATO Research Fellowship, Rome: CeSPI, Final Report to the NATO Office for Information and Press (Rome, 1997), 5-6, www.nato.int/acad/fellow/95-97/perani.pdf.

⁸ О подобных заявлениях см. также Donatas Palavenis, "The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War," *Air Land Sea Application Center*, October 1, 2022, по состоянию на 26 мая 2023, www.alsa.mil/Portals/9/Documents/articles/221001_ALSA_Article_Donatas_Palavenis.pdf, 2-3; и Śliwa, "The Synergy Between Technology and Soldiers in Warfare," 57-59. Первый опыт войны в Украине показывает, что российской оборонной промышленности сложно производить современную военную технику без западных технологий, и существенные улучшения кажутся маловероятными даже при поддержке Ирана, Беларуси или Китая.

⁹ На данном этапе конфликта мы должны критически оценивать имеющуюся, но неполную информацию, признавая отсутствие достоверных и проверяемых показателей эффективности.

¹⁰ Fridbertsson, "Technological Innovation for Future Warfare," 4; Palavenis, "The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War."

¹¹ Margarita Konaev and Owen J. Daniels, "Agile Ukraine, Lumbering Russia: The Promise and Limits of Military Adoption," *Foreign Affairs*, March 28, 2023, www.foreignaffairs.com/ukraine/russia-ukraine-war-lumbering-agile.

качественной техники само по себе не компенсирует долгосрочных экономических издержек войны, а также связанных с этим политических и общественных последствий.¹²

Русско-украинская война не ограничивается полем боя и охватывает более широкую сферу технологий и стремления стран к технологическому превосходству.¹³ Наряду с военно-политическими событиями, технологическая конкуренция теперь определяет рейтинг государств, методы и средства ведения будущих войн. Переоценка украинского опыта даёт представление о ближайшем будущем, где вооружённые конфликты будут вестись и выигрываться при помощи более тесного взаимодействия человека с машиной, с революционными технологическими инновациями и данными в качестве движущих сил для стран. Основываясь на первоначальном опыте войны, эта статья имеет целью предложить понимание значимости новых западных продуктов и технологий, в основном двойного назначения, которые появились в Украине.¹⁴ Наш анализ призван дать представление о том, как этот опыт может потенциально изменить картину вооружённых конфликтов и технологических инноваций.

Киберпространство и критическая инфраструктура

Различные кибератаки и меры противодействия им сыграли важную роль в русско-украинском конфликте.¹⁵ В феврале 2022 года физическому вторжению России предшествовали часы непрерывных кибератак в виртуальной среде, характеризующиеся распределёнными атаками типа «отказ в обслу-

¹² Исходя из геополитических соображений, Соединенные Штаты Америки в настоящее время оказывают — и будут оказывать — поддержку Украине, обеспечивая уровень обязательств путём поставок оружия. Однако, в отличие от двадцатилетнего присутствия в Ираке и Афганистане, русско-украинская война выявила истощение американских и европейских арсеналов и уязвимость их цепочек поставок. У Соединенных Штатов, похоже, нет ресурсов для продолжения долгосрочной поддержки Украины и одновременного сдерживания Китая на Тайване. См. Jacquelyn Schneider, "Does Technology Win Wars? The U.S. Military Needs Low-Cost Innovation — Not Big-Ticket Boondoggles," *Foreign Affairs*, March 3, 2023, www.foreignaffairs.com/ukraine/does-technology-win-wars; Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 43-44; Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

¹³ McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine."

¹⁴ Śliwa, "The Synergy Between Technology and Soldiers in Warfare," 55; Fridbertsson, "Technological Innovation for Future Warfare," 3, 5; Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 56-57, 63.

¹⁵ Хотя эти события часто называют первой «мировой кибервойной» (см., например, McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine," Kenneth R. Rosen, "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, <https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486>), таких преувеличений в терминологии следует избегать. Тем не менее действия в виртуальном пространстве во время атаки имели беспрецедентный эффект, по скорости и масштабу.

живании» и сбоями в работе информационных систем.¹⁶ За первыми атаками последовало применение российского кибероружия. Выявленные Microsoft вредоносные программы¹⁷ использовались для обрушения украинской интернет-сети и систем государственного управления, с повторяющимися попытками нанести дальнейший ущерб.

В ответ Украина быстро перевела свою цифровую инфраструктуру на облачные сервисы при поддержке европейских центров обработки данных.¹⁸ Этот стратегический шаг был направлен на защиту от дальнейших сбоев и укрепление киберспособностей Украины.¹⁹

Вторжение России и нанесённый ущерб не ограничились Украиной, затронув по меньшей мере 42 страны и 128 организаций.²⁰ Эта атака, в частности, нарушила работу высокопроизводительного геостационарного телекоммуникационного спутника KA-SAT, используемого Viasat.²¹ Важную роль в поддержке Украины сыграли американские и западные технологические компании, в частности, Cloudflare и Microsoft. Они помогли восстановить её цифровую инфраструктуру, повысить устойчивость систем и улучшить возможности шифрования.²² Ещё до вторжения Cloudflare зафиксировала рост атак типа «распределённый отказ в обслуживании» (DDoS).²³ Для обеспече-

¹⁶ Например, атаки DDoS (распределённый отказ в обслуживании), которые подавляют и выводят из строя сетевые сервисы и системы, перегружая их.

¹⁷ См., например, FoxBlade, Lasainraw (он же IsaacWiper), DesertBlade, FiberLake, SonicVote, CaddyWiper и т.д.; Microsoft, “Special Report: Ukraine. An Overview of Russia’s Cyberattack Activity in Ukraine,” April 27, 2022, 19-21, <https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/>.

¹⁸ Microsoft, “Special Report: Ukraine. An Overview of Russia’s Cyberattack Activity in Ukraine,” 19-12. Пока не ясно, придерживает ли Россия более эффективное кибероружие, или её возможности в этой области переоценены. Fridbertsson, “Technological Innovation for Future Warfare,” 4.

¹⁹ Microsoft, “Special Report: Ukraine. An Overview of Russia’s Cyberattack Activity in Ukraine,” 19; McGee-Abe, “One Year on: 10 Technologies Used in the War in Ukraine.”

²⁰ Microsoft, “Defending Ukraine: Early Lessons from the Cyber War,” June 22, 2022, 10-11, <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>.

²¹ Viasat, “KA-SAT Network Cyber Attack Overview,” March 30, 2022, по состоянию на 12 мая 2023, <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview>. Сбой 22 февраля 2022 года лишил доступа в Интернет тысячи украинских клиентов и десятки тысяч других пользователей проводной широкополосной связи. Отключение ограничивалось инфраструктурой Skylogic, дочерней компании Eutelsat, для Viasat. Оно не повлияло на прямых коммерческих, правительственных и других пользователей спутника KA-SAT Viasat. Ущерб от атаки типа «отказ в обслуживании» (DoS) был устранён за нескольких часов, а полностью система была стабилизирована в течение нескольких дней.

²² Fridbertsson, “Technological Innovation for Future Warfare,” 4.

²³ Взаимосвязь систем и технологических сервисов очевидна из того, что сбой в работе сервисов, вызванный атакой на отдельные элементы сети, первыми обнаружили США. См. Microsoft, “Special Report: Ukraine. An Overview of Russia’s Cyberattack Activity in Ukraine,” 6.

ния бесперебойной работы правительственных и телекоммуникационных систем Украины Cloudflare предоставила бесплатный доступ к своим услугам. Такое сотрудничество между США, западными технологическими структурами и Украиной имело решающее значение для решения проблемы кибератак.²⁴

Важно подчеркнуть, что физический и виртуальный ущерб во время конфликта наносились одновременно и были тесно взаимосвязаны.²⁵ Так, по данным украинского телекоммуникационного провайдера RETN,²⁶ на октябрь 2022 года 22 % оптоволоконной сети страны были повреждены и требовали постоянного ремонта.²⁷ С августа 2022 года также наблюдается заметное увеличение числа вредоносных кибератак, совпадающих с российскими авиационными и ракетными ударами. Эти кибератаки были нацелены на критически важные службы – поиска и спасения, здравоохранения – и организации, отвечающие за снабжение предметами первой необходимости – едой, водой, лекарствами. Этот синхронный и взаимосвязанный физический и виртуальный ущерб существенно усугубил общее воздействие конфликта, иллюстрируя многогранную природу современной войны.²⁸

Поскольку кибератаки, вероятно, будут сопровождать любой будущий конфликт, усиление механизмов защиты и устойчивости к таким угрозам имеет важное значение. Эти меры должны включать разработку передовых

²⁴ John Graham-Cumming, "Internet Traffic Patterns in Ukraine since February 21, 2022," *The Cloudflare Blog*, March 4, 2022, по состоянию на 14 мая 2023, <https://blog.cloudflare.com/internet-traffic-patterns-in-ukraine-since-february-21-2022/>; Matthew Prince, "Steps We've Taken around Cloudflare's Services in Ukraine, Belarus, and Russia," *The Cloudflare Blog*, March 7, 2022, <https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/>. Проект Cloudflare Galileo предлагает бесплатные услуги безопасности уязвимым, но социально значимым группам, сталкивающимся с угрозами DDoS и других кибератак. С февраля 2022 года 81 украинская организация, в первую очередь – в сфере чрезвычайных ситуаций, воспользовалась этой услугой, www.cloudflare.com/galileo/ (по состоянию на 24 апреля 2023).

²⁵ Microsoft, "Special Report: Ukraine. An Overview of Russia's Cyberattack Activity," 3-4; Microsoft, "Defending Ukraine: Early Lessons from the Cyber War," 7-9.

²⁶ Компания RETN, зарегистрированная в Великобритании, предлагает услуги по обеспечению пропускной способности, передаче данных и услуг электросвязи с IP в Европе и Азии как Украине, так и России. См. <https://www.retn.net> (по состоянию на 10 мая 2023).

²⁷ McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine." См. также: International Telecommunication Union (ITU), "Interim Assessment on Damages to Telecommunication Infrastructure and Resilience of the ICT Ecosystem in Ukraine" (ITU, December 2022), https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructure%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22_FINAL.pdf.

²⁸ Jocelyn Woolbright, "Nine Years of Project Galileo and How the Last Year Has Changed It," *The Cloudflare Blog*, June 5, 2023, <https://blog.cloudflare.com/nine-years-of-project-galileo-and-how-the-last-year-has-changed-it/>.

технологических возможностей и повышение автоматизации для сокращения времени реагирования человека, облегчая нагрузку на людские ресурсы.²⁹ Ввиду уязвимости физической инфраструктуры ожидается рост применения беспроводных сетей и облачных сервисов в телекоммуникационной отрасли. Однако эти изменения могут быть нивелированы постоянными угрозами вредоносного программного обеспечения, атак типа DDoS и высокими требованиями к энергопотреблению ИТ-систем. Поэтому для решения этих новых проблем в киберпространстве нужен комплексный подход, гарантирующий достаточную надёжность инфраструктуры и технологий, чтобы противостоять сложностям современной кибервойны и адаптироваться к ним.³⁰

Спутники и связь

По данным Государственной службы специальной связи и защиты информации Украины,³¹ на октябрь 2022 года были повреждены или уничтожены около 4000 ретрансляторов, 60 000 километров оптических кабельных линий и 18 вещательных станций.³² В этих тяжёлых условиях в Украине быстро поняли потенциал передовых технологических решений. После прямого обращения к SpaceX американская компания сделала доступ к своей спутниковой интернет-сети Starlink³³ бесплатным. Несмотря на масштабное разрушение инфраструктуры, эта инициатива позволила Украине сохранить и гражданскую, и военную связь.³⁴

Услуги, предоставляемые SpaceX³⁵ при помощи сети из 4000 спутников и более 42 000 наземных станций, обеспечили доступ граждан Украины к Интернету и дальнейшую координацию обороны.³⁶ Однако это решение вызвало и проблемы, из-за сложностей обслуживания и связанных с этим

²⁹ Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 49-50.

³⁰ "Branża telekomunikacyjna i jej największe wyzwania na 2023 rok," *ISB Tech*, 23 stycznia 2023, www.isbtech.pl/2023/01/branza-telekomunikacyjna-i-jej-najwieksze-wyzwania-na-2023-rok/.

³¹ См. <https://cip.gov.ua> и <https://cip.gov.ua/en/news/u-bukharesti-trivaye-povnovazhna-konferenciya-mizhnarodnogo-soyuzu-elektrozv-yazku-mse> (по состоянию на 12 мая 2023).

³² McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine;" Romina Bandura and Janina Staguhn, "Digital Will Drive Ukraine's Modernization," *Center for Strategic & International Studies (CSIS)*, January 10, 2023, по состоянию на 24 марта 2023, 2, <https://www.csis.org/analysis/digital-will-drive-ukraines-modernization>.

³³ Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

³⁴ Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 40.

³⁵ См. <https://www.starlink.com> (по состоянию на 10 мая 2023).

³⁶ На околоземной орбите работают около 7700 спутников (на 2023 год), более 4000 из них принадлежат проекту SpaceX Starlink. См. Stephen Clark, "SpaceX Rockets Past 4,000 Starlink Satellites in Orbit with Another Launch," *Spaceflight Now*, May 04,

расходов. Примечательно, что SpaceX не поддержала использование своего спутникового интернет-сервиса для наступательных операций, что Украина не полностью выполнила.³⁷ Поддержка бесплатного сервиса тоже стала финансово обременительной. В октябре 2022 года SpaceX объявила о планах прекратить финансовую поддержку, а в декабре 2022 года повысила плату за свои инструменты и услуги.³⁸ В итоге Украине для доступа к этому важному сервису теперь помогает правительство США.³⁹

Коммерческие спутники различных компаний неожиданно стали важным инструментом российско-украинского конфликта, в частности, благодаря широкому использованию спутниковых снимков и публичному разоблачению действий России.⁴⁰ Новым моментом тут стало не просто получение изображений Земли со спутников, что уже давно используется в различных целях, в том числе военных, а скорее резкий рост частного сектора в последнее десятилетие, что привело к быстрому увеличению доступности и охвата.⁴¹ Одним из главных преимуществ коммерческих спутниковых сетей стала скорость и простота доступа к важной информации. В отличие от государственных, часто засекреченных систем, практика обмена данными частных компаний заметно облегчила и ускорила поток данных, необходи-

2023, <https://spaceflightnow.com/2023/05/04/falcon-9-starlink-5-6-coverage/>. Подробнее см. <https://planet4589.org/space/con/star/stats.html> (по состоянию на 10 мая 2023).

³⁷ Аргумент Илона Маска таков: «[Starlink] — это основа связи Украины, особенно на линии фронта, где почти все другие интернет-каналы уничтожены. Но мы не допустим эскалации конфликта, которая может привести к Третьей мировой», <https://x.com/elonmusk/status/1624876021433368578>, February 12, 2023. Стоит отметить, что наряду с моральными соображениями, существенным фактором стали и значительные финансовые потери SpaceX, понесённые в результате работы Starlink в Украине. Подробнее см. Amritha Jayanti, “Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?” *Harvard Kennedy School, Belfer Center for Science and International Affairs*, March 9, 2023, www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose.

³⁸ McGee-Abe, “One Year on: 10 Technologies Used in the War in Ukraine.”

³⁹ Alex Marquardt, “Exclusive: Musk’s SpaceX Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick up the Tab,” *CNN Politics*, October 14, 2022, <https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html>.

⁴⁰ Fridbertsson, “Technological Innovation for Future Warfare,” 4.

⁴¹ По состоянию на 2023 год на орбите находилось 7700 спутников — намного больше, чем 11 в 2006 году. После 2015 года количество коммерческих спутников для наблюдения за Землей резко возросло, достигнув 596 к концу 2022 года. Примечательно, что две трети этих спутников принадлежат американским корпорациям. Подробнее см. UCS Satellite Database, www.ucsusa.org/resources/satellite-database (updated January 01, 2023).

мых для принятия военных решений.⁴² Технологии, используемые этими частными компаниями, возможно, не столь продвинуты, как у государственных систем, но качество их услуг продолжает улучшаться. Эти системы теперь могут обеспечить постоянное наблюдение за теми или иными областями и мониторинг изменений, предоставляя ценный ресурс в текущем конфликте.⁴³

Реакция Украины на российское вторжение включала беспрецедентный контроль и анализ обществом российских военных приготовлений и операций, что стало возможным благодаря поддержке восьми коммерческих спутниковых компаний при активной помощи США.⁴⁴ С самого начала конфликта важную роль в этих совместных усилиях сыграли такие американские компании, как Maxar Technologies, Planet⁴⁵ и BlackSky, имеющие опыт электрооптической съёмки.⁴⁶ Заметную помощь оказали также Microsoft⁴⁷ и Capella Space.⁴⁸

Исследователи и эксперты сыграли важную роль в анализе спутниковых снимков и событий в реальном времени, часто делясь своими выводами в соцсетях. Эта прозрачность позволила глубже понять конфликт и помогла привлечь агрессоров к ответственности. Группа студентов Стэнфордского университета продемонстрировала это, подготовив отчет для Организации Объединенных Наций, в котором задокументировала зверства российских

⁴² Mariel Borowitz, "War in Ukraine Highlights Importance of Private Satellite Companies," *Astronomy Online*, August 16, 2022, <https://www.astronomy.com/science/war-in-ukraine-highlights-importance-of-private-satellite-companies/>.

⁴³ Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 58, 60.

⁴⁴ Borowitz, "War in Ukraine Highlights Importance of Private Satellite Companies." При поддержке американских компаний и помощи правительства США Украина получила данные о более 40 млн. кв. км в первые две недели конфликта. Для сравнения, этого объема данных было бы достаточно для картографирования Украины пять раз в день или картографирования территории, оккупированной российскими войсками в марте 2022 года, и её изменений 18 раз в день. Открытых данных о точном покрытии спутниковых снимков нет, но считается, что оно включает украинскую территорию и оперативные и тыловые зоны украинских и российских войск.

⁴⁵ См., например, Planet Labs PBC, "Global Heritage Fund Leveraging Planet SkySat to Protect the Cultural Fabric of Ukraine," *Planet*, August 18, 2022, по состоянию на 25 марта 2023, <https://www.planet.com/pulse/global-heritage-fund-leveraging-planet-skysat-to-protect-the-cultural-fabric-of-ukraine/>.

⁴⁶ Courtney Albon, "Intelligence Agencies Accelerate Use of Commercial Space Imagery to Support Ukraine," *Defense News Online*, April 6, 2022, www.defensenews.com/battlefield-tech/space/2022/04/06/intelligence-agencies-accelerate-use-of-commercial-space-imagery-to-support-ukraine/.

⁴⁷ Microsoft, "Special Report: Ukraine. An Overview of Russia's Cyberattack Activity," 16.

⁴⁸ Capella Space – первая космическая компания США, которая запустила и использует спутники с РЛС с синтезированной апертурой (SAR), <https://www.capella.space.com> (по состоянию на 12 мая 2023); Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

военных в Украине. Для сбора информации и выводов они использовали комбинацию тепловых и электрооптических спутниковых снимков, видео TikTok, геолокационные приложения и другие инструменты.⁴⁹

Большую работу проделал и Институт изучения войны, который создал интерактивную карту украинского ТВД.⁵⁰ Эта карта была разработана на основе открытых несекретных первоисточников при поддержке военных специалистов, аналитиков и исследователей.⁵¹ Она даёт детальное и доступное представление о текущем конфликте, что ещё больше повысило уровень общественного понимания и помогло миру отреагировать на российское вторжение.

Социальные сети и информационное общество

Соцсети и распространение информации из открытых источников стали палкой о двух концах в русско-украинской войне, создавая существенные преимущества, но и потенциальные ловушки. Эти платформы позволяют быстро распространять важную информацию, но одновременно стирают грань между коллективной мудростью и дезинформацией, где голос общества может как помочь в оборонных усилиях, так и посеять хаос.⁵²

Стратегическая цифровизация Украины, начатая за несколько лет до войны, сыграла важную роль в использовании информации из открытых источников для отпора российскому вторжению. Этой инициативе предшествовало создание Министерства цифровой трансформации Украины⁵³ в августе 2019 года и запуск сервиса электронного управления «Дія»⁵⁴ в феврале 2020 года.⁵⁵ «Дія» поначалу служила платформой государственных

⁴⁹ Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 56.

⁵⁰ См. <https://www.understandingwar.org/interactive-map-russias-invasion-ukraine>.

⁵¹ Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 56. См. также Allison Puccioni, "How to Change the World from Space," *Futuring Peace*, UN DPPA, July 9, 2021, по состоянию на 14 мая 2023, <https://medium.com/futuring-peace/how-to-change-the-world-from-space-d4186e76da43>.

⁵² Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 63.

⁵³ Ministry of Digital Transformation of Ukraine, <https://thedigital.gov.ua> (по состоянию на 1 июня 2023).

⁵⁴ Приложение служит интерфейсом между украинским народом и правительством, насчитывая в настоящее время более 18 миллионов зарегистрированных пользователей. Эта инициатива электронного управления предлагает в общей сложности 99 услуг, доступных как через интернет-платформу, так и через мобильные приложения, и 26 услуг через мобильные приложения. Через этот сервис граждане могут запрашивать информацию об имуществе, транспортных средствах, бизнесе, продлевать лицензии, платить за парковку, сообщать о дефектах на дорогах и многое другое. International Telecommunication Union (ITU), "Interim Assessment on Damages to Telecommunication Infrastructure and Resilience of the ICT Ecosystem in Ukraine," 22.

⁵⁵ Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 38, 40.

услуг, но в марте 2022 года её быстро адаптировали для неотложных нужд войны. Обновленное приложение «Дія» позволило регистрировать и отслеживать перемещённых лиц,⁵⁶ загружать фото и видео военной техники противника и её перемещений, передавать данные геолокации и сообщать властям о подозрительных субъектах.⁵⁷ Этот инструмент фактически сделал каждого гражданина Украины, имеющего смартфон, потенциальным участником обороны страны.

Параллельно с этим мобильное приложение eVorog,⁵⁸ запущенное в марте 2022 года, ещё больше позволило гражданам Украины сообщать о действиях врага. Доступный через интерфейс «Дія», eVorog работает как защищённый чат-бот Telegram, позволяя пользователям конфиденциально сообщать информацию военному руководству, украинской разведке и контрразведке.⁵⁹ Такое цифровое сопротивление с широким участием населения стало важнейшим элементом оборонной стратегии Украины, обеспечив быстрый сбор и использование данных с оккупированных территорий.⁶⁰

Различные приложения и платформы соцсетей стали полем битвы для сбора информации из открытых источников, пропаганды, дезинформации и психологических операций. Все участники стремились формировать общественное мнение, распространять ложную информацию, манипулировать нарративами. Как российская, так и украинская стороны использовали цифровые и социальные медиа-инструменты в своих информационных (пропагандистских) операциях. Техническая и тактическая универсальность украинских военных очевидна в их способности фиксировать ключевые моменты и поддерживать интерес в виртуальном пространстве и соцсетях,

⁵⁶ International Telecommunication Union (ITU), "Interim Assessment on Damages to Telecommunication Infrastructure and Resilience," 23.

⁵⁷ McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine;" Den Prystai, "From Ukrainians to Ukrainians. 5 Digital Tools and Products Created to Help in Wartime," *Official Website of Ukraine*, October 5, 2022, по состоянию на 10 июня 2023, <https://war.ukraine.ua/articles/digital-tools-created-to-help-in-wartime/>.

⁵⁸ См. ссылку на бот eVorog [eEnemy]: https://t.me/evorog_bot (по состоянию на 5 июня 2023); StrategEast, "Ukrainian Digital Resistance to Russian Aggression" (Washington, D.C.: StrategEast Center for a New Economy, 2022), 9, www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf.

⁵⁹ В марте 2022 года пользователям дали возможность загружать фото и видео, делиться данными геолокации и сообщать о пережитом. Эту функцию расширили в апреле 2022 года, добавив сбор и обмен информацией о военных преступлениях, совершённых российскими военными. С августа пользователи также могут сообщать о местонахождении неразорвавшихся боеприпасов, мин, взрывчатых веществ и т.п. Prystai, "From Ukrainians to Ukrainians. 5 Digital Tools and Products Created to Help in Wartime."

⁶⁰ McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine;" Fridbertsson, "Technological Innovation for Future Warfare," 4.

даже когда линия фронта месяцами оставалась статичной зимой 2022 и весной 2023 года.⁶¹

Приложения и технологические решения на основе искусственного интеллекта общедоступны, что упрощает создание и распространение ложного или манипуляционного контента без глубоких технических знаний. Российская сторона успешно производила так называемые «дипфейковые» изображения и аудиозаписи, сея неопределённость путём фабрикации новостей об украинских событиях.⁶² Так, в фейковом видеообращении президента Владимира Зеленского от марта 2022 года украинских солдат призывали сложить оружие и прекратить боевые действия. Аналогичным образом, в сентябре 2022 года распространялись лживые сообщения с бывшим послом США в России (2012-2014) Майклом Макфолом, запрашивавшим данные о военных приготовлениях Украины.⁶³ Ещё одним примером стал разговор – вероятно, российского происхождения – между (якобы) мэром Киева Виталием Кличко и мэром Будапешта Гергеем Карачоном, призванный посеять неуверенность.⁶⁴

Беспилотные летательные аппараты и наземные роботизированные комплексы

С начала русско-украинской войны обе стороны широко применяют военные⁶⁵ и коммерческие беспилотные летательные аппараты (БПЛА) и си-

⁶¹ Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China," Konaev and Daniels, "Agile Ukraine, Lumbering Russia." Это показывает взаимосвязь разных областей техники, где малогабаритные коммерческие БПЛА, или дроны, стали инструментом военного пиара и пропаганды. Дроны дали невиданные ранее кадры военных действий, которые затем расходились в соцсетях – Telegram, YouTube, Twitter и т.д. Они успешно справлялись с нетрадиционными ситуациями, примером чего стали такие проекты, как «Хочу жить», когда русский солдат сдался в плен украинскому дрону в ноябре 2022 года, и «Спасти рядового Мавика», когда потерянный за российскими линиями дрон был найден и доставлен обратно на подконтрольную Украине территорию с помощью двух других дронов в январе 2023 года.

⁶² Michael C. Horowitz, Lauren Kahn, and Laura Resnick Samotin, "A Force for the Future: A High-Reward, Low-Risk Approach to AI Military Innovation," *Foreign Affairs* (May-June, 2022), 157-158, <https://www.foreignaffairs.com/articles/united-states/2022-04-19/force-future>.

⁶³ Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 61.

⁶⁴ Оригинал записи доступен на канале "Orosz Hírek": "Ál-Vitalij Klicskóval társalog Karácsony Gergely főpolgármester", 8 августа 2022, <https://www.youtube.com/watch?v=x1GhWEe9o2o> – на венгерском языке.

⁶⁵ В этой статье мы не рассматриваем наземные и воздушные аппараты, разработанные в военных целях. Не вдаваясь в подробности, их примерами являются турецкий Baykar Bayraktar TB2, используемый Украиной, Punisher, производимый UA Dynamics в Украине, Warmate польской WB Electronics, американский Switchblade и советский Ту-141 «Стриж» «Туполева». Кроме того, существуют такие

стемы.⁶⁶ Эти средства используют больше, чем когда-либо, особенно для разведки и наблюдения.⁶⁷ Такой всплеск их применения обусловлен не только экономической эффективностью, но и необходимостью компенсировать отсутствие или ограниченную применимость обычных военно-воздушных сил. Мнения о текущей роли и будущем значении беспилотных и дистанционно управляемых летательных аппаратов расходятся. Некоторые предполагают, что это революционные технологические инновации, другие утверждают, что они просто изменили наше восприятие современной войны. Истина, вероятно, лежит где-то между этими двумя точками зрения: украинский опыт поможет нам понять настоящее и даст перспективу на будущее.⁶⁸ Заметно лишь недостаточное использование наземных роботизированных комплексов. Россия имеет передовые автономные наземные системы на разных стадиях разработки, но либо не хочет, либо не может применять их.⁶⁹

Первоначально внимание привлёк военный беспилотник Bayraktar TB2, оснащённый ракетами класса «воздух-земля» с лазерным наведением. Однако его успех померк из-за работы российской ПВО и РЭБ, что отодвинуло Bayraktar на задний план, где он использовался скорее как дополнительное средство разведки.⁷⁰ Украина первой массово применила доступные коммерческие малые БПЛА (дроны).⁷¹ В отличие от довольно дорогих военных беспилотников, Украина в основном использовала коммерческие продукты

беспилотные системы российского производства, как «Куб» «Калашникова»/группы ZALA AERO, «Элерон-3СВ», разработанный ENICS, «Орлан-10» разработки российского СТЦ, израильский «Форпост Р», используемый Россией (на базе Searcher II израильской IAI), «Орион-Э» компании «Кронштадт» и др. Adam Lowther and Mahbube K. Siddiki, "Combat Drones in Ukraine," *Air and Space Operations Review* 1, no. 4 (Winter 2022): 3-13, www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-1_Number-4/Lowther.pdf.

⁶⁶ Konaev and Daniels, "Agile Ukraine, Lumbering Russia." Во избежание недоразумений из-за разных терминологических определений и классификации (например, в FAA и НАТО), в этой статье использован термин «дрон» из повседневной речи. «Дрон» здесь означает малогабаритный и менее сложный беспилотный летательный аппарат, обычно для гражданского и коммерческого применения.

⁶⁷ McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine;" Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China."

⁶⁸ Lowther and Siddiki, "Combat Drones in Ukraine," 3-4.

⁶⁹ Palavenis, "The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War," 2; Konaev and Daniels, "Agile Ukraine, Lumbering Russia." Россия применяла в Сирии ряд систем для разминирования, разведки туннелей и непосредственной огневой поддержки – «Скарабей», «Уран-6», «Уран-9», но все они имели серьёзные проблемы со связью, управлением и нацеливанием.

⁷⁰ Konaev and Daniels, "Agile Ukraine, Lumbering Russia;" Lowther and Siddiki, "Combat Drones in Ukraine," 5-6, 13.

⁷¹ Palavenis, "The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War," 3; Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China;" Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

с камерами высокого разрешения, управляемые со смартфона, прежде всего для разведки.⁷² Главными факторами этих массовых беспилотников стали вес, характеристики и стоимость закупки устройства.⁷³ В этой технико-экономической гонке победил недорогой китайский продукт, а именно дрон DJI Mavic 3.⁷⁴ Китайский поставщик официально не продавал свою продукцию в военных целях, но и не принял никаких мер для предотвращения её использования в конфликте.⁷⁵

Затем, когда зимой 2022 года и весной 2023 года возросло значение артиллерийских и ракетных ударов, обе стороны повысили точность своих ударов, используя небольшие дроны.⁷⁶ Эти дроны обеспечивали огневую поддержку в реальном масштабе времени и собирали данные о целях для новых ударов. Обещание украинских БПЛА собственной разработки не было полностью реализовано, но такие общественные группы, как украинская «Аеророзвідка», приобрели немалый опыт.⁷⁷ Этот опыт проявился на

⁷² McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine."

⁷³ Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 42-44; Mykhaylo Zabrotskyi et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022* (London: Royal United Services Institute for Defence and Security Studies (RUSI), 2022), 2-3, www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022.

⁷⁴ Общедоступную статистику даёт только Фейн Гринвуд, эксперт по БПЛА, который проанализировал типы дронов, используемых российскими и украинскими силами, на основе примерно 900 проверенных образцов по открытым источникам. В его анализе 463 случая, или 59 % – продукция китайской DJI, причём чаще всего использовались небольшие портативные дроны Mavic этого производителя. Остальные 41 % включали широкий спектр дронов различного происхождения. Более подробную информацию можно найти в инициативе Украины «Армия дронов», в рамках которой к июлю 2022 года было закуплено около 1400 коммерческих дронов за счёт пожертвований, собранных украинской платформой United24. Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China."

⁷⁵ Стоит отметить, что китайский поставщик DJI имеет возможность ограничивать использование своих коммерческих дронов в зонах военных действий с помощью системы так называемого «виртуального забора», как это было сделано в Ираке и Сирии в 2017 году. На практике это означает, что DJI может знать о военном применении своих устройств. Система AeroScope компании предназначена для обнаружения и предотвращения несанкционированного использования дронов. Однако, несмотря на эти возможности, DJI продолжает поставлять дроны в Россию и соседние с Украиной страны, что вызывает обеспокоенность в связи с их использованием в продолжающемся конфликте. Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China."

⁷⁶ Konaev and Daniels, "Agile Ukraine, Lumbering Russia," Zabrotskyi et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine*, 17.

⁷⁷ «Аеророзвідка» – общественная инициатива, поддерживающая военные усилия Украины сетевыми и технологическими средствами с 2014 года. Организация привлекла внимание СМИ своей ролью в операциях, включая постепенное уничтожение продвигавшихся к Киеву колонн российской техники и постоянные

поле боя, в виде разработки, модернизации и адаптации гражданских дронов.⁷⁸ Делались попытки дополнить разведывательные возможности этих дронов средствами боевой поддержки, но менее эффективно. Технология аддитивного производства оказалась полезной, позволив дорабатывать устройства на месте и добавлять крылья-стабилизаторы к ручным и бронебойным гранатам,⁷⁹ что позволило использовать последние в свободном падении.⁸⁰

С распространением различных БПЛА, особенно малых, обе стороны сосредоточились на обнаружении и нейтрализации техники противника. Чтобы нарушить инфраструктуру командования и управления, и Россия, и Украина широко использовали системы РЭБ для противодействия сетям связи, радиолокации и средствам обнаружения противника. Эффективность России проявилась в почти полном выводе из строя украинской связи на Донбассе после 2015 года и её способности препятствовать надлежащему использованию малых БПЛА. Однако это преимущество России, похоже, сошло на нет в 2022 году.⁸¹ Хотя российские средства РЭБ оказались менее эффективными, каждая сторона пыталась ограничить возможности другой при помощи контрмер.⁸² Ожидается, что в будущем массовые БПЛА будут небольшими, экономичными и легко модифицируемыми, поскольку противоборствующим сторонам придётся постоянно приспосабливаться к развитию технологий и сложностям радиоэлектронной борьбы.⁸³

удары по российским позициям. Подробнее см. <https://aerorozvidka.ngo> (по состоянию на 12 июня 2023).

⁷⁸ Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China."

⁷⁹ Например, при помощи аддитивного производства (3D-печати) в Украине модернизируют кумулятивные противотанковые гранаты РКГ-З, удаляя рукоять и добавляя пластиковые стабилизаторы к резьбовой части корпуса гранаты, что сделало их пригодными для поражения цели в свободном падении. Любопытно, что к апрелю 2022 года для продукции DJI был сделан напечатанный на 3D-принтере механизм сброса, который крепится к дронам, и его можно было заказать через китайскую службу доставки AliExpress. Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China."

⁸⁰ McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine;" Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China;" Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

⁸¹ Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

⁸² Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China;" Zabrodskiy et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine*, 2-3. С февраля по июль 2022 года было потеряно 90 % дронов, что сделало главными приоритетами экономическую эффективность и одноразовость. Согласно анализу, проведенному в ноябре 2022 года, украинский дрон в среднем мог выполнить три миссии, прежде чем его приземляли, либо нарушая связь между передатчиком и приемником, либо нейтрализуя оператора. Меры РЭБ необходимо было постоянно адаптировать к программным средам, обновляемым DJI, чьи дроны наиболее широко использовались на поле боя.

⁸³ При массовом применении небольших автономных дронов, таких, как SWARM (Smart Warfighting Array of Reconfigured Modules), контрмеры потребуют уси-

Искусственный интеллект

С распространением и развитием искусственного интеллекта (ИИ) мы становимся свидетелями технологической революции, серьёзно влияющей на ведение войны, что показал русско-украинский конфликт.⁸⁴ Обе стороны используют алгоритмы анализа и визуализации огромных объёмов информации. Эта технология позволяет отображать реальное поле боя в виртуальном пространстве, облегчает создание более убедительных ложных или поддельных изображений и аудиозаписей, а также помогает распространению дезинформации. Кроме того, ИИ помогает принимать решения, анализируя открытые данные из соцсетей.⁸⁵ На войне ИИ даёт существенные преимущества. Он может оповещать в режиме реального времени о действиях противника, автоматически обрабатывать и анализировать большой объём данных и выявлять важные закономерности. Поскольку людские ресурсы всё ограничней, автоматизированные системы, управляемые ИИ, будут играть важную роль в организации и обеспечении обороны и устойчивости.⁸⁶

В отличие от русских, украинские военные эффективно использовали ИИ для объединения информации от различных источников разведки, ускоряя процессы наблюдения, ориентации, принятия решений и действий. Хотя ИИ в первую очередь помогает людям принять решение, технологии развиваются. Ожидается, что даже в военное время системы ИИ в конечном счёте будут принимать некоторые решения автономно. Американские технологические компании с самого начала помогали украинцам в разведке и принятии решений. Алгоритмы машинного обучения автоматизировали перехват, считывание, перевод и анализ сообщений, передаваемых по незащищённым российским каналам.⁸⁷ Кроме того, украинская компания Primer адаптировала своё программное обеспечение для считывания и перевода речи на базе искусственного интеллекта для фильтрации и обработки важной в военном отношении части перехваченных сообщений.⁸⁸

ИИ и технологии двойного назначения нашли практическое применение на поле боя, в частности, благодаря сервису распознавания лиц Clearview AI, который привлёк внимание СМИ. При поддержке американской компании

ния возможностей РЭБ, а также оборонительных лазерных, микроволновых, артиллерийских и ракетных систем. См. Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 43, 49-52.

⁸⁴ ИИ имеет широкий спектр применения, о чём не раз говорится в этой статье.

⁸⁵ Horowitz, Kahn, and Samotin, "A Force for the Future: A High-Reward, Low-Risk Approach to AI Military Innovation," 157-158.

⁸⁶ Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics."

⁸⁷ Konaev and Daniels, "Agile Ukraine, Lumbering Russia;" Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics."

⁸⁸ McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine."

украинские власти идентифицировали погибших российских солдат по фотографиям в их профилях в соцсетях и уведомляли их семьи. С марта 2022 года, после добровольного предложения Clearview AI, сотрудничество компании с Украиной расширилось. Clearview AI активно помогала не только в идентификации погибших солдат, но и в противодействии дезинформации, обнаружении российских диверсантов, идентификации лиц на контрольно-пропускных пунктах, воссоединении семей и помощи в расследовании военных преступлений.⁸⁹

Компания Palantir Technologies Inc.,⁹⁰ которая уже более 20 лет сотрудничает с американской разведкой, тоже сыграла важную роль в обороне и восстановлении Украины с начала войны.⁹¹ Сервисы обработки и визуализации данных Palantir помогают картографировать поле боя в реальном масштабе времени.⁹² Компания собирает и анализирует информацию о перемещениях и позициях российских войск в своей системе ситуационной осведомлённости. Она также помогает оценивать и документировать повреждения инфраструктуры из-за конфликта, предлагая на основе этих данных эффективные решения по её восстановлению.⁹³

Выводы и заключение

Обмен информацией, внедрение новых технологий и обеспечение доступа к этим технологиям сыграли ключевую роль в защите цифровых систем и инфраструктуры Украины. Эти усилия позволили противостоять лживым российским нарративам и помогли ударах Украины по России. Хотя прорывные технологические решения, как в дополнение к обычному оружию,

⁸⁹ McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine." Основатель и руководитель ClearView AI Хоан Тон-Тат 1 марта 2022 года бесплатно предложил услуги компании правительству Украины. В начале войны база данных ClearView AI включала около двух миллионов фотографий пользователей российской социальной сети Вконтакте. С марта по июль 2022 года семь украинских ведомств и более 600 военнослужащих регулярно использовали эту платформу, выполнив более 60 000 поисковых запросов всего за четыре месяца. "War in Ukraine," *Clearview AI*, по состоянию на 20 мая 2023, www.clearview.ai/ukraine.

⁹⁰ Palantir Technologies Inc., <https://www.palantir.com>.

⁹¹ Руководитель Palantir Алекс Карп первым среди руководителей крупных технологических компаний встретился с президентом Украины. Palantir также открыл представительство в Украине для дальнейшей поддержки страны в ходе конфликта. Jeffrey Dastin, "Ukraine Is Using Palantir's Software for 'Targeting,' CEO Says," *Reuters*, February 2, 2023, www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/.

⁹² Например, программное обеспечение технологической компании может использовать изображения с коммерческих спутников и социальных сетей для создания цифровых карт подразделений противника. McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine."

⁹³ "Media Coverage," *Palantir*, по состоянию на 12 июня 2023, www.palantir.com/newsroom/media/.

так и вместо него, сами по себе не возымели немедленного или решающего эффекта, успехи Украины во многом были обусловлены применением инноваций и западных технологических продуктов. Краткосрочное технологическое превосходство не гарантировало стратегической победы, но сочетание новых технологий и обычных систем вооружения дало ценную информацию о будущем арсенале и методах вооружённого конфликта. Широкое использование информации из открытых источников, систем связи, БПЛА и ИИ при принятии решений сыграли определяющую роль в оборонной стратегии Украины.

На раннем этапе конфликта мы стали свидетелями одновременного появления обычных продуктов и технологий, часто двойного назначения, наряду с инновационными технологическими решениями. Возник парадокс: у руководителей частного сектора появились обязанности, которых они не желали, в то время как руководители правительств стремились получить возможности, которых у них не было.⁹⁴ Извлекая уроки из войны в Украине, важно определить долгосрочные приоритеты исследований и разработок. Оборонная промышленность должна решать новые проблемы, связанные с новыми технологиями, сотрудничая с коммерческим технологическим сектором, формируя общую инновационную сеть, желательно – при поддержке государства.⁹⁵ Приоритет экономически эффективных технологий, снижение административного давления и минимизация расходов сектора имеют решающее значение. Инвестиции в оборонную промышленность необходимы, но устойчивость и инновации не должны измеряться исключительно себестоимостью продукции.⁹⁶

Примечание

Мнения, выводы, заключения и рекомендации в данной публикации принадлежат авторам и могут не отражать официальную политику или пози-

⁹⁴ Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 61.

⁹⁵ См. также обзор военной промышленности Южной Кореи, где рассмотрен опыт и уроки из русско-украинской войны: Jaret C. Riddick and Cole McFaul, "Lessons from the Ukraine-Russia War," *Issues in Science and Technology* 39, no. 3 (Spring 2023), <https://issues.org/lessons-ukraine-russia-war-joeng-seo-heo/>; Josep Borrell, "Lessons from the War in Ukraine for the Future of EU Defence," *European Union External Action*, May 29, 2023, www.eeas.europa.eu/eeas/lessons-war-ukraine-future-eu-defence_en.

⁹⁶ Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics." Инновационное общество или армия характеризуются способностью легко интегрировать новые технологии. Будущая военная единица получит стратегическое преимущество, если она будет мобильной, сетевой и децентрализованной. Она будет успешно принимать решения в сети и эффективно применять современные инструменты искусственного интеллекта.

цию Консорциума «Партнёрство ради мира», организаций-участниц и любых правительственных или международных организаций, связанных с его руководящими структурами.

Благодарность

Проект № 2022-2.1.1-NL-2022-00012 реализован при поддержке Министерства культуры и инноваций Венгрии из Национального фонда исследований, разработок и инноваций, финансируемого в рамках схемы финансирования 2022-2.1.1-NL-2022-00012.

Об авторах

Д-р Имре Порколаб – руководитель Института исследования оборонных инноваций. *Электронная почта:* porkolab.imre@hm.gov.hu

Д-р Иштван Локотош – заместитель декана факультета автомобилестроения Audi Hungaria Университета Иштвана Сечени, руководитель отдела автомобильного и железнодорожного транспорта.
Электронная почта: lakatos@sze.hu

Д-р Ференц Давид – старший консультант и научный сотрудник Национальной лаборатории совместных технологий Института передачи технологий.
Электронная почта: david.ferenc@techtra.hu

Библиография

- "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022, <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>.
- "Interim Assessment on Damages to Telecommunication Infrastructure and Resilience of the ICT Ecosystem in Ukraine" (International Telecommunication Union, December 2022), https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructure%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22_FINAL.pdf.
- "KA-SAT Network Cyber Attack Overview," Viasat, March 30, 2022, <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview>.
- "Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine," Microsoft, April 27, 2022, <https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/>.
- "The Telecommunications Industry and Its Biggest Challenges for 2023," ISB Tech, January 23, 2023, <https://www.isbtech.pl/2023/01/branza-telekomunikacyjna-jej-najwieksze-wyzwania-na-2023-rok/>. – in Polish
- "Ukrainian Digital Resistance to Russian Aggression" (Washington, D.C.: StratEast Center for a New Economy, 2022), 9, https://www.strateast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf.
- "War in Ukraine," *Clearview AI*, accessed May 20, 2023, <https://www.clearview.ai/ukraine>.
- Albon, Courtney, "Intelligence Agencies Accelerate Use of Commercial Space Imagery to Support Ukraine," *Defense News Online*, April 6, 2022, www.defensenews.com/battlefield-tech/space/2022/04/06/intelligence-agencies-accelerate-use-of-commercial-space-imagery-to-support-ukraine/.
- Bandura, Romina, and Janina Staguhn, "Digital Will Drive Ukraine's Modernization," Center for Strategic & International Studies, January 10, 2023, www.csis.org/analysis/digital-will-drive-ukraines-modernization.
- Borowitz, Mariel, "War in Ukraine Highlights Importance of Private Satellite Companies," *Astronomy Online*, August 16, 2022, <https://www.astronomy.com/science/war-in-ukraine-highlights-importance-of-private-satellite-companies/>.
- Borrell, Josep, "Lessons from the War in Ukraine for the Future of EU Defence," European Union External Action, May 29, 2023, www.eeas.europa.eu/eeas/lessons-war-ukraine-future-eu-defence_en.
- Clark, Stephen, "SpaceX Rockets Past 4,000 Starlink Satellites in Orbit with Another Launch," *Spaceflight Now*, May 04, 2023, <https://spaceflightnow.com/2023/05/04/falcon-9-starlink-5-6-coverage/>.

- Dastin, Jeffrey, "Ukraine Is Using Palantir's Software for 'Targeting,' CEO Says," *Reuters*, February 2, 2023, <https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/>.
- Fridbertsson, Njall Trausti, "Technological Innovation for Future Warfare," NATO Science and Technology Committee, Sub-Committee on Technology Trends and Security, 5-8 (2023), <https://www.nato-pa.int/document/2022-future-warfare-report-fridbertsson-025-stctts>.
- Graham-Cumming, John, "Internet Traffic Patterns in Ukraine since February 21, 2022," The Cloudflare Blog, March 4, 2022, <https://blog.cloudflare.com/internet-traffic-patterns-in-ukraine-since-february-21-2022/>.
- Greenwood, Faine, "The Drone War in Ukraine Is Cheap, Deadly and Made in China," *Foreign Policy*, February 16, 2023, <https://foreignpolicy.com/2023/02/16/ukraine-russia-war-drone-warfare-china/>.
- Horowitz, Michael C., Lauren Kahn, and Laura Resnick Samotin, "A Force for the Future: A High-Reward, Low-Risk Approach to AI Military Innovation," *Foreign Affairs* (May-June, 2022), <https://www.foreignaffairs.com/articles/united-states/2022-04-19/force-future>.
- Jayanti, Amritha, "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?" Harvard Kennedy School, Belfer Center for Science and International Affairs, March 9, 2023, <https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose>.
- Konaev, Margarita, and Owen J. Daniels, "Agile Ukraine, Lumbering Russia: The Promise and Limits of Military Adoption," *Foreign Affairs*, March 28, 2023, <https://www.foreignaffairs.com/ukraine/russia-ukraine-war-lumbering-agile>.
- Lowther, Adam, and Mahbube K. Siddiki, "Combat Drones in Ukraine," *Air and Space Operations Review* 1, no. 4 (Winter 2022): 3-13, www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-1_Number-4/Lowther.pdf.
- Marquardt, Alex, "Exclusive: Musk's SpaceX Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick up the Tab," *CNN Politics*, October 14, 2022, <https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html>.
- McGee-Abe, Jason, "One Year on: 10 Technologies Used in the War in Ukraine," *TechInformed*, February 24, 2023, <https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/>.
- Palavenis, Donatas, "The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War," Air Land Sea Application Center, October 1, 2022, https://www.alsa.mil/Portals/9/Documents/articles/221001_ALSA_Article_Donatas_Palavenis.pdf.
- Perani, Giulio, "Military Technologies and Commercial Applications: Public Policies in NATO Countries," NATO Research Fellowship (Rome, 1997), 5-6, <https://www.nato.int/acad/fellow/95-97/perani.pdf>.

- Prince, Matthew, "Steps We've Taken around Cloudflare's Services in Ukraine, Belarus, and Russia," The Cloudflare Blog, March 7, 2022, <https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/>.
- Prystai, Den, "From Ukrainians to Ukrainians. 5 Digital Tools and Products Created to Help in Wartime," Official Website of Ukraine, October 5, 2022, <https://war.ukraine.ua/articles/digital-tools-created-to-help-in-wartime/>.
- Puccioni, Allison, "How to Change the World from Space," *Futuring Peace*, UN DPPA, July 9, 2021, <https://medium.com/futuring-peace/how-to-change-the-world-from-space-d4186e76da43>.
- Riddick, Jaret C., and Cole McFaul, "Lessons from the Ukraine-Russia War," *Jaret C. Issues in Science and Technology* 39, no. 3 (Spring 2023), <https://issues.org/lessons-ukraine-russia-war-joeng-seo-heo/>.
- Rosen, Kenneth R., "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, <https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486>.
- Sayler, Kelley M., "Emerging Military Technologies: Background and Issues for Congress," *Congressional Research Service Report R46458*, (February 2024), <https://sgp.fas.org/crs/natsec/R46458.pdf>.
- Schmidt, Eric, "Innovation Power: Why Technology Will Define the Future of Geopolitics," *Foreign Affairs* (March-April 2023): 40, <https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics>.
- Schneider, Jacquelyn, "Does Technology Win Wars? The U.S. Military Needs Low-Cost Innovation – Not Big-Ticket Boondoggles," *Foreign Affairs*, March 3, 2023, <https://www.foreignaffairs.com/ukraine/does-technology-win-wars>.
- Śliwa, Zdzisław, "The Synergy Between Technology and Soldiers in Warfare – The Russian Armed Forces Image During the War in Ukraine," *Wiedza Obronna* 281, no. 4. (2022): 53-69, <https://doi.org/10.34752/2022-d281>.
- Tian, Nan et al., "Trends in World Military Expenditure, 2022," SIPRI Fact Sheet, April 2023, 9-11, https://www.sipri.org/sites/default/files/2023-04/2304_fs_milex_2022.pdf.
- Woolbright, Jocelyn, "Nine Years of Project Galileo and How the Last Year Has Changed It," The Cloudflare Blog, June 5, 2023, <https://blog.cloudflare.com/nine-years-of-project-galileo-and-how-the-last-year-has-changed-it/>.
- Zabrodskiy, Mykhaylo, et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022* (London: Royal United Services Institute for Defence and Security Studies, 2022), <https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022>.

Zegart, Amy, "Open Secrets: Ukraine and the Next Intelligence Revolution," *Foreign Affairs* 102, no. 1 (January-February, 2023): 54-70, 56-57, <https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart>.