ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БОРЬБЕ С ТЕРРОРИЗМОМ В ИНТЕРНЕТЕ

Адылова Фатима Туйчиевна

Институт математики им. В. И. Романовского АН Республики Узбекистан, доктор технических наук,профессор, руководитель лаборатории

fatadilova@gmail.com

Аннотация: Целью данного аналитического обзора является оценка современного практического применения искусственного интеллекта (ИИ) для борьбы с терроризмом в Интернете, что считается наибольшей угрозой безопасности в Центральной Азии. Автор показывает актуальные направления и модели ИИ, успешность их применения в этой области в качестве инструмента, который может обрабатывать огромные объемы данных и обнаруживать в них скрытые закономерности. Обзор даёт чёткое доказательство того, что искусственный интеллект является эффективным инструментом для анализа и прогнозирования различных механизмов, особенностей террористических атак в мировой практике борьбы с терроризмом, в том числе и в регионе Центральной Азии.

Ключевые слова: *математическое моделирование, интерпретация, глубокое обучение, прогнозирование террористических событий, интернет, тактика борьбы с терроризмом*.

INTERNETDA TERRORIZMGA QARSHI KURASHDA SUN'IY INTELLEKTNI AMALIY QO'LLANILISHI

Adilova Fatima Tuychiyevna

O'zbekiston Respublikasi Fanlar Akademiyasi V. I. Romanovskiy nomidagi matematika instituti, texnika fanlari doktori, professor, laboratoriya mudiri

fatadilova@gmail.com

Annotatsiya: Ushbu tahliliy sharhdan ko'zlangan maqsad Markaziy Osiyo mintaqasida xavfsizlikka eng katta tahdid hisoblangan internetda terrorizmga qarshi kurashishda sun'iy intellektning amaliy qo'llanilishini baholashdan iborat. Muallif sun'iy intellektning hozirgi tendentsiyalari va modellarini, ularni katta hajmdagi ma'lumotlarni qayta ishlash va ulardagi yashirin qonunlarni kashf eta oladigan vosita sifatida ushbu sohada qo'llash muvaffaqiyatini ko'rsatadi. Sharhda sun'iy intellekt

terrorizmga qarshi kurashning jahon amaliyotida, jumladan, Markaziy Osiyo mintaqasida terrorchilik xurujlarining turli mexanizmlari, xususiyatlarini tahlil qilish va bashorat qilishning samarali vositasiga aylanishi haqida aniq dalillar keltirilgan.

Kalit so'zlar: *matematik modellashtirish, talqin qilish, chuqur o'rganish, terroristik hodisalarni bashorat qilish, internet, terrorizmga qarshi kurash taktikasi.*

PRACTICAL APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE FIGHT AGAINST TERRORISM ON THE INTERNET

Adilova Fatima

V. I. Romanovsky Institute of Mathematics of the Academy of Sciences of the Republic of Uzbekistan, Doctor of Technical Sciences, Professor, Head of the Laboratory

fatadilova@gmail.com

Abstract: The purpose of this analytical review is to evaluate the current practical application of artificial intelligence to combat terrorism on the Internet, which is considered the greatest threat to security in the Central Asian region. The author shows the modern trends and models and the success of their application in this field as a tool that can process huge amounts of data and detect hidden patterns in them. The review provides clear evidence that artificial intelligence is an effective tool for analyzing and predicting various mechanisms and features of terrorist attacks in the global practice of combating terrorism, including in the Central Asian region.

Keywords: *mathematical modeling, interpretation, deep learning, prediction of terrorist events, Internet, counterterrorism tactics*

Введение

В последние годы интеграция цифровых технологий в повседневную жизнь в Южной и Юго-Восточной Азии увеличилась необычайными темпами, причем использование социальных сетей преимущественно молодым населением регионов превышает среднемировой показатель. Есть данные, что потенциально уязвимая молодежь подвергается воздействию онлайн-контента, создаваемого террористическими и экстремистскими группами онлайн.

В 2020 году Европол и 17 государств-членов выявили и удалили 1906 URL-адресов, ссылающихся на террористический контент, на 180 платформах и веб-сайтах за один день. Facebook указал, что в течение двух лет он удалил более 26 миллионов фрагментов контента от таких групп, как ИГИЛ и «Аль-Каида». В течении 2020 года было выявлено более 27 миллионов угроз вредоносной и подозрительной активности в адресном пространстве "Uznet".

Интернет и социальные сети оказываются мощными инструментами в руках таких групп, позволяя им общаться, распространять свои послания, собирать средства, вербовать сторонников, вдохновлять и координировать атаки, а также нацеливаться на уязвимых лиц.

В Глобальной контртеррористической стратегии Организации Объединенных Наций (A/RES/60/288) государства-члены приняли решение сотрудничать с ООН, чтобы изучить пути координации усилий на международном и региональном уровнях для противодействия терроризму во всех его формах и проявлениях в Интернете, и не дать использовать Интернет в качестве инструмента противодействия распространению терроризма.

Искусственному интеллекту (ИИ) уделяется значительное внимание во всем мире как инструменту, который может обрабатывать огромные объемы данных и обнаруживать в них скрытые закономерности, что может повысить эффективность анализа сложной информации. Поскольку ИИ является технологией общего назначения, эти преимущества могут быть использованы и в области борьбы с терроризмом.

В связи с этим среди контртеррористических ведомств во всем мире растет интерес к изучению того, как можно раскрыть потенциал искусственного интеллекта в этой области.

Целью данного аналитического обзора является оценка текущего состояния применения ИИ для борьбы с терроризмом в Интернете.

Актуальные направления и модели ИИ

Представляет большой интерес отчет UNCCT и UNICRI [1], который служит введением в использование контртеррористическими агентствами искусственного интеллекта для борьбы с терроризмом онлайн в регионах Южной и Юго-Восточной Азии. В отчете дается широкая оценка различных вариантов использования искусственного интеллекта, демонстрируются возможности технологии, а также выявляются проблемы. Отчет знакомит с возможными вариантами использования технологий ИИ, которые теоретически могут быть развернуты в регионах, при этом выявляет ключевые проблемы, которые должны быть решены властями, чтобы обеспечить ответственное использование ИИ. Приведем несколько примеров из отчета [1].

INSIKT Intelligence использует различные модели машинного обучения для обнаружения потенциальных угроз в Интернете на контенте с открытым исходным кодом. Алгоритм SOMA (Stochastic Opponent Modeling Agents) смог выработать политические рекомендации, способствующие сокращению числа нападений. Алгоритм STONE (Shaping Terrorist Online Network Efficacy) дает прогнозы о том, кто добьется успеха на определенной должности в данной

террористической сети, если субъект будет насильственно удален в результате вмешательства сил безопасности; как сеть перестроится, если несколько участников будут удалены; и, наконец, как управлять сетью, чтобы свести к минимуму «ожидаемую летальность» сети.

Поскольку проблема религиозного экстремизма является актуальной для республик Центральной Азии, интерес представляет финансируемая Евросоюзом система RED-Alert (Real-time Early Detection and Alert System), которая является одним из инструментов выявления ранних стадий радикализации на основе контента социальных сетей при одновременном соблюдении высоких стандартов конфиденциальности и безопасности.

Проект Германии MOTRA (Monitoring System and Transfer Platform Radicalization) разрабатывает инструмент для мониторинга громких общественных событий, который позволит быстро выявить, классифицировать новые тенденции и служит основой прогноза таких явлений; ожидается, что проект будет запущен в 2023 году.

Эти примеры показывают, как прогностическая аналитика может функционировать в случаях, если имеется достаточно данных для информирования о контртеррористических операциях. Онлайн-данные, в частности данные социальных сетей, теоретически могут изменить правила игры для прогнозной аналитики, предлагая совершенно новое измерение общедоступных данных или данных с открытым исходным кодом о террористических организациях, их членах, а также действиях других субъектов, которые могут повлиять на их поведение.

В монографии [2] утверждается, что для разработки контртеррористической стратегии, эффективной в предотвращении терроризма, необходимо грамотное и эффективное прогнозирование. Террористические нападения направлены на то, чтобы подорвать общественную поддержку правительств [3]. Даже если последствия нападения успешно устраняются, желательно полностью предотвратить такое нападение. Следовательно, профилактика находится в центре внимания стратегий борьбы с терроризмом [4]. Есть два способа предотвратить террористические нападения. Первый из них- сдерживание посредством защиты инфраструктуры, применения мер безопасности и обещания наказания. Второй способ, - лишение возможности совершать нападения путем задержания террористов до того, как их планы осуществятся, а также противодействие вербовке и радикализации будущих террористов. Как эти способы реализуются с помощью ИИ?

Анализ данных с помощью ИИ посредством их визуализации имеет целью поддержку деятельности служб разведки и безопасности, в частности, алгоритмы ИИ определяют приоритет подозреваемых в терроризме [5,6] и регулярно оценивают риск для пассажиров, совершающих авиаперелеты [7]. Информация может быть

собрана и сохранена по умолчанию, чтобы быть проанализирована позднее с целью выявления закономерностей и связей, которые разоблачают террористические сети или подозрительную деятельность [8]. При этом используемое машинное обучение позволяет интерпретировать и анализировать скрытые закономерности в больших объемах данных [9], используя фильтрацию, анализ взаимосвязей между объектами или более сложные инструменты распознавания изображений или голоса [10].

Разведывательные агентства и службы безопасности – не единственные, кто признает прогностическую ценность данных и пытается ее реализовать. В этом также заинтересованы коммерческие субъекты, так как правительства требуют от поставщиков услуг связи активности по мониторингу и исключению террористической деятельности на их собственных платформах [11]. Некоторые технологические компании используют сочетание человеческого опыта и изощренных прогностических мер для мониторинга и пресечения террористической деятельности на своих платформах [12].

Очевидно, что в будущем такие технологические компании, опираясь на применение ИИ, смогут самостоятельно бороться с терроризмом, а не просто закрывать неприемлемые сайты или профили пользователей [13].

Благодаря разработкам в области искусственного интеллекта недавно стал реальным анализ рутинной деятельности для прогнозирования террористических событий или идентификации террористов путем выделения того, чем отличается деятельность конкретной подгруппы. Огромное количество цифровой информации, генерируемой в настоящее время среднестатистическим человеком, означает, что большая часть этой рутинной деятельности может быть понята только с помощью анализа. Источники включают метаданные связи и записи о подключениях к Интернету, данные о местоположении и активности в социальных сетях. Значительные усилия, особенно со стороны академических ученых, направлены на разработку моделей, которые предсказывают местоположение и время террористических атак [14]. Основные подходы включают «эффект афтершока», при котором вероятность другого события увеличивается после нападения, что позволяет делать точные модели прогнозирования террористических атак [15].

Сложные модели, основанные на информации из открытых источников, включают данные с открытым исходным кодом, генерируемые отдельными лицами, использующими социальные сети и приложения на своих мобильных телефонах. Примером такой модели является система распознавания событий EMBERS (Early Model-Based Event Recognition using Surrogates), которая использует результаты различных отдельных прогностических моделей для прогнозирования таких событий, как вспышки болезней и гражданские беспорядки. Проект представляет собой сотрудничество между академическими и деловыми кругами и финансируется программой индикаторов с открытым исходным кодом США, – IARPA (Intelligence

Advanced Research Projects Activity). Входные данные также включают RSS-каналы с новостных веб-сайтов и блогов, каналы Twitter, страницы событий на сайтах социальных сетей и даже приложения для бронирования ресторанов [16].

Дочерняя компания Alphabet Inc. Jigsaw (ранее Google Ideas) создает технологии для решения некоторых самых сложных проблем глобальной безопасности [17], например, путем пресечения радикализации и пропаганды в Интернете. Проект Jigsaw "Redirect Method" нацелен на пользователей сайтов обмена видео, которые могут быть восприимчивы к пропаганде со стороны террористических групп, таких как ИГИЛ, и перенаправляет их на видеоролики, поддерживающие правдоподобный контраргумент [18]. Эти практические примеры использования, прогнозирующего ИИ в борьбе с терроризмом в интернете, пока подтверждают его потенциал, поскольку сегодня нереалистично ожидать, что искусственный интеллект обеспечит немедленные решения сложных вопросов.

Предполагая, что тенденция цифровизации сохранится, а производительность ИИ улучшится, в будущем появится больше возможностей для получения точных, математически обоснованных прогнозов на основе ИИ, и их использование в борьбе с терроризмом возрастет. Приведем в доказательство последние интересные исследования по рассматриваемой проблеме. На основе количественного анализа деятельности глобальных террористических организаций с 1970 по 2017 год в [19] предложена система классификации террористических организаций, основанная на ансамблевом обучении и прогнозирования их активности. Автор изучил различные атрибуты и характеристики времени, мест разных террористических организаций в базе данных GTD (Global Terrorism Database). Вначале выполняется необходимая предварительная обработка данных, затем террористические организации делят по частоте нападений, и подробно дают характеристики и тенденции отобранных 32 организаций с более чем 500 террористическими актами. На рисунке 1 показаны названия, количество нападений и рейтинг этих 32 террористических организаций. Организацией с максимальным числом террористических нападений оказалось движение «Талибан», которое совершило в общей сложности 7478 террористических нападений, за ним следуют ИГИЛ и "Shining Path" (SL) с 5613 и 4555 террористическими актами, соответственно. Для прогнозирования участия террористических организаций в атаках были выбраны 36 признаков и построены пять классификаторов, которые оказались полезными для эффективного прогнозирования активности террористических организаций, ответственных за нападения, и могут быть расширены для прогнозирования всех террористических организаций [20].

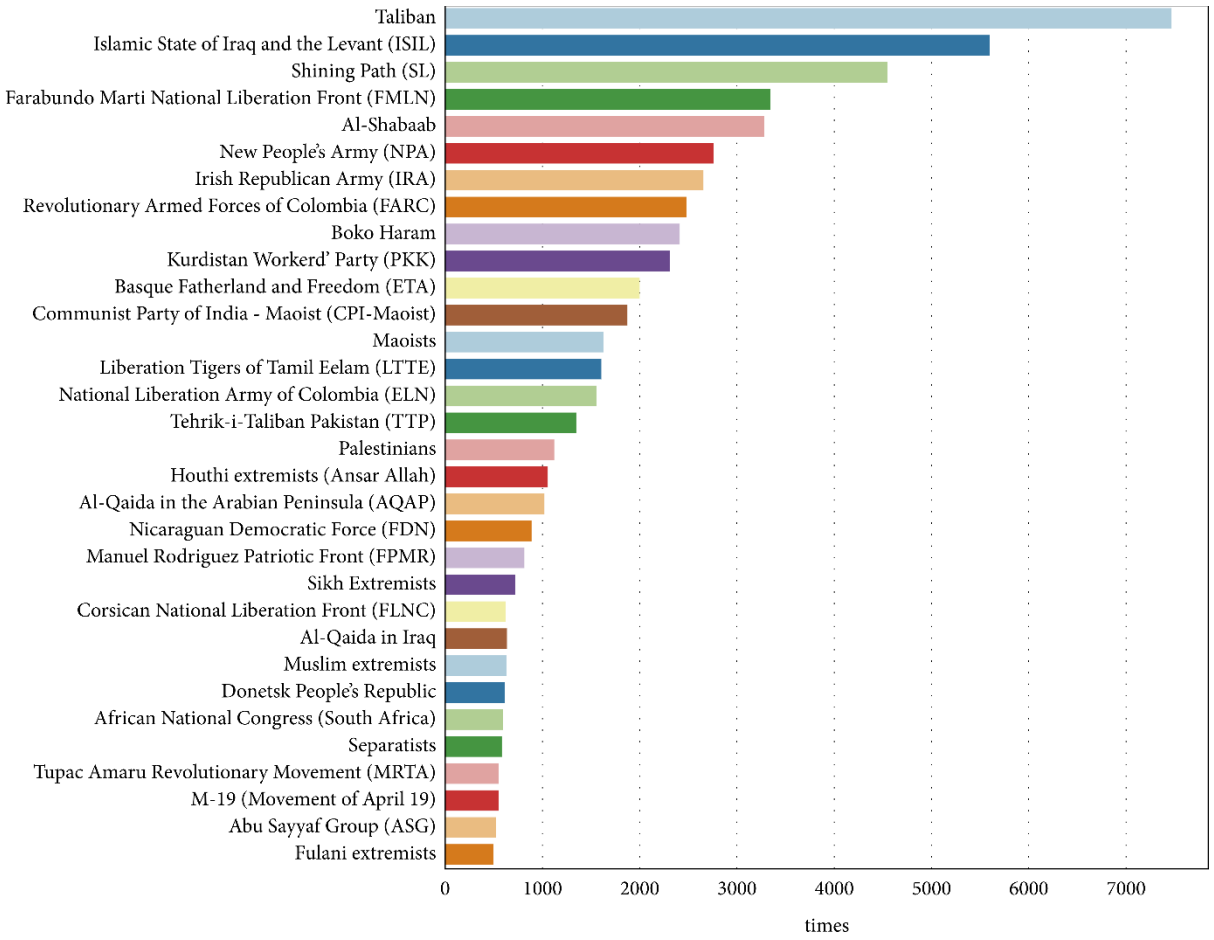

Рис. 1. Рейтинги террористических организаций с более чем 500 терактами

В исследовании [21] авторы предложили новый подход машинного обучения (ML), чтобы имитировать опасности террористического удара по всему миру с точки зрения ресурсов, длинных серий и информации, распространяемой по всему миру. Данные с 1970 по 2015 год были использованы для обучения и тестирования модели ML. Вероятность успеха этой модели в прогнозировании мест, где в 2015 году произойдут террористические атаки, оказалась более 96%. [22]. В [23] предложили ультрасовременный гибридный классификатор для прогнозирования террористических атак на основе больших данных, который оказался лучше, чем одиночный классификатор с точки зрения точности. В [24] авторы обратились к прогнозированию террористических групп, ответственных за теракты в Египте в период с 1970 по 2013 год. Для достижения поставленной цели авторы экспериментировали с пять различных моделей в проекте START. В работе [25] авторы предложили усовершенствованный алгоритм рекомендаций для построения трехмерной модели оценки риска террористической атаки, которая обеспечивают хорошую точность в обнаружении террористической деятельности при небольших и несложных наборах данных. Существующие наборы данных огромны и обладают сложными характеристиками, требует повышения точности методов.

Описанные выше модели прогнозирования в основе своей использовали алгоритмы машинного обучения, но сегодня наибольшее внимание привлекает глубокое обучение нейронных сетей (DL) и методы обработки естественного языка (Natural Language Processing, NLP).

В работе [26] предложена платформа глубокого обучения (DL) для изучения временных характеристик из GTD и прогнозирования характеристик будущей террористической деятельности с учетом множества факторов, - место (территория), тип используемого оружия, успешность или нет атаки, вид атаки и категория террориста. Исследовались 12 территорий, включая Центральную Азию.

В последнее время наибольший интерес ученых в области ИИ привлекает направление Natural Language Processing (NLP), в рамках которого разработаны популярные сервисы, например, ChatGPT. Совсем новая разработка,- чат-бот от Google,названный BARD выполнен на языковой модели LaMDA https://www.ixbt.com/tag/bard/. Поэтому в заключение статьи приведем разработку [27], в которой используется метод NLP для прогнозирования цели террористов. Применив методы обработки естественного языка (NLP) для извлечения особенностей из заявленного мотивационного повествования о террористических атаках, были определены категории целей исполнителя (Perpetrator Aim Categories, PACS). Удалось подтвердить эффективность классификации PAC, оценив прогностическую эффективность 11 различных моделей машинного обучения (ML). В таблице 1 показано распределение категорий целей террористических атак в различных регионах мира.

Таблица 1

Доля каждого PAC в разбивке по регионам мира

Регион	Презрение	Принуждение	Запугивание	Протест	Возмездие	Ослабление
Австралия и Океания	0.26%	0.06%	0.26%	0.19%	0.24%	0.14%
Центральная Америка и Карибский бассейн	0.00%	0.00%	0.00%	0.13%	0.03%	0.00%
Центральная Азия	**0.51%**	**0.37%**	**0.26%**	**0.58%**	**0.07%**	**0.85%**
Восточная Азия	0.39%	0.12%	0.13%	0.84%	0.37%	0.00%
Восточная Европа	3.56%	1.71%	11.40%	2.01%	1.73%	0.71%
Средний Восток и Северная Африка	28.02%	16.67%	40.08%	20.01%	30.51%	66.15%

Северная Америка	9.51%	4.52%	1.92%	8.23%	0.98%	0.71%
Южная Америка	2.31%	5.80%	2.82%	5.12%	2.81%	1.85%
Южная Азия	25.58%	43.65%	27.66%	34.26%	37.31%	16.22%
Юго-Восточная Азия	5.40%	8.73%	3.20%	10.75%	12.86%	4.55%
Африка к югу от Сахары	13.62%	14.29%	9.35%	7.25%	8.22%	6.83%
Западная Европа	10.54%	4.09%	2.94%	10.62%	4.87%	1.99%

Выявленное предпочтение заявленных мотивов террористических нападений указывает на разнообразный набор целей. В этом исследовании были применены два метода искусственного интеллекта (ИИ), которые помогли выделить цели преступников из полного списка террористических атак по всему миру. Удалось определить шесть основных категорий целей, которые заключались в презрении, протесте, возмездии, ослаблении, принуждении и запугивании. Впервые были применены методы обработки естественного языка (NLP) для создания эмпирического процесса классификации тем (Empirical Topic Classification, ETC), когда извлекались текстовые элементы из доступных мотивационных описаний террористических событий. Затем авторы применили 11 различных типов моделей ML к текстовым элементам, извлеченным из краткого описания каждого события, которое не было задействовано в обучении модели. Шесть наиболее эффективных моделей ML предсказывали PACs с точностью от 86% до 94% и соответствующими показателями AUC в диапазоне от 86% до 93%. Эти значения обеспечивают надёжный уровень достоверности результатов классификации по сравнению с результатами других оцениваемых моделей. Уровень доверия может служить основой принятия решений о распределении ресурсов для достижения цели, определенной из сообщений о террористических актах. Обычная стратегия в борьбе с терроризмом заключается в уменьшении стимулов, о которых необходимо знать заранее. Следовательно, заинтересованные стороны могут рассматривать PACs как стимулирующую структуру, помогающую определять и настраивать стратегии сдерживания.

Заключение

Таким образом, приведенный обзор о применении искусственного интеллекта в борьбе с терроризмом говорит о том, что ИИ станет отличным инструментом для анализа и прогнозирования правил и характера террористических атак. В [28] обобщили три способа улучшения прогнозирования конфликтов и призвали ООН инвестировать в проекты прогнозирования. Сегодня

разработано множество методов, включая новые методы машинного обучения, глубокого обучения и NLP, получено много информации о различных причинах конфликтов и их разрешении, а также построены теоретические модели, которые лучше отражают сложность социальных взаимодействий и принятия решений человеком.

С дальнейшим улучшением производительности и точности алгоритмов искусственного интеллекта эти технологии могут помочь находить лучшие модели и соответствующие наборы данных для повышения точности прогнозов, связанных с террористическими атаками. Однако, учитывая локальную редкость террористических атак и их универсальность в планировании и исполнении, даже при непрерывном прогрессе машинного обучения, исследования по крупномасштабным алгоритмам мониторинга и прогнозирования, тем не менее, как ожидается, будут сложными.

Список использованной литературы

1. Countering terrorism online with artificial intelligence An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia https://unicri.it/News/-Countering-Terrorism-Online-with-Artificial-Intelligence

2. Kathleen McKendrick International Security Department | August 2019 Artificial Intelligence Prediction and Counterterrorism https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf

3. Kurth Cronin, A. (2004), 'Sources of Contemporary Terrorism', in Kurth Cronin, A. and Lundes, J. (eds) (2004), *Attacking Terrorism: Elements of a Grand Strategy*, Washington, DC: Georgetown University Press, 2004, p.33.

4. Monaco, L (2017) 'Preventing the Next Attack; A Strategy for the War on Terrorism' *Foreign Affairs* 96(6), pp.23–29.

5. Van Puyvelde, D., Coulthart, S. and Hossain, M. S. (2017), 'Beyond the Buzzword: big data and national security decision-making', International Affairs, 93(26), pp. 1397–1416.

6. Anderson, D. (2017), Attacks in London and Manchester March–June 2017, independent assessment of M15 and police internal reviews, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/

7. Elias, B. (2014), Risk-Based Approaches to Airline Passenger Screening, Congressional Research Service Report, 31 March 2014, https://www.hsdl.org/?view&did=752251

8. Akhgar, B., Saathoff, G. B., Arabnia, H., Hill, R., Staniforth, A. and Bayerl, P. (2015), Application of Big Data for National Security, Oxford: Butterworth-Heinemann.

9. Van Puyvelde et al. (2017), 'Beyond the Buzzword: big data and national security decision-making', p. 1398.

10. Weaver, M. (2016), 'Search for UK jihadi in Isis video to use voice and vein recognition software', Guardian, 4 January 2016, https://www.theguardian.com/world/2016/jan/04/isis-video-uk-jihadi-voice-vein-recognition-software

11. Stewart, H. (2017), 'May calls on internet firms to remove extremist content within two hours', Guardian, 20 September 2017, https://www.theguardian.com/uk-news/2017/sep/19/theresa-may-will-tell-internet-firms-to-tackle-extremist-content

12. Titcomb, J. (2017), 'Internet giants insist they are tackling terrorism, but it is right to demand more', Telegraph, 17 October 2017; Chazan, G.(2018), 'Twitter suspends top AfD MP under new German hate speech law', Financial Times, 2 January 2018, https://www.ft.com/content/19f89fb2-efc7-11e7-b220-857e26d1aca4

13. Bickert, M. (2017), 'Hard Questions: How We Counter Terrorism', Facebook Newsroom, https://newsroom.fb.com/news/2017/06/how-we-counter-terrorism/

14. Murphi, M. (2018), 'Facebook pays terror victims to talk down extremists on Messenger', Telegraph, 27 February 2018, https://www.telegraph.co.uk/technology/2018/02/27/facebook-funds-terror-victims-talk-extremists-messenger/

15. Subrahmanian, V. S. (ed.) (2013), Handbook of Computational Approaches to Counterterrorism, New York: Springer.

16. Dickerson, J. P., Simari, G. I. and Subrahmanian, V. S. (2013), 'Using Temporal Probabilistic Rules to Learn Group Behaviour', in Subrahmanian, V. S. (ed.) (2013), Handbook of Computational Approaches to Counterterrorism, New York: Springer.

17. Ramakrishnan, N. et al. (2014), 'Beating the News' with EMBERS: Forecasting Civil Unrest using Open Source Indicators, New York:KDD, 14 August 2014, https://people.cs.vt.edu/naren/papers/kddindg1572-ramakrishnan.pdf

18. Jigsaw (2018), 'How can technology make people in the world safer?', https://jigsaw.google.com/vision/

19. Jigsaw (2016). 'The Redirect Method', https://www.redirectmethod.org

20. Xiaohui Pan Quantitative Analysis and Prediction of Global Terrorist Attacks Based on Machine Learning Scientific Programming Volume 2021, Article ID 7890923, 15 pages https://doi.org/10.1155/2021/7890923

21. J. Bergstra and Y. Bengio, "Random search for hyper-parameter optimization," Journal of Machine Learning Research, vol. 13, no. Feb, pp. 281–305, 2012.

22. Ding F, Ge Q, Jiang D, Fu J, Hao M. Understanding the dynamics of terrorism events with multiple-discipline datasets and machine learning approach. PloS One 2017;12(6):e0179057.

23. Gao Y, Wang X, Chen Q, Guo Y, Yang Q, Yang K, Fang T. Suspects prediction towards terrorist attacks based on machine learning. In: 2019 5th International Conference on Big Data and Information Analytics (BigDIA). IEEE; 2019. p. 126–31.

24. Meng Xi, Nie Lingyu, Song Jiapeng Big data-based prediction of terrorist attacks Computers& Electrical Engineering,volume 77,July 2019,p.120-127

25. Khorshid MM, Abou-El-Enien TH, Soliman GM. Hybrid classification algorithms for terrorism prediction in middle east and north africa. Int J Emerging Trends Technol Computer Sci 2015;4(3):23–9.

26. Zhang X, Jin M, Fu J, Hao M, Yu C, Xie X. On the risk assessment of terrorist attacks coupled with multi-source factors. ISPRS Int J Geo-Inform 2018;7 (9):354.

27. Firas Saidi, Zouheir Trabelsi A hybrid deep learning-based framework for future terrorist activities modeling and prediction Egyptian Informatics Journal 23 (2022) 437–446

28. Bridgelall, Raj. 2022. An Application of Natural Language Processing to Classify What Terrorists Say They Want. Social Sciences 11: 23. https://doi.org/10.3390/socsci11010023

29. W. Guo, K. Gleditsch, and A. Wilson, "Retool AI to forecast and limit wars" Nature, vol. 562, no. 7727, pp. 331–333, 2018.