I. Введение

Статья DGAP "Why major Powers launch destructive cyber operations and what to do about it" является частью более широкого исследования DGAP в области технологий и их влияния на международные отношения, включая аспекты кибербезопасности «умных городов» и риски, связанные с технологической зависимостью.

В этом анализе будут рассмотрены предполагаемые мотивы, стоящие за инициированием кибер-активностей крупными державами, последствия таких действий и стратегические ответные меры, которые могут быть сформулированы для решения этой растущей проблемы.

Основное внимание публикации уделяется анализу прошлых кибер-операций и их последствий для лучшего понимания и прогнозирования будущих кампаний, а также предложению стратегий борьбы с такими угрозами.

Цель этого анализа – предоставить ценную информацию специалистам по кибербезопасности и стратегическому планированию (но не ограничиваясь ими)

A. Критическая составляющая статьи

Как выше было отмечено, публикация является частью более широкого исследования DGAP в области технологий и их влияния на международные отношения, включая аспекты кибербезопасности «умных городов» и риски, связанные с технологической зависимостью. Это также вписывается в контекст глобальных вызовов безопасности, таких как кибер-война и распространение оружия массового уничтожения, и необходимости стратегического реагирования на эти угрозы.

В статье даётся исчерпывающий обзор положительных и отрицательных аспектов кибербезопасности. В качестве положительных аспектов выделяются достижения в области технологий безопасности, такие как передовые методы шифрования, биометрическая аутентификация и обнаружение угроз на базе искусственного интеллекта. Повышение осведомлённости общественности о проблемах кибербезопасности также рассматривается как позитивное событие. В качестве отрицательных аспектов отмечаются сохранение угроз, недостаточная осведомлённость о киберпространстве и причастность преступных организаций.

Из недостатков статьи стоит отметить недостаточную глубину обсуждения негативных аспектов кибербезопасности. Хотя упоминается о сохраняющихся угрозах и причастности преступных организаций, коллективный автор не вникает в специфику этих вопросов и не приводит конкретных примеров и особенно нет глубокой проработки потенциальных решений этих проблем.

Говоря про опыт при подготовке материала, который, как правило, имеет решающее значение, подразумевается, что опыт работы в области кибербезопасности позволяет обладать глубоким пониманием сложностей данной области, что позволит ему провести глубокий анализ и высказать обоснованные мнения. Недостаток этого опыта, очевидно, наблюдается и наличие опыта придало бы статье достоверности, сделав её надёжным источником информации для читателей.

В целом, что касается положительных и отрицательных сторон статьи, то она даёт некий сбалансированный взгляд на кибербезопасность, подчёркивая как её достижения, так и текущие проблемы. Этот взгляд полезен для читателей, стремящихся понять текущее состояние кибербезопасности. Тем не менее отмеченные недостатки определённо снижают качество статьи.

II. ОСНОВНЫЕ ВЫВОДЫ

В разделе представлено несколько ключевых моментов, второстепенных тезисов и выводов.

A. Ключевые и второстепенные моменты:

Основными мотивами для начала деструктивных кибер-операций являются территориальные завоевания, предотвращение угроз и ответные действия.

Первой известной кибер-операцией, уничтожившей физические объекты, была Stuxnet, американо-израильская операция в 2010 году, в ходе которой был осуществлён саботаж иранских центрифуг по обогащению урана.

Размер выборки деструктивных кибер-операций, нацеленных на государства за пределами крупного конфликта, довольно ограничен. Исторически было выбрано пять операций.

Все рассмотренные кибератаки проводились с учётом фактора, что атакующие страны, США и другие чувствовали себя в безопасности и не боялись какой-либо серьёзной реакции на совершаемые действия.

B. Основные выводы:

Иран, Северная Корея, Южная Корея, и Тайвань были основными целями деструктивных кибер-операций.

Для США будущие цели, вероятно, будут ограничены странами, которые стремятся приобрести ядерное оружие, такими как Иран и Северная Корея, а также расширения своего экономического влияния в Южно-Азиатском регионе.

Учитывая продолжающиеся пограничные споры, развязанные США ряд стран, в частности, Китай вероятно, будут нацелены на соседние страны с помощью деструктивных кибератак.

C. Основные рекомендации:

В публикации подчёркивается необходимость сравнительного анализа того, почему некоторые страны

проводят деструктивные кибер-атаки, и даются рекомендации относительно того, что Германия и другие государства-члены Европейского Союза могут сделать для их смягчения.

Публикация определяет деструктивные кибер-операции как те, которые приводят к значительному физическому ущербу или значительным экономическим потерям.

В публикации также отмечается, что некоторые операции были исключены из анализа из-за неопределённых утверждений и фактов.

III. Краткая история деструктивных кибератак

В разделе представлен обзор значительных кибератак, имевших место в прошлом, с акцентом на их мотивации, воздействии и общих чертах.

Первой обсуждаемой крупной кибератакой является американо-иранский конфликт 2010–2019 годов. Ярким примером является операция Stuxnet в 2010 году, целью которой вероятно были объекты по обогащению урана в Иране. В 2019 году США отключили иранские базы данных, использовавшиеся для атак на нефтяные танкеры в Персидском заливе.

Американо-северокорейский конфликт 2014–2017 годов – ещё одна важная кампания. Однако анализ исключает некоторые операции из-за неопределённых утверждений о причастности, таких как Китай, вызвавший перебои в подаче электроэнергии в Индии в 2021 году и закрытие порта в Японии в 2023 году, и США, вызвавшие взрывы газопровода.

Общим для этих кампаний является стремление снизить атакующие возможности противника. Например, США развернули разрушительные кампании против Северной Кореи и Ирана, чтобы задержать их приобретение и развёртывание наступательных вооружений

IV. Общие черты прошлых и будущих кибератак

Деструктивные кибератаки часто преследуют общие цели, такие как снижение возможностей противника, нанесение значительного физического ущерба и даже травматизм человека.

Изощрённость и опыт злоумышленников, неизбирательный размах атак и целенаправленное враждебное намерение максимизировать ущерб являются общими характеристиками этих кампаний

Использование искусственного интеллекта и расширенной системы анализа угроз улучшило обнаружение этих атак

Растущая кибер-угроза может в итоге заставить пересмотреть значение оружия массового уничтожения.

Глобальные пути распространения интернета означают, что кибер-активность стирает большую часть давней

Следующая крупная деструктивная кибератака может быть вызвана различными мотивами, включая геополитическую напряжённость, финансовую выгоду или желание нанести значительный физический ущерб или травмы людям

Идентификация кибератак может быть сложной из-за способности участников скрывать свою личность, выдавать себя за другие компьютеры, использовать виртуальные частные сети для усложнения наблюдения или захватывать другие устройства для проведения операций

Кибератаки затронули 120 стран, чему способствовал шпионаж, спонсируемый правительством.

Международное сообщество ещё официально не разработало конвенцию, классифицирующую кибервойны, но оно предприняло шаги для определения этого

V. Что делать

В разделе "Что делать" обсуждаются стратегии и рекомендации по смягчению последствий деструктивных кибер-операций.

В публикации предлагается, чтобы страны сосредоточились на наращивании своего потенциала в области кибербезопасности и сборе разведданных, особенно в отношении угроз финансовой системе.

В нем также подчёркивается важность международного сотрудничества в борьбе с кибер-угрозами, учитывая глобальный взаимозависимый характер системы.

В документе подчёркивается необходимость уменьшения фрагментации среди заинтересованных сторон и инициатив, которая в настоящее время препятствует международному сотрудничеству и ослабляет возможности восстановления системы и реагирования.

В публикации упоминается, что странам необходимо разработать более эффективные пути и средства противодействия информационным операциям с использованием киберпространства.

В нем также обсуждается идея создания новых инструментов для достижения целей, которые ставят перед собой разные страны в отношении того, как они действуют в киберпространстве.

В документе предлагается, чтобы крупные державы рассмотрели вопрос о том, как использовать кибер-операции для усиления сдерживания вооружённого нападения.

A. Основные рекомендации:

Международное сотрудничество имеет решающее значение в борьбе с кибер-угрозами, учитывая глобально взаимозависимый характер системы.

Необходимо уменьшить фрагментацию среди заинтересованных сторон и инициатив, которая в настоящее время препятствует международному сотрудничеству и ослабляет возможности восстановления системы и реагирования.

Существует необходимость в создании новых инструментов для достижения целей, которые различные страны ставят перед собой в отношении того, как они действуют в киберпространстве.