Секция «Социология безопасности»

Современные методы информационной войны

Научный руководитель – Гребенюк Александр Александрович

Полянцева Елизавета Дмитриевна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа современных социальных наук (факультет), Кафедра социологии и менеджмента общественных процессов, Москва, Россия
E-mail: liza.polyantseva25@gmail.com

В современных военных, социальных, политических и геополитических конфликтах информационные угрозы выступают как новая форма давления и социально-политического воздействия на государство, организацию или индивида.

Воздействием на информационные системы оппонента с целью достижения информационного превосходства называют информационную войну. Важно отметить, что информационная война - это в первую очередь средство стратегической атаки или противодействия, а не конечная цель.

Исследователи Манойло А. В., Петренко А. И. и Фролов Д. Б. интерпретируют понятие информационной войны как соперничество социальных систем по поводу влияния в информационно-психологической сфере на те сферы социальных взаимодействий и захвата контроля над источниками стратегических ресурсов, по итогу которого одни участники получают преимущества над другими [3]. Лауреат Нобелевской премии Альберт Гор определяет информационную войну как «атака на разум», автор указывает на роль информационного воздействия на принятие или лоббирование политических решений, а также выявляет особенности поведенческой реакции индивидов на дезинформацию [1].

Основные формы информационной войны в настоящее время следующие: использование средств электронной разведки, обучение и введение хакеров и специалистов кибернетики, аналитиков социальных сетей.

Комбинированный характер и возможность использования неограниченного количества информационных ресурсов составляют специфику ведения информационной войны.

Области, обеспечивающие жизнедеятельность государства, наиболее часто находятся под влиянием информационной войны, в частности это сферы экономики, образования, СМИ, науки, охраны природы, государственного управления. Распространёнными примерами являются воздействие на электростанции, телекоммуникации, транспортные сети, банковские системы [2]. Также к средствам информационной войны относятся: шпионаж (хищение/искажение/уничтожение особо важной информации, взлом и использование паролей, рассекречивание конфиденциального плана, электронное вмешательство в управление информационными системами и объектами.

Современными методами ведения информационной войны являются:

- создание искусственных финансовых кризисов для установления экономического контроля;

- скрытие особо важных информационных данных при лоббировании

интересов, а также при принятии решений;

- создание информационного шума для ограничения доступа к качественной информации;

- развитие клипового мышления у подверженной влиянию информационных атак аудитории для внедрения ложных смыслов;

- смещение понятий для замены общепринятых смыслов на необходимые для атакующей стороны;

- отвлечение внимания от реально значимых новостей;

- использование приоритета негативной информации над позитивной для снижения уровня достоверности новостных сообщений в СМИ;

- отсылка на несуществующие основания или источники для увеличения рейтинга либо охвата для работы с сознанием неуверенных индивидов;

- распространение заведомо ложной информации.

Таким образом, информационная война - это инструмент, который можно использовать как дополнение к обычной войне, а также как самостоятельную геополитическую стратегию, направленную на установление контроля над информационными системами противника.

Источники и литература

1) 1. Гор А. Атака на разум. (Перевод Богданов А.) – СПб. Амфора. 2018. – 478 с.
2) 2. Крутских А., Федоров А. О международной информационной безопасности. / А. Крутских, А. Федоров - М.: Слово, 2019. – С.118.
3) 3. Манойло, А. В. Государственная информационная политика в условиях информационно-психологической войны / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. – 3-е изд., стер. – Москва Горячая линия – Телеком, 2012. – 542 с.: ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=253556 (дата обращения: 18.02.2023). – Библиогр. в кн. – ISBN 978-5-9912-0253-4. – Текст: электронный.