Секция «Политические науки»

Особенности киберпространства как нового пространства международной политики в области безопасности.

Курилкин Антон Владимирович
Студент
Московский государственный университет имени М.В. Ломоносова, Факультет политологии, Москва, Россия
E-mail: tommy.ligrant@yandex.ru

Развитие компьютерной техники и новых технологий в сфере коммуникаций позволяет говорить о формировании новой сферы жизнедеятельности человека, а именно о киберпространстве как совокупности всех компьютерных сетей, созданных человеком либо для общения, хранения и получения информации (самым ярким примером является сеть Интернет а также многочисленные закрытые сети различных государственных и негосударственных организаций во многих странах мира), так и созданных для решения специфических технических задач (например, компьютерная сеть атомных электростанций или же сети энергетических компаний в США).

Необходимость обеспечения безопасности в различных сетях из теоретической проблемы превратилась в практическую в 1988 году, а именно с момента появления «червя Морриса» - первого в истории человечества компьютерного вируса, который за довольно короткий промежуток времени вывел из строя почти шесть тысяч узлов сети APRANET – предшественницы Интернета.

Стоит также сказать, что сам термин «киберпространство» появился изначально в художественной литературе Уильямом Гиббсоном. Однако, термин был быстро подхвачен в научной среде и на сегодня существует понимание киберпространства как совокупности всех сетей мира, а также всего, что их объединяет и контролирует (именно так трактует киберпространство Ричард Кларк, бывший советник Белого дома по безопасности и эксперт в области кибербезопасности).

До недавнего времени проблема безопасности в киберпространстве носила скорее технический характер, но начиная с XXI века, к киберпространству начинает возрастать интерес со стороны военных разных стран мира, что показывает появление во многих странах так называемых «кибервойск» и создания руководящих документов по ведению операций в киберпространстве. Пионерами в данной области являются США, которым удалось первыми создать кибервойска и разработать руководящие документы. Однако, на сегодняшний день подобные войска созданы в Китае, России, Евросоюзе и, по некоторым источникам, в Северной Корее. Повышенный интерес и стремление создать подобные рода войск связано с теми возможностями, которые предоставляет киберпространство – начиная от ведения пропаганды и проведения информационно-психологических операций до шпионажа и вполне ощущаемых физически диверсий.

Для начала необходимо выделить особенности киберпространства как новой сферы. Данные особенности особенно четко сформулированы в руководящем документе ВВС США AFDD3-12 “Cyberspace operations”:

1) Отсутствие физического пространства и вследствие этого высокая скорость действий

2) Так как киберпространство является полностью рукотворным, то необходимо выделять силы на поддержку инфраструктуры.

3) По характеру ведения боевых действий киберпространство близко к воздушному пространству – нет необходимости контролировать всю атмосферу, необходимо владеть лишь ключевыми точками и инфраструктурой

Однако, данный список не является полным – к нему необходимо добавить как минимум один весьма важный пункт, а именно – относительную анонимность действий в киберпространстве и возможности государств действовать не напрямую, а через негосударственных акторов. Также является весьма высоким процент и действий независимых негосударственных акторов в киберпространстве. К тому же, из предыдущих особенностей можно вывести и следующее отличие, которое прежде всего касается сети Интернет – относительная экстерриториальность киберпространства в физическом пространстве.

Исходя из особенностей киберпространства можно выделить и те угрозы, которые исходят из него:

Первой большой группой являются угрозы информационно-психологического характера. К данной области относится ведение пропаганды и проведение информационно-психологических операций в Интернете. Особенностью данного вида угроз является то, что практически все они исходят из сети Интернет. Однако, в данном случае Интернет как часть киберпространства является всего лишь инструментом для проведения информационно-психологических операций.

Второй большой группой являются угрозы информационно-технического характера, а именно проблемы кибершпионажа.

Третьей группой угроз являются угрозы инфраструктурно-технического характера – то есть данная группа угроз имеет непосредственно отношение к технической стороне компьютерных сетей. Сюда относятся такие виды угроз как: выведение оборудования из строя путем закладки «логических бомб», использование вредоносных программ для вывода оборудования из строя, изменение сетевых данных и многое другое.

Литература

1. Кларк Р., Нейк Р. Третья мировая война: какой она будет? - СПб.: Питер 2011
2. Най, С. Джозеф (младший) Будущее власти - Москва.: АСТ, 2014.
3. Libicki MC Conquest in cyberspace. National security and information warfare. — Cambridge, 2007
4. Arquilla J., Ronfeldt D. Cyberwar is coming!/ In Athena's camp. Preparing for conflict in the information age. Ed. By J. Arquilla, D. Ronfeldt. — Santa Monica, 1997