Эссе «Будущие вызовы России».

Автор: Дарья Басова, МГИМО(У) МИД России

Современный мир проходит стремительные трансформации, вызванные качественными сдвигами в технологической и информационной сферах, что обусловливает в свою очередь появление новых вызовов, против которых конвенциональные методы борьбы оказываются нерелевантными и даже бессмысленными. С началом нового тысячелетия мир вступил в фазу информационного общества, в котором стратегическим ресурсом и одновременно инструментом борьбы является информация. Иными словами, принципы и логика «реалполитик» сместилась с географического в киберпространство, где сами понятия времени и пространства сжимаются в миллионы раз. Наблюдается ужесточение межгосударственного соперничества на принципиально новой технологической основе, с внедрением ИКТ в государственную и общественную инфраструктуры. Следовательно, угрозы информационной безопасности, киберпреступность и шире – потенциальная милитаризация космоса, будут определять характер международных отношений в обозримом будущем. В этой связи, для России важно не упустить тот момент, когда отрыв отдельных государств (прежде всего, речь идет о США) по информационным технологиям достигнет такого уровня, который позволит им претендовать на информационно-космическое доминирование.

В чем непосредственно заключается *новизна* обозначенных выше угроз и их негативные последствия? Они обусловливаются следующими соображениями:

1) Сфера ИКТ концентрирует вокруг себя все остальные сферы, в которых существуют свои конвенциональные угрозы. Информационная безопасность связывает государственный аппарат, бизнес-сообщества и простых граждан, что влечет за собой повышенную уязвимость как государственного суверенитета в целом, так и коммерческой и персональной тайны в частности. Иными словами, разрушение ключевой банковско-финансовой структуры государства посредством атаки хакеров может парализовать всю государственную систему и сделать режим полностью управляемым. На этом фоне «цветные революции» кажутся лишь «занятием для новичков»;
2) ИКТ будут определять будущее военных технологий, что автоматически означает высокоточность и опережающее действие военной техники и оборудования. Наиболее негативным последствием большего проникновения ИКТ в военную сферу станет возможность отдельных стран – лидеров в информационном

пространстве обезоружить противника благодаря проникновению в его информационные сети и их последующей дезорганизации. Кроме того, угрозы, исходящие из киберпространства, практически не поддаются прогнозированию, что многократно повышает риски безопасности;

3) ИКТ позволяют не только контролировать информационный контент, но и формировать его. В этой связи, государства оказываются практически незащищенными от вбрасывания необходимой противнику информации, которая направлена на структурирование определенных общественных настроений. Подобное апробирование можно было наблюдать в случае с событиями «Арабской весны», а также деятельностью WikiLeaks.
4) Наконец, информационное пространство остается во многом нерегулируемым, что обеспечивает непредсказуемость и повышенную конфликтность. Нормы международного права не применимы в игре между различными акторами мировой политики на киберполе. Следовательно, это провоцирует ожесточенную конкуренцию между государевыми за наращивание ИКТ-потенциала, а значит, - и за глобальное информационное доминирование.

На сегодняшний момент Россия обладает необходимыми информационными разработками и ресурсами в космическом пространстве для того, чтобы выдерживать конкуренцию со стороны других государств в информационном пространстве и космосе. Однако наблюдаются тревожные тенденции, связанные со снижением ИКТ-расходов федеральных ведомств (по данным CNews Analytics, 2015) и снижением инвестирования в космическую деятельность. Игнорирование киберугроз и отказ от попыток обеспечить регулируемость Интернет-пространства на уровне международного сообщества может грозить России подрывом суверенитета в будущем, которое, как известно, создается сегодня.