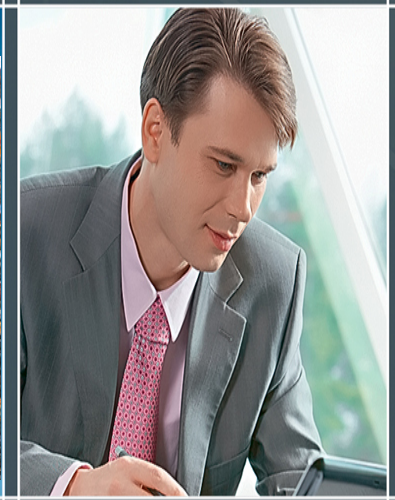
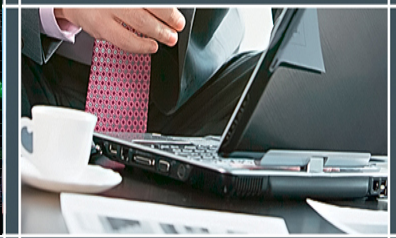
ВОПРОСЫ ОБЕСПЕЧЕНИЯ КОЛЛЕКТИВНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЮЗНОГО ГОСУДАРСТВА

Российский технологический университет - МИРЭА
(Институт кибербезопасности и цифровых технологий)



Григорьев В.Р. (РТУ - ИКБ)
Зав. кафедрой «Информационное противоборство», зам. директора ИКБ
к.т.н., доцент, член-корр. РАЕН



6 января 1995 года было подписано соглашение о Таможенном союзе,
21 февраля 1995 года — Договор о дружбе, добрососедстве и сотрудничестве сроком на 10 лет.
Направление в сторону интеграции началось после 1995 г.

Во второй половине 1990-х гг. были подписаны межгосударственные документы:

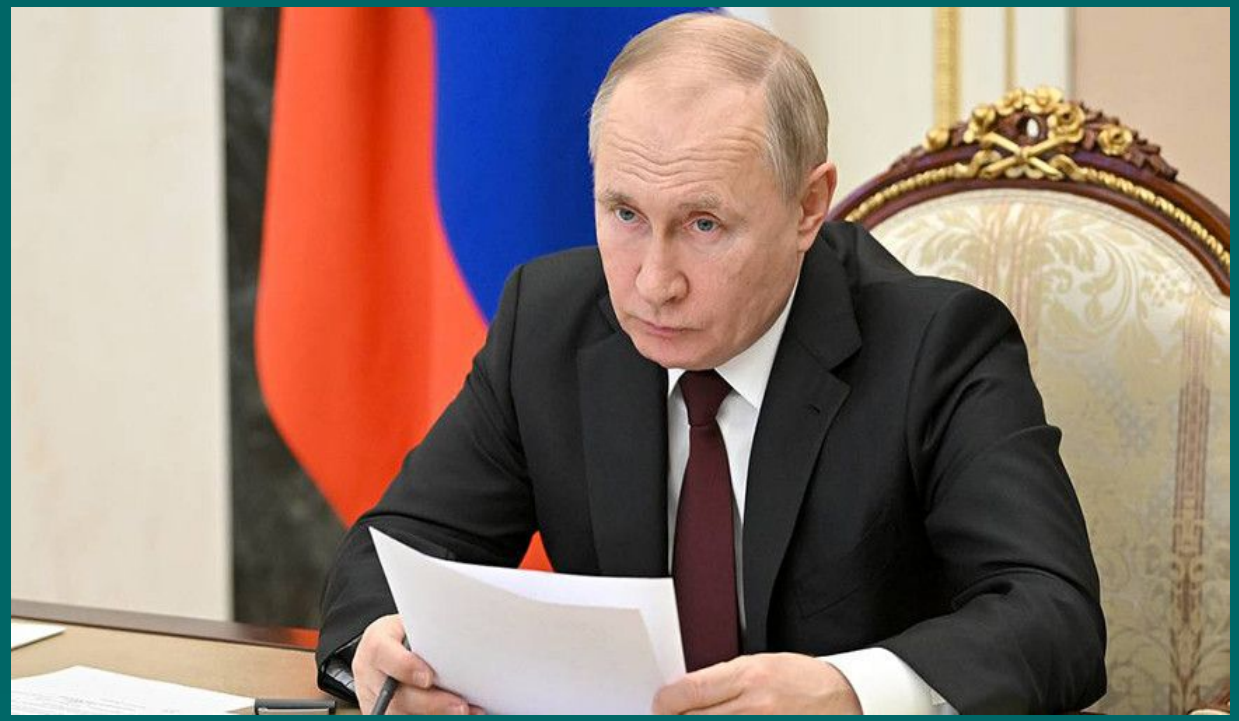
1996 год — «Договор о создании сообщества Беларуси и России»;
1997 год — «Договор о Союзе Беларуси и России»;
1998 год — «Договор о создании Союзного государства».

В Москве 16 мая состоялся юбилейный саммит Организации Договора о коллективной безопасности (ОДКБ), посвященный 30-летию подписания Договора о коллективной безопасности и 20-летию создания ОДКБ.

Среди первоочередных шагов, направленных на укрепление ОДКБ в нынешней беспрецедентной ситуации глава Республики Беларусь указал на повышение эффективности противодействия вызовам и угрозам в информационном пространстве, включая борьбу с фейками и дезинформацией.

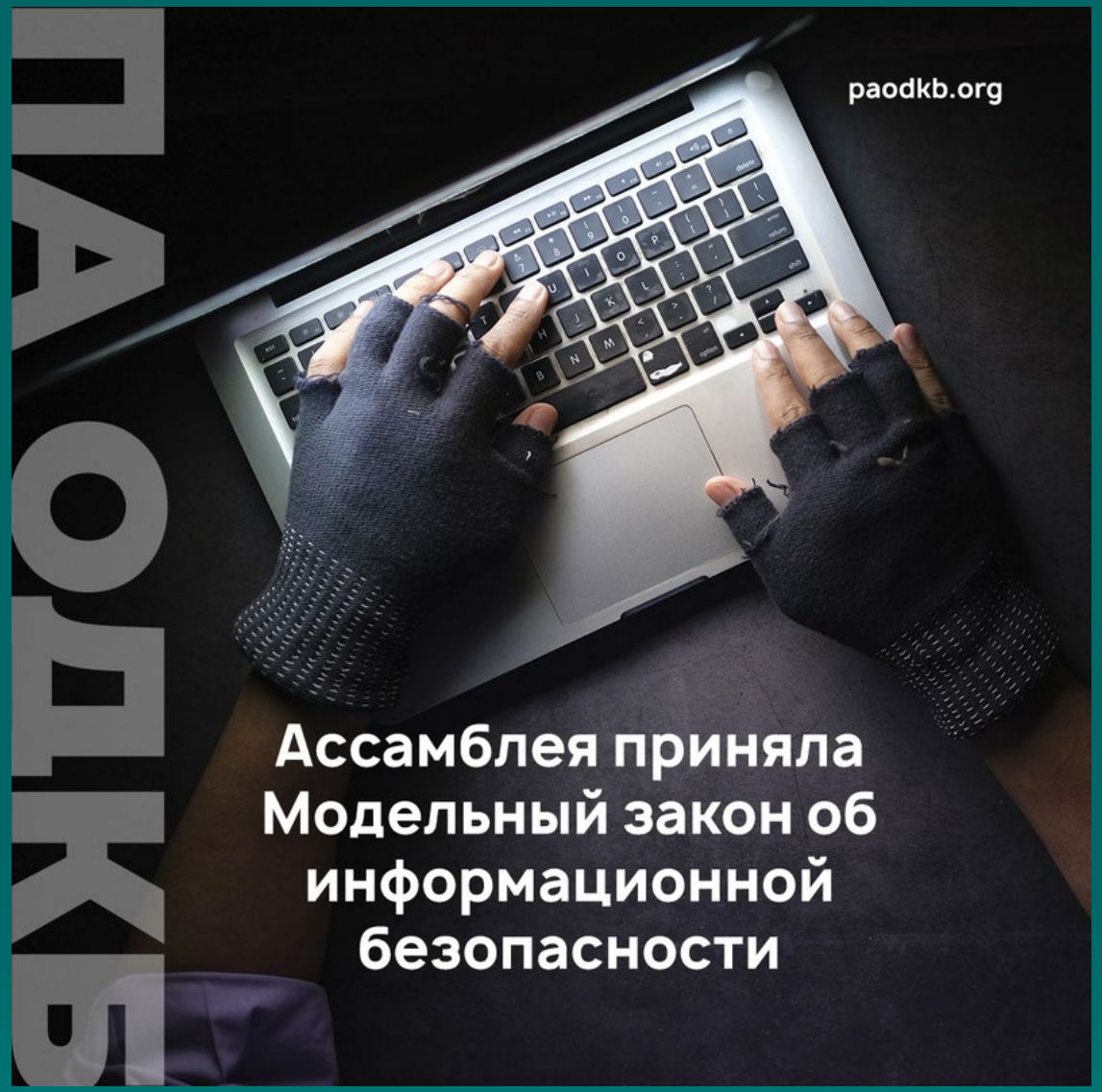
Он отметил: **«Понятно, что против нас развернута сейчас гибридная война с составляющей частью, в которой основной является информационная война. Для того чтобы этому противостоять, следует по максимуму использовать потенциал соглашения ОДКБ 2017 года о сотрудничестве в области информационной безопасности, активнее продвигать ОДКБ в социальных сетях, которые интенсивно используют наши западные оппоненты, с целью действенного реагирования на фейки и информационные вбросы. Притом надо подумать серьезно и, может быть, пойти по пути Китая в информационной борьбе, особенно в Интернете. Соответствующие задачи должны быть поставлены всем - внешнеполитическим ведомствам, спецслужбам и Секретариату ОДКБ».**

В пятницу 20 мая с.г. на заседании Совета безопасности Президент России Владимир Путин заявил, что против РФ в киберпространстве развязали войну. На РФ наносятся чётко скоординированные кибератаки. Число кибератак на Россию выросло в разы.



"Вызовы в этой сфере стали еще более острыми и серьёзными, более масштабными", - отметил российский лидер. - Атаки наносятся из разных государств, при этом они четко скоординированы. По сути, это действия государственных структур", - отметил Путин, напомнив, что в состав ряде армий некоторых стран официально входят кибервойска. В то же время, считает Президент РФ, **киберагрессия против страны, как и в целом "санкционный наскок", провалились.**

"В целом мы были готовы к этой атаке, и это результат той системной работы, которая велась все последние годы", - подчеркнул Путин.



Модельный закон ОДКБ "Об информационной безопасности" принят на пленарном заседании ПА ОДКБ **29 ноября 2021.**

Целесообразность его разработки была обусловлена многими причинами, в их числе, как непосредственно расширением спектра угроз информбезопасности, включая изменения их характера и интенсивности; так и попытками иностранных государств получать конфиденциальную информацию о состоянии обеспечения национальной информбезопасности.

Причем с каждым днем новые угрозы в информационном пространстве, кибератаки, требуют всё более оперативного реагирования путем совместных действий стран ОДКБ в рамках единых правовых механизмов.

Законом определено содержание деятельности по обеспечению информбезопасности, которое включает в себя выявление и оценку угроз, разработку и внедрение современных технологий с защитой информации, составление единого списка лиц и организаций, которые осуществляют кибератаки, чтобы установить эффективные механизмы и правила противодействия кибератакам.

Модельный закон позволяет, учитывая, в том числе, трансграничное информпространство, своевременно вскрывать и парировать гибридные угрозы, инспирированные как западными спецслужбами, так и транснациональными корпорациями, а также разрабатывать совместные планы по отражению информатак, внедрять технологию защищенного обмена информацией между союзниками, предусматривать совместные шаги по борьбе с развертыванием и финансированием, в том числе, так называемых "цветных революций»

Сегодня в эпоху глобализации, ослабления государственных границ, развития средств коммуникации важнейшим фактором стало изменение форм разрешения межгосударственных противоречий. В современных конфликтах все чаще акцент используемых методов борьбы смещается в сторону комплексного применения политических, экономических, информационных и других невоенных мер, реализуемых с опорой на военную силу. Это так называемые гибридные методы.

Их содержание заключается в достижении политических целей с минимальным вооруженным воздействием на противника. Преимущественно за счет подрыва его военного и экономического потенциала, информационно-психологического давления, активной поддержки внутренней оппозиции, партизанских и диверсионных методов. В качестве главного средства используются «цветные революции», которые, по мнению инициирующих их сторон, должны привести к ненасильственной смене власти в стане оппонента. По сути любая «цветная революция» – это государственный переворот, организованный извне. А в основе лежат информационные технологии, предусматривающие манипуляцию протестным потенциалом населения в сочетании с другими невоенными средствами.

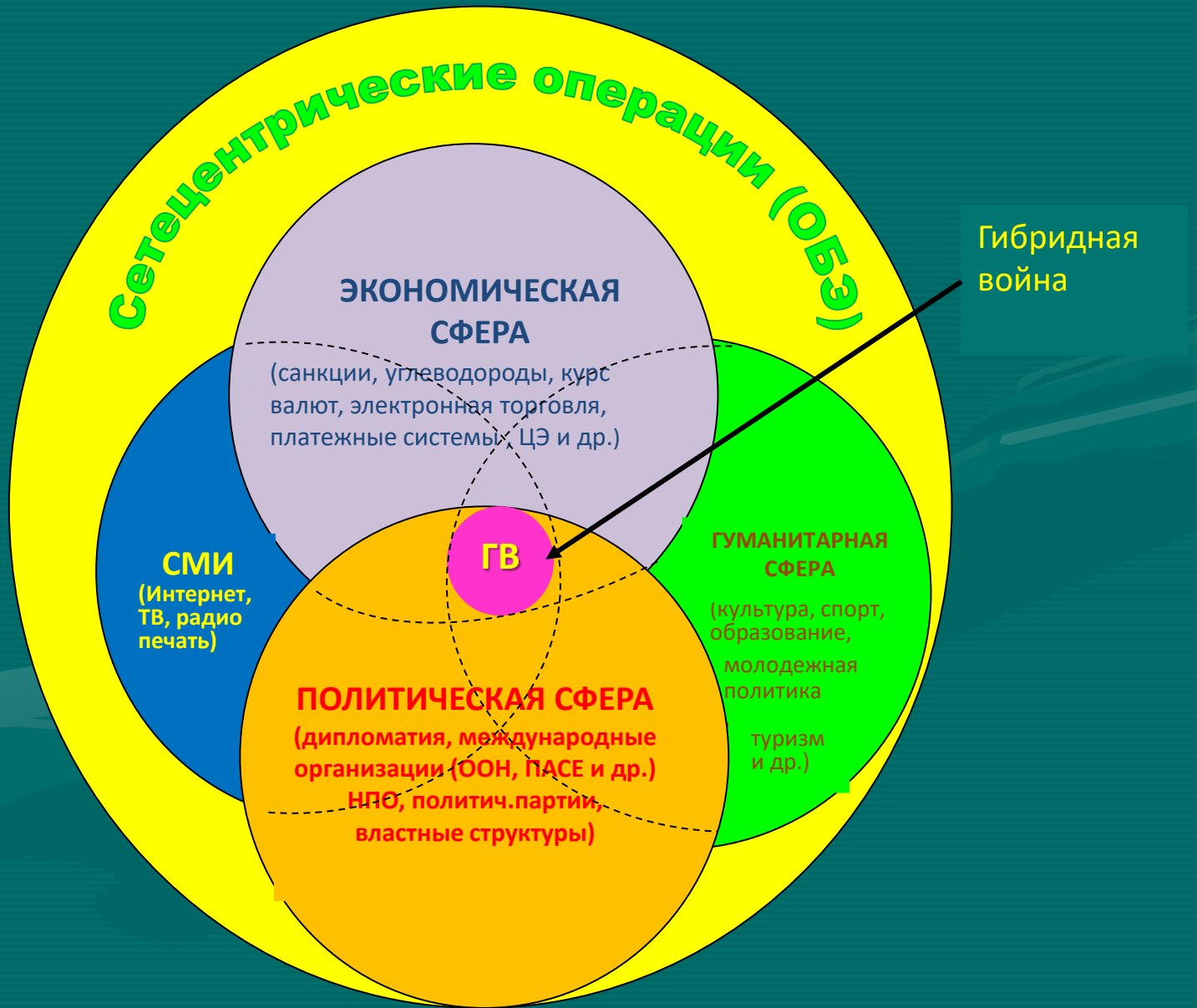
Важное значение при этом приобретает массированное, целенаправленное воздействие на сознание граждан государств – объектов агрессии посредством глобальной сети Интернет. Информационные ресурсы стали одним из самых эффективных видов оружия. Широкое их использование позволяет в считаные дни раскачать ситуацию в стране изнутри.

Начальник Генерального штаба Вооруженных С ил РФ , генерал армии Валерий Герасимов

Попытки дестабилизации государственного строя в государствах-членах ОДКБ

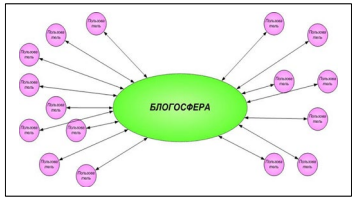
- 2020 г. - Беларусь
  - Армения
- 2022 г. - Казахстан
  - Россия (?)  Союзное государство (?)

Сетецентрический формат гибридной войны



Информационная безопасность в СТС

Социальные ресурсы Интернет

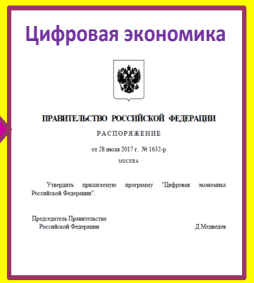


Почему важен мониторинг этих сетей?

Кибербезопасность
(информационная безопасность ИТС)

Информационная безопасность социотехнических систем (ИБ СТС)

Цифровая экономика



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

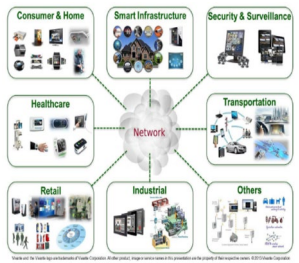
от 28 июля 2017 г. № 1632-р

МОСКВА

Утвердить прилагаемую программу "Цифровая экономика Российской Федерации".

Председатель Правительства Российской Федерации Д.Медведев

Направления развития Интернета вещей



Cyber-Physical Systems

Кибер-физическая безопасность

Информационное противоборство в СТС

Новая-старая стратегия США в отношении России

Новая стратегия сдерживания/изматывания России посредством методичного перенапряжения её экономических и общественных сил изложена в трёх докладах RAND Corporation, появившихся в последнее время:

«Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue. Different Challenges, Different Responses» («Россия агрессивна, но не игрок высшей лиги, Китай – игрок высшей лиги, но не агрессивен. Разные ответы»);

«Overextending and Unbalancing Russia. Assessing the Impact of Cost-Imposing Options» («Слишком большая и несбалансированная Россия. Оценка влияния затратных вариантов»);

«Extending Russia. Competing from Advantageous Ground» («Истощая Россию. Противоборство на лучших условиях»).

Новая-старая стратегия США в отношении России

Extending Russia

Competing from Advantageous Ground

James Dobbins, Raphael S. Cohen, Nathan Chandler, Bryan Frederick, Edward Geist, Paul DeLuca, Forrest E. Morgan, Howard J. Shatz, Brent Williams

RAND

BRIEF

Overextending and Unbalancing Russia

ASSESSING THE IMPACT OF COST-IMPOSING OPTIONS

October 2018

Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

JAMES DOBBINS, HOWARD J. SHATZ, ALI WYNE

Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue

Different Challenges, Different Responses

The Trump administration's National Security Strategy identifies "three main sets of challengers—the revisionist powers of China and Russia, the rogue states of Iran and North Korea, and transnational threat organizations, particularly jihadist terrorist groups," all of which "are actively competing against the United States and our allies and partners."[1] It goes on to characterize the threat from the two revisionist powers in identical terms: "China and Russia want to shape a world antithetical to U.S. values and interests."[2] Both states

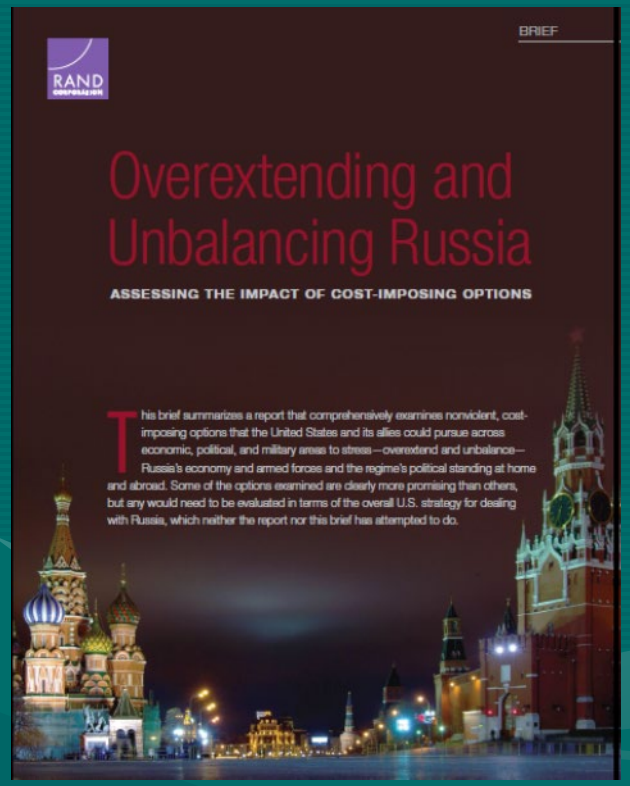
> challenge American power, influence, and interests, attempting to erode American security and prosperity. They are determined to make economies less free and less fair, to grow their militaries, and to control information and to repress their societies and expand their influence.[3]

RAND

«Extending Russia. Competing from Advantageous Ground» («Истощение России через расширение ее вовлеченности: противоборство на лучших условиях»)

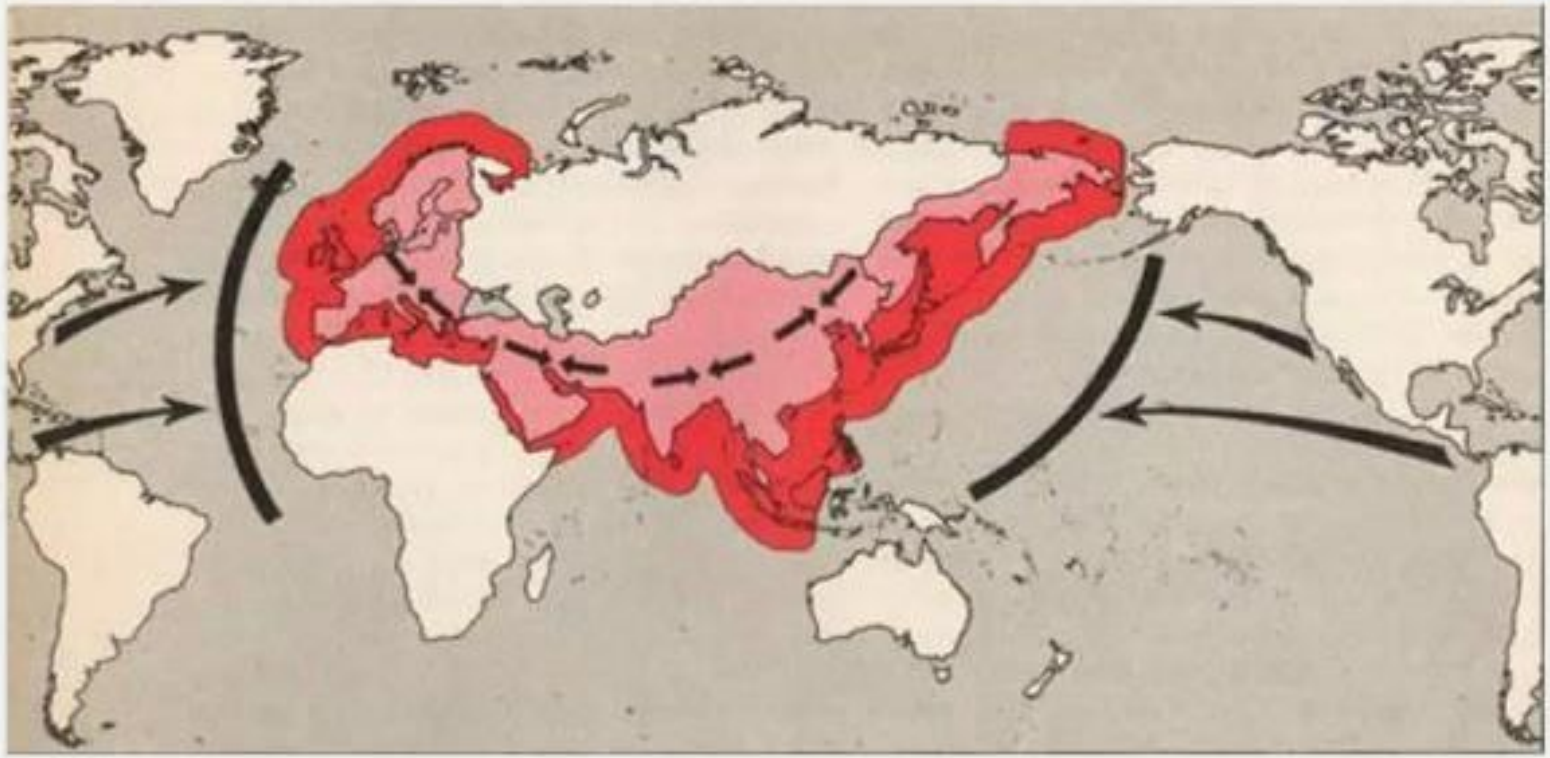
В рамках стратегии «истощения» России ключевое внимание будет уделяться процессам на постсоветском пространстве. Если обратить внимание на предлагаемые американскими аналитиками шаги, то в подавляющем большинстве они касаются создания «точек давления» на Россию на постсоветском пространстве (исключение составляют Сирия и в целом Средний Восток, но важно отметить, что в данном случае отмечается высокая рисковость такого подхода). Ключевыми направлениями давления на Россию выступают силовое давление из Прибалтики, разрушение Союзного государства России и Беларуси, **дальнейшая дестабилизация на Украине** (хотя это направление считается высокорисковым), а также разрушение партнерских отношений, складывающихся вокруг Каспийского моря, включая расшатывание ситуации в Карабахе.

Overextending and Unbalancing Russia. Assessing the Impact of Cost-Imposing Options («Слишком большая и несбалансированная Россия. Оценка влияния затратных вариантов»).



Геополитический блок представлен шестью сценариями, которые охватывают не только РФ, но и соседние страны.

- По мнению авторов, предоставление помощи Украине через поставки оружия помогло бы использовать наибольшую уязвимость России. При этом увеличение поставок вооружений и советников должно быть «откалибровано», чтобы увеличить расходы Москвы без провоцирования широкого конфликта с Киевом, в котором РФ имела бы значительные преимущества. Данная опция стоит на первом месте. И от нее эксперты RAND ожидают наибольшие выгоды для США.
- Второй сценарий — увеличение поддержки сирийским боевикам. Эксперты также отмечают, что это может поставить под угрозу борьбу с радикальным исламским терроризмом и привести к дальнейшей дестабилизации всего региона.
- Третий — содействию либерализации в Беларуси. По сути, речь идет о «цветной» революции. Авторы отмечают, что это может спровоцировать сильный ответ России, но выгоды также могут быть значительными.
- Расширение связей на Южном Кавказе, экономически конкурирующем с Россией, — следующий, четвертый сценарий.
- Пятый — уменьшение российского влияния в Центральной Азии.
- Шестой — организация переворота в Приднестровье и изгнание российских войск.



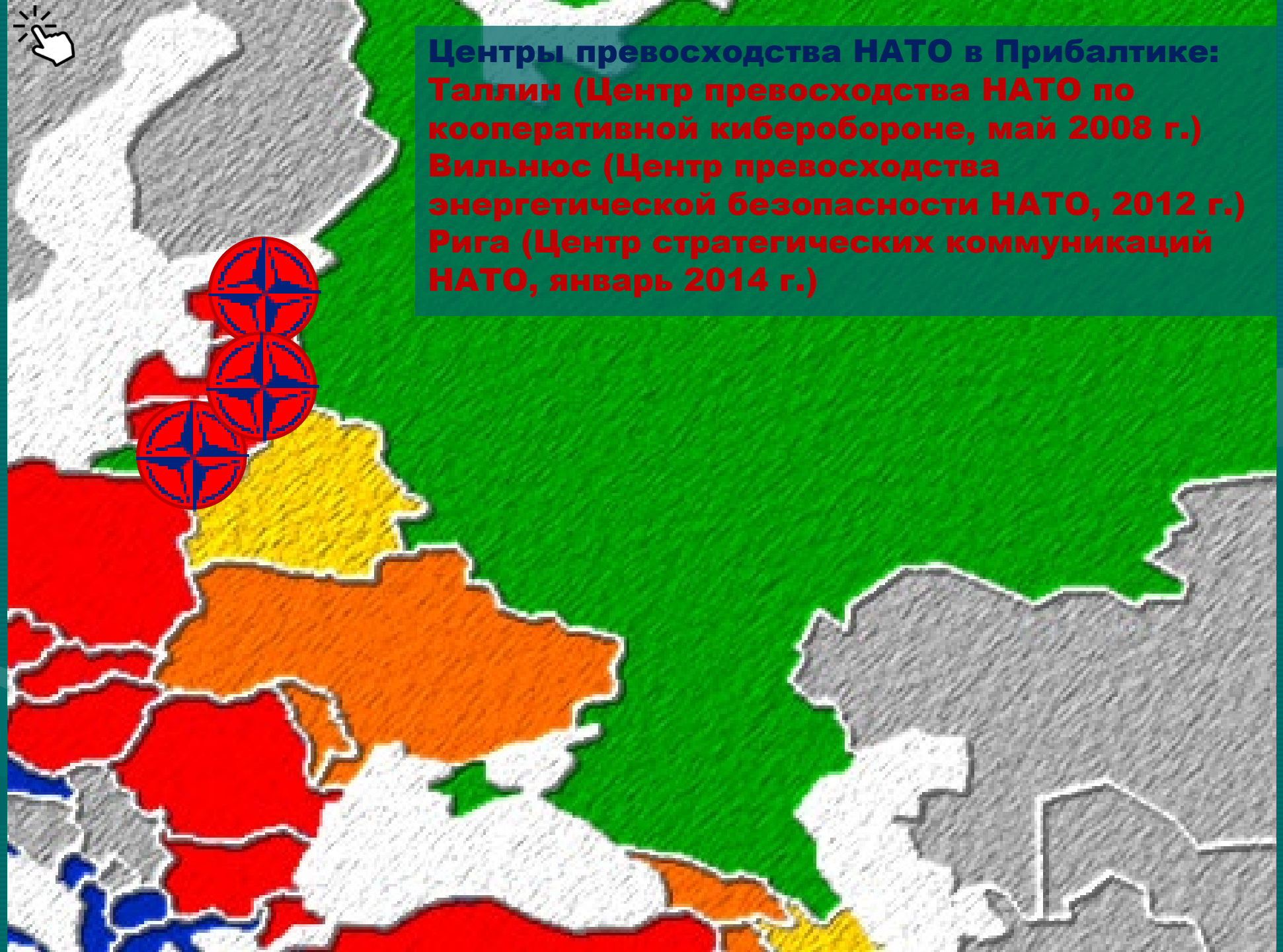
План “Анаконда” против России

Центры превосходства НАТО в Прибалтике:

Таллин (Центр превосходства НАТО по кооперативной кибероборoне, май 2008 г.)

Вильнюс (Центр превосходства энергетической безопасности НАТО, 2012 г.)

Рига (Центр стратегических коммуникаций НАТО, январь 2014 г.)



ЦЕНТРЫ ПРЕВОСХОДСТВА НАТО В ПРИБАЛТИКЕ

Таллин (Центр превосходства НАТО по кооперативной кибероборонe, май 2008 г.)

Вильнюс (Центр превосходства энергетической безопасности НАТО, 2012 г.)

Рига (Центр стратегических коммуникаций НАТО, январь 2014 г.)

Рига (Центр стратегических коммуникаций НАТО)

Он начал работать в январе 2014 г., а аккредитацию от НАТО получил 1 сентября 2014 г. Его соучредителями являются представители Эстонии, Германии, Италии, Латвии, Литвы, Польши и Великобритании.

Как указано на сайте центра, в его функции и возможности входят: общественная дипломатия, работа со СМИ по информированию деятельности НАТО, гражданско-военные связи, информационные операции и психологические операции.

Ему придается особое значение по причине комплексного характера выполняемых задач.

На базе центра проходят регулярные конференции, издаются журналы и специальные доклады-исследования. Тематический спектр самый широкий - война с помощью мемов, методы информационной войны ИГИЛ, нарративы экстремистских организаций, безопасность в ЕС, кибервойна, национализм, биометрические технологии и т.п. России уделяется особое внимание.

Так, в ноябре 2016 г. вышло два аналитических документа, посвященных России - "Когда гибридная война поддерживает идеологию: Россия сегодня" и "Русская схема игры: Понять российское влияние в Центральной и Восточной Европе".

Организации стран НАТО и союзников, задействованные в информационных операциях против России

Министерство обороны США (округ Арлингтон, шт. Вирджиния, США)

Стратегическое командование США (база ВВС США Оффут, шт. Небраска, США)

Киберкомандование США (Форт им. Джорджа Дж. Мида, шт. Мэрилэнд, США)

Агентство Национальной Безопасности США (Форт им. Джорджа Дж. Мида, шт. Мэрилэнд, США)

Информационный оперативный центр Центрального разведывательного управления США

Агентство коммуникации и информации Северо-Атлантического Альянса (НАТО) (г. Брюссель, Бельгия)

Объединённый центр передового опыта электронного противодействия НАТО (г. Таллин, Эстония)

Объединённый центр передового опыта стратегических коммуникаций НАТО (г. Рига, Латвия)

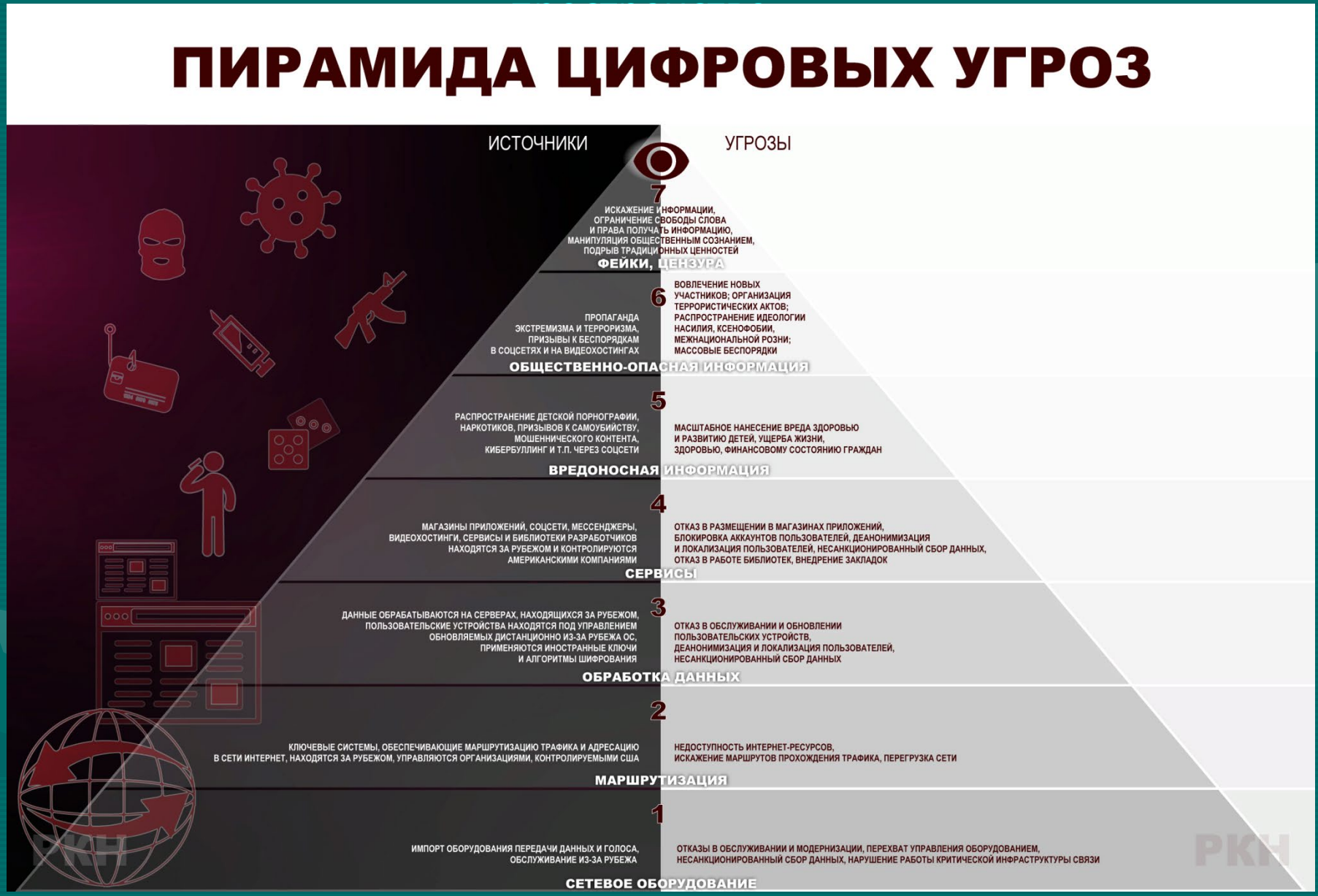
6-й центр информационно-психологических операций (ИПСО) (в/ч А1182 пос. Гуйва, Житомир, Украина)

72-й главный центр ИПСО (в/ч А4398 Бровары, Киев, Украина)

74-й центр ИПСО (в/ч А1277, Львов, Украина)

83-й центр ИПСО (в/ч А2455, Одесса)

3.02.21 г. Роскомнадзор опубликовал пирамиду современных взаимосвязанных сетевых угроз, вызванных применением цифровых технологий на семи уровнях информационного



Компьютерные атаки

Информационно-телекоммуникационное пространство глобальной сети Интернет

Информационные атаки

Программно-аппаратные платформы

Сознание: индивидуальное, групповое, общественное

Объекты атаки

- КИИ
  - Хабы, маршрутизаторы
  - ИТКС, СУБД, АСУ, СЦ, ….
- Социум
  - Личный состав МО, правоохранительных органов гражданские лица
  - ЛПР, лидеры государственных и общественных организаций

Цели атак

- Разведка уязвимостей
- Деструктивные действия/атаки
  - Целостность, конфиденциальность, доступность
- Поражение ресурса
  - ИТКС, АСУ, СУБД, СЦ,…
- Определение точек напряженности (конфликтности) в обществе
- Деструктивные действия: разжигание «цифровой толпы»
  - Сплоченность, информированность, доступность СМИ
- Захват общественного сознания
  - ИТКС, АСУ, СУБД, СЦ,…

Среда доставки атак

- Федеральные, ведомственные, региональные ИТКС, объектовые ЛВС
- Социальные сети, блогосфера, эл. форумы, видеохостинги, коммуникаторы и др.

Инструменты атак

- НСД, программно-аппаратные закладки
- Вирусы/черви
- НПО, зарубежные фонды, НОО
- Социальные вирусы/деструктивные идеи, мемы

Системы предупреждения и обнаружения воздействий/атак

- ГосСОПКА
- Социальный «РАДАР»

Коллективная информационная безопасность Союзного государства

Достижение стратегической цели обеспечения коллективной информационной безопасности Союзного государства осуществляется путем разработки и системной реализации комплекса взаимосвязанных политических, дипломатических, оборонных, экономических, информационных и иных мер, направленных на упреждение или снижение угроз коллективной информационной безопасности Союзного государства.

В области информационной безопасности:

– формирование системы коллективной информационной безопасности Союзного государства;

– развитие межгосударственного сотрудничества и укрепление межведомственной координации в сфере обеспечения информационной безопасности;

– совершенствование механизмов по противодействию угрозам в информационной сфере;

– проведение совместных мероприятий по противодействию и нейтрализации противоправной деятельности в информационно-телекоммуникационном пространстве Союзного государства;

– взаимодействие в вопросах обеспечения международной информационной безопасности;

– выработка согласованных правил взаимодействия в информационной сфере, продвижение их на международный уровень;

– создание условий и реализация совместных практических мероприятий, направленных на формирование основ скоординированной информационной политики в интересах Союзного государства.

В сфере противодействия современным, в том числе, комбинированным формам воздействия на Союзное государство с целью разрушения государственности, дестабилизации внутриполитической ситуации или смены политических режимов необходимо осуществить следующие действия:

– на основе изучения и анализа практики применения извне технологий так называемых «цветных революций» и «гибридных войн» разработать совместные меры и технологии противодействия им;

– сформировать коллективную систему упреждения и реагирования на «гибридные», в том числе, информационные угрозы, использующие в качестве среды воздействия единое информационное пространство Союзного государства.

Предложения по консолидации деятельности государственных и общественных структур в целях ещё более тесного сближения братских народов Беларуси и России в рамках Союзного государства

1. Парламентскому Собранию Союза Беларуси и России.

Разработать и принять в кратчайший срок Закон «О коллективной информационной безопасности Союза Беларуси и России»

(Предусмотреть в нем гармонизацию национальных законов в этой сфере; спектр общих угроз; зоны ответственности; систему оперативного реагирования на коллективные вызовы и угрозы в этой сфере).

2. Советам Безопасности Беларуси и России.

2.1. Создать межгосударственную совместную рабочую группу Союза Беларуси и России по разработке «Концепции совместного реагирования на вызовы и угрозы информационной безопасности Союзного государства».

2.2. Разработать и принять Стратегию совместных антисетевых действий в едином информационном пространстве Союзного государства».

3. Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры) и Министерству информации Республики Беларусь (Мининформ).

3.1. Создать ТВ-канал Союзного государства под эгидой Парламентского Собрания Союза Беларуси и России.

3.2. Создать интернет-ресурс «Наш Союз», на котором открыть молодежный портал творческих инициатив, стартапов, инновационных проектов, объединений по интересам, клубы исторической памяти, поисковиков и т.д.

3.3. Проводить совместные фестивали песни и музыкального творчества помимо Витебска (год в России, год в Беларуси).

3.4. Проводить форумы, в том числе, on-line, по восстановлению исторической памяти о тяжких испытаниях, которые прошли братские народы России, Белоруссии и Украины в годы ВОВ:

- организация совместного неразделного Бессмертного полка 9 мая ежегодно
- правда о геноциде славянских народов СССР;
- обличение преступных организаций и подразделений СС из этнических добровольцев, творивших невиданные злодеяния на оккупированных территориях СССР

4. Минобрнауки РФ и Министерству образования РБ

Гармонизировать образовательные стандарты и программы в области ИБ (мягкая сила, взаимная приемлемость дипломов, обмен студентами и аспирантами и др.);

5. Министерству спорта и туризма Республики Беларусь и Министерству спорта РФ

Обеспечить развитие историко-патриотического туризма, включающего:

- сохранение и восстановление всех видов памятников военной истории;
- создание историко-культурных центров, кружков, которые бы занимались подобными проектами;
- поддержка военно-исторических клубов, поисковых организаций;
- организация на постоянной основе военно-патриотических спортивных соревнований, военно-исторических реконструкций
- создать совместную цифровую площадку Союзного государства, где бы молодежь могла делиться интересными маршрутами, в том числе проходящих через Союзное государство;
- создать актуализированный цифровой контент, в том числе, для продвижения рекламы о туризме в Беларуси и России на внутреннем и мировом уровне и т.д.

- Благодарю за внимание!

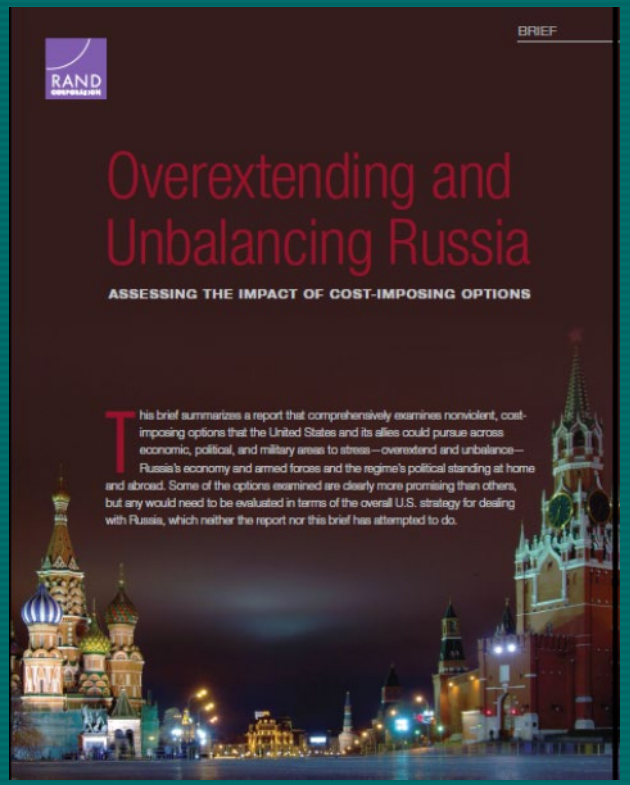
«Extending Russia. Competing from Advantageous Ground»

(«Истощение России через расширение ее вовлеченности: противоборство на лучших условиях»)

Новая стратегия нацелена на то, чтобы заставить Москву отказаться от планов укрепления позиций на перспективных внешних площадках (например, на Ближнем и Среднем Востоке, в Арктике, на Дальнем Востоке), концентрируя ограниченные ресурсы на поддержании стабильности в своем ближайшем окружении и нейтрализуя конфликты с ключевыми в экономическом плане партнерами.

Цель политики США в том, чтобы лишить Москву самостоятельного операционного и инвестиционного потенциала для консолидации вокруг себя контролируемого экономического пространства и формирования значимых в геоэкономическом плане инвестиционных систем, обеспечивающих хотя бы базовый уровень экономического роста. Естественно, в этих условиях ключевым пространством конкуренции становится постсоветская Евразия, что в целом не скрывается американскими политическими аналитиками.

Новая-старая стратегия США в отношении России



Американская корпорация RAND — один из главных аналитических центров Пентагона и разведслужб США — представила доклад **Overextending and Unbalancing Russia. Assessing the Impact of Cost-Imposing Options («Слишком большая и несбалансированная Россия. Оценка влияния затратных вариантов»)**. Документ является практической рекомендацией: как Западу использовать уязвимости Москвы, чтобы еще сильнее ограничить ее политические и экономические возможности? Главная цель всего комплекса мер — усилить давление на Москву, чтобы заставить её «перенапрячься и разбалансироваться».

Меры воздействия на Кремль сгруппированы в четыре блока.

Первый блок — экономический. Включает следующие опции:

- увеличение добычи и экспорта энергоносителей в США, чтобы повлиять на мировые цены и снизить прибыль РФ.
- Усиление санкций, и участие других стран в этом процессе.
- Помощь Европе в поисках новых поставщиков газа, включая СПГ.
- Поддержка миграции из России в другие страны образованной молодежи.

Overextending and Unbalancing Russia. Assessing the Impact of Cost-Imposing Options

Третий блок доклада — идеологические и информационные меры, направленные на дестабилизацию ситуации внутри РФ. Он включает в себя:

— подрыв доверия к избирательной системе;

— создание восприятия, что политическая элита не служит интересам общества;

— подстрекательство к протестам и ненасильственному сопротивлению;

— подрыв имиджа России за рубежом.

Таллин (Центр превосходства НАТО по кооперативной кибероборонe, май 2008 г.)

Центр превосходства НАТО по кооперативной кибероборонe является первой организацией подобного рода на постсоветском пространстве в странах Прибалтики. Он размещен в столице Эстонии Таллине. Часто в высказываниях представителей НАТО или американских экспертов дается оценка, что решение по созданию такого центра именно в Эстонии было связано с инцидентом вокруг памятника советскому солдату в 2007 г. Якобы тогда хакеры из России обвалили кибер инфраструктуру Эстонии - банки не смогли работать, сервера государственных служб были парализованы. На самом деле просьба о создании киберцентра в Таллине поступила гораздо раньше — еще в 2004 г, сразу же после вступления страны в альянс. В 2006 г. верховное командование окончательно одобрило это решение и в 2007 г. начались переговоры о создании центра.

С данным центром связано и появление так называемого Таллинского руководства по кибервойне. Хотя этот документ представляет всего лишь экспертные мнения и не является полевым уставом или стратегией, на Западе часто ссылаются на него в качестве принципиального свода правил по действиям в киберпространстве в случае каких-либо конфликтов.

Вильнюс (Центр превосходства энергетической безопасности НАТО, 2012 г.)

Это первый и единственный центр подобного рода в Альянсе. Центр передового опыта НАТО по энергетической безопасности будет заниматься идентификацией потенциальных энергетических угроз и выработкой предложений для членов Альянса по эффективной борьбе с ними, разрабатывать механизмы оказания союзниками НАТО взаимной помощи в чрезвычайных ситуациях и проводить обучения военных по защите энергетических объектов и инфраструктуры стратегического значения.

Центр проводит курсы и имеет места для студенческой практики (расходы на проживание и обучение оплачиваются НАТО).

Также издаются тематические журналы и публикуются результаты исследований, в которых нередко говорится о необходимости избавиться от "энергетической зависимости от России". *Угроза энергетической безопасности Украины со стороны России — одна из постоянных тем последних номеров. Хотя не забываются и другие регионы постсоветского пространства, а также сама Европа.*

Лейтмотив "энергетической войны" с Россией хоть и не обозначен в официальных задачах центра, но очевиден не только в материалах, но и проводимых мероприятиях. Причем заметны постоянные попытки втянуть в орбиту НАТО страны, которые не входят в альянс и находятся на границе с Россией.

ДЕНЬ ЕДИНЕНИЯ НАРОДОВ БЕЛАРУСИ И РОССИИ

ИСТОРИЯ ПРАЗДНИКА

2 апреля — День единения народов Беларуси и России. В этот день в 1996 году был подписан Договор «Об образовании Сообщества России и Белоруссии».

Союзное государство, как записано в Договоре о его создании, — это светское, демократическое, социальное, правовое государство, в котором признано политическое и идеологическое многообразие.

Союзное государство базируется на принципах суверенного равенства Республики Беларусь и Российской Федерации, добровольного и добросовестного выполнения ими взаимных обязательств. Основой его является разграничение предметов ведения и полномочий между Союзным государством и государствами-участниками.

И Беларусь, и Россия, с учетом добровольно переданных Союзному государству полномочий, сохраняют свои суверенитет, независимость, территориальную целостность, государственное устройство, конституцию, государственный флаг, герб и другие атрибуты государственности.

В Союзном государстве признаются и равным образом защищаются все формы собственности, признаваемые на территориях государств-участников, и обеспечиваются равные права граждан на приобретение, владение, пользование и распоряжение имуществом.

По случаю Дня единения народов Беларуси и России в Республике проводят следующие праздничные мероприятия:

— торжественные заседания, в которых принимают участие представители интеграционных органов, законодательной и исполнительной власти, творческой и научной интеллигенции, молодежи;

— концерты, в которых выступают ведущие исполнители и коллективы из двух стран;

— церемонии вручения премий Союзного государства в области литературы и искусства.

СТУДГАЗЕТА МЕТРОНОМ

Гибридная война – что это такое?

Гибридная война – совокупность методов военно-силового, политико-дипломатического,финансово-экономического, информационно-психологического и информационно-технического давления, а также технологий цветных революций, терроризма и экстремизма, мероприятий спецслужб, формирований сил специального назначения, сил специальных операций и структур публичной дипломатии, осуществляемых по единому плану органами управления государства, военно-политического блока или ТНК.

Цели гибридной войны – полная или частичная дезинтеграция государства, качественное изменение его внутри — или внешнеполитического курса, замена государственного руководства на лояльные режимы, установление над страной внешнего идеологического и финансово-экономического контроля, ее хаотизация и подчинение диктату со стороны других государств или ТНК.

Духовная война

•перекодировка национального самоосознания,
•смена веры(ований), уничтожение (подмена) знаний,
•искажение(подмена) языка(логоса),
•уничтожение (подмена) культурных артефактов (письменных источников, памятников архитектуры, эпоса, песенного и танцевального фольклора, замена национального костюма на одежду «унисекс» и т.д.)

Психотронная война

•HAARP,
• психотроника: генераторы НЧ, СВЧ;
•пси-вирусы;
•психокорректирующие игры;
•НЛП

Информационно-психологическая война

➢**дуплексные коммуникативные каналы воздействия:**
•социальные сети, ЖЖ, блогосфера;
➢**интерактивное ТВ, мобильные платформы коммуникаторов; однонаправленные каналы воздействия:**
•электронные СМИ (ТВ, радио, печать),

Информационно-техническая война

•глобальные и локальные сети, телекоммуникации, СУБД,
• ЦАТС, маршрутизаторы, трансляторы,
•SCADA-системы, АСУ ТП и т.д.)

Информационно-биологическая война (рассовое оружие)

➢информационное воздействие на генном уровне: генномодифицированные и синтетические продукты, наркотики, лекарства, алкоголь, «энергетические» напитки,
➢воздействие на среду обитания (биофизические воздействия, воздействия на климат).

«Для предотвращения и сдерживания злонамеренной киберактивности против Соединённых Штатов могут быть использованы все инструменты государственной власти. Сюда относятся дипломатические, информационные, военные, финансовые, интеллектуальные, общественные и правоохранительные возможности», – говорится в Стратегии.

«Все инструменты» – это и санкции, и пропагандистская кампания и ракетный удар.

И ещё один примечательный пункт Стратегии, на который обратило внимание издание Global Security: «Национальная киберстратегия сохранит в долгосрочной перспективе открытость Интернета, что поддержит и заново обозначит американские интересы». То есть американцы по-прежнему отвергают обсуждение проблем национальной юрисдикции в Интернете. «Ответственное поведение» в киберпространстве должно сводиться к следованию правилам, которые установят США. А тот, кто откажется этим правилам следовать, будет объявлен изгоем и обвинён в «злонамеренных действиях». Уже сам отказ от принятия американских правил будет трактоваться как ведение войны против Америки. Это так же серьёзно, как знаменитая фраза Джорджа Буша-младшего после атаки на небоскрёбы в Нью-Йорке 11 сентября 2001 года: «Кто не с нами, тот против нас».