Хибридна война срещу (назоваването на) Хибридната война

Hybrid warfare against (the naming of) the Hybrid warfare

д-р Велизар Шаламанов

Българска Академия на Науките

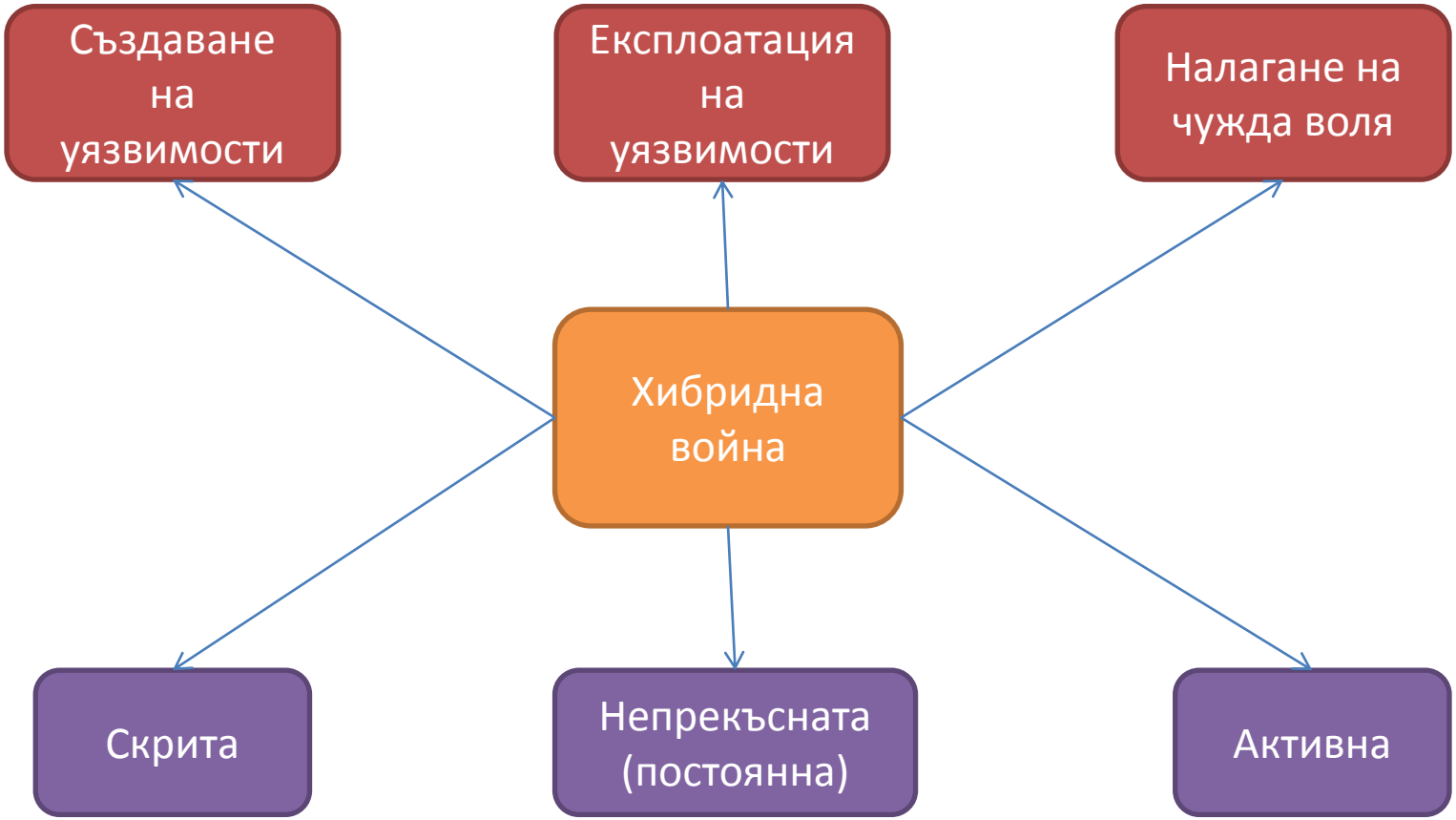
Основни въпроси:

- Свобода – сила – демократичен контрол
- Характеристики на хибридната война, като инструмент за налагане на чужда воля и подтискане на правото на избор
- Примери от кризите 1999 и 2014
- Поуки от опита по противодействие на хибридни заплахи (вкл. от СИ Европа)
- Пътят напред: формиране на среда, отговор на заплахи, подготовка за бъдещето

Свобода – сила – демократичен контрол

- Основната разлика / граница между нас и „другите“ е свободният избор
- За нас свободният избор е основен източник на сила – за тях свободният избор е основна заплаха
- Войната е налагане на чужда воля със силови действия (от различен характер) и ограничаване правото на избор
- Силата, без демократичен контрол на свободно общество бързо става брутална и често се срива под собствената си тежест
- Хибридната война е използване на сила под нивата на чл. 5 на Вашингтонския договор и изисква нови модели за възпиране и отбрана (без да намалява значението на ядреното възпиране и поддържането на технологично превъзходство за конвенционални действия)
- Новите модели изискват същите нива на демократичен контрол, както конвенционалните и ядрените сили, за да могат да служат на свободния свят

Характеристики на хибридната война



Тези характеристики я правят много „подходяща“ за изпълнение от ГРУ, като все повече фокуса е върху кибер пространството, но не само.

Примери от кризите 1999 и 2014

- 1999 - Косово: ВМСЦ-СС-МС откроии доста случаи на хибридни атаки от Сърбия, подкрепени от Русия – създаените мрежи за хибридни действия действат и до днес
- 2014 - Украйна:
  - Реакция на „Визия 2020“ от Атака, АБВ и др.
  - Фестивал на военни оркестри в Москва по време на срещата в Уелс
  - Авиошоу на аерогара „София“ преди изборите
  - Реакция на НП 2020 от вицепремиера Рогозин

Поуки от опита по противодействие на хибридни заплахи

1. Противодействието изисква добро боравене с много източници на информация в реално време
2. Реалното възпиране на атаките изисква координирано действие на много (ако не всички) инструменти на властта – **всеобхватен подход**
3. Взаимодействието в съюзна среда е от ключово значение
4. Превантивното и постоянно усъвършенстване на институциите, заедно с подготовка на обществото е най-важната мярка
5. Решително противодействие на чужди разузнавания е основополагаща мярка
6. Първата стъпка е назоваването на заплахата и източника
7. Горните мерки трябва да са подкрепени от способности за възпиране на конвенционални заплахи и ядрени провокации

Пътят напред: формиране на среда, отговор на заплахи, подготовка за бъдещето

1. Изграждане на център за противодействие на хибридни и кибер заплахи в МО с междуведомствени способности, интегриран в мрежата на НАТО и ЕС
2. Укрепване на контраразузнаването
3. Развитие на пакет от инструменти за неутрализиране на действия от хибриден характер (вкл. дипломатически)
4. Укрепване на институциите със системна подготовка, вкл. редовни симулационни учения и изследвания по жибридните заплахи (JTSAC-Resilience)
5. Засилена координация със съседите – съюзници и партньори в ЮИЕ/Черноморието
6. Особен фокус на кибер пространството, вкл. социални мрежи и критична инфраструктура
7. Използване на NFIU и CoE, изградени по линия на НАТО (опит от Скандинавсия регион, Балтийския регион и Вишеградската група)

Balkans (10 countries) + Black Sea-Caucasus (4 more to the East)

Basic Environment for Simulation & Training: „Resilience“