МГИМО УНИВЕРСИТЕТ

НАМИБ

НИИГлоБ

НАЦИОНАЛЬНЫЙ ИНСТИТУТ ИССЛЕДОВАНИЙ ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ

NATIONAL INSTITUTE FOR RESEARCH OF GLOBAL SECURITY

Международная конференнция 13.12.2018

Киберстабильность: подходы, перспективы, вызовы

INFOGENIC CHALLENGES OF HYBRID WARS IN THE CONTEXT OF GLOBAL SECURITY

ANATOLY I. SMIRNOV

Director General of the National Association of International Information Security, President of NIIGLOB,

Doctor of Historical Sciences, Professor, Chief Scientific Officer of MGIMO of the MFA of the Russian Federation

http://namib.online/

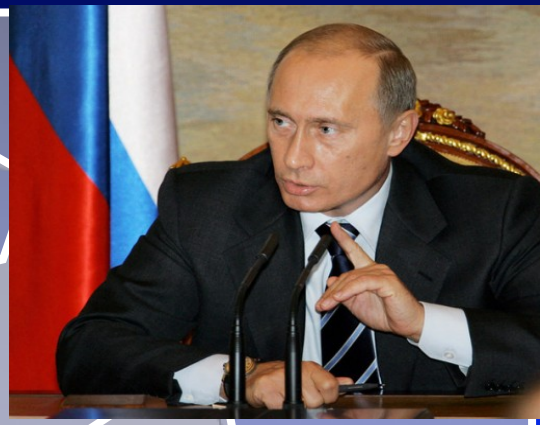
- The history of wars is a history of technological breakthroughs…

- It is said that wars start in people's heads, but according to this logic, it is also in people's heads that they should end!

-You cannot wait until a house burns down to buy fire insurance on it

http://www.stantonchase.com/wp-content/uploads/2016/09/Leadership-in-F

Russian National Security Strategy, December 2015



12. The strengthening of Russia is taking place against a backdrop of new threats to national security that are of a multifarious and interconnected nature. The Russian Federation's implementation of an independent foreign and domestic policy is giving rise to opposition from the United States and its allies, who are seeking to retain their dominance in world affairs. The policy of containing Russia that they are implementing envisions the exertion of political, economic, military, and informational pressure on it.

21. The intensifying confrontation in the global information arena caused by some countries‘ aspiration to utilize informational and communication technologies to achieve their geopolitical objectives, including by manipulating public awareness and falsifying history, is exerting an increasing influence on the nature of the international situation.

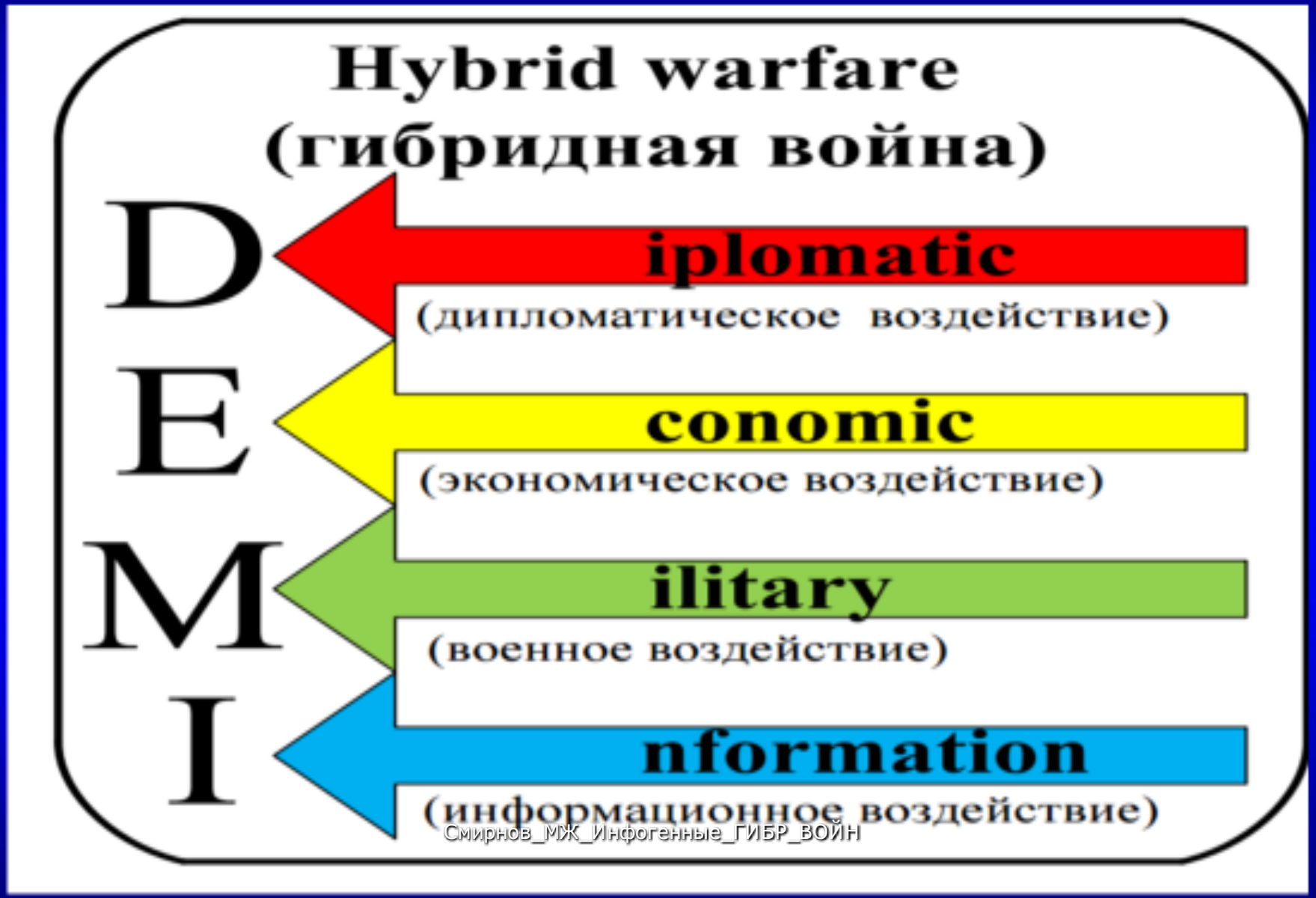
FOREIGN POLICY CONCEPT OF THE RUSSIAN FEDERATION

Approved by V. Putin 30.11 2016

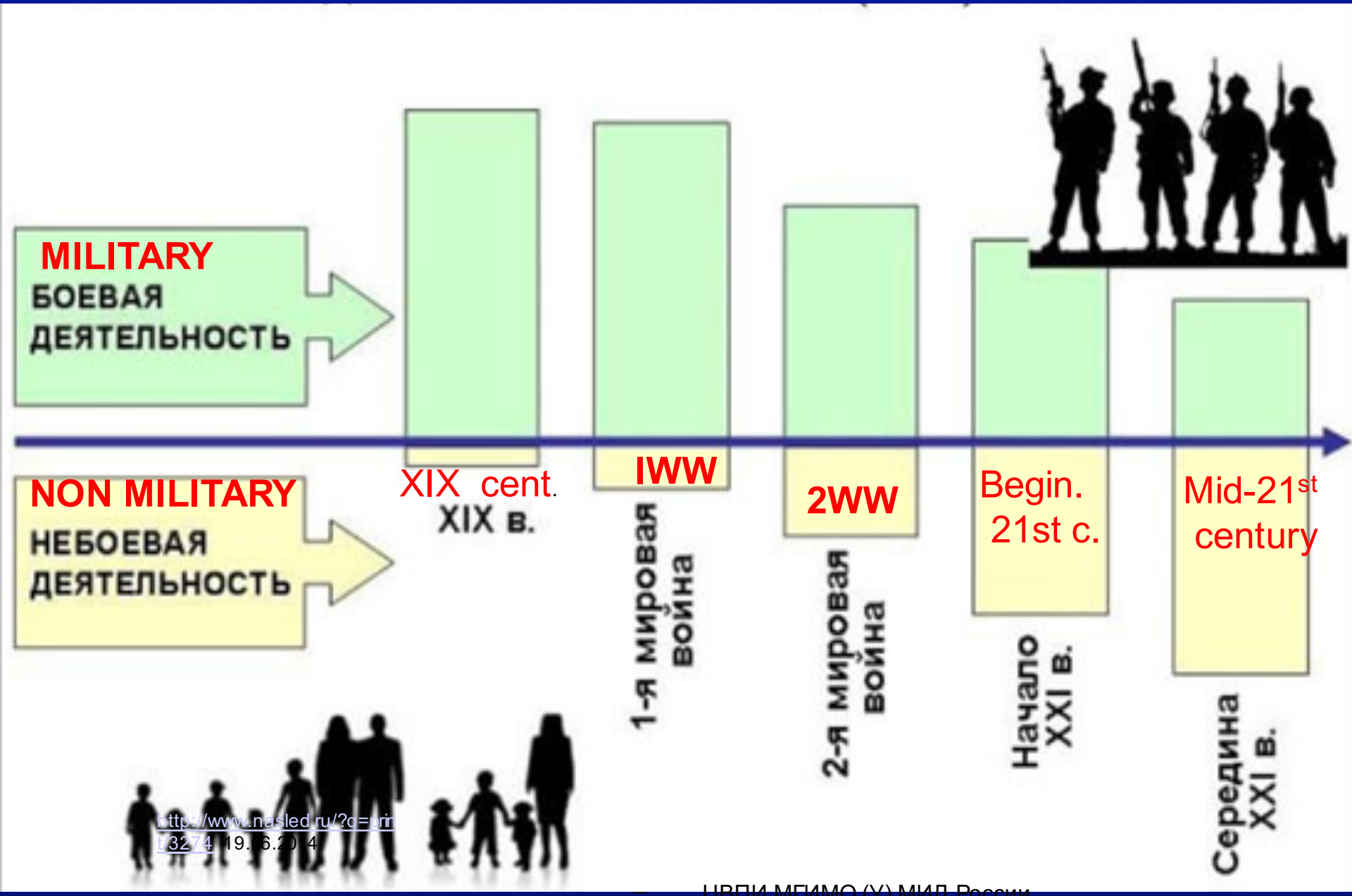
28. Russia takes necessary measures to ensure national and international cyber security, counter threats to State, economic and social security emanating from cyberspace, combat terrorism and other criminal threats involving the use of information and communication technology;

- deters their use for military-political aims that run counter to international law, including actions aimed at interfering in the domestic affairs of States or posing a threat to international peace, security and stability;
- and seeks to devise, under the UN auspices, universal rules of responsible behaviour with respect to international cyber security, including by rendering the internet governance more international in a fair manner.

HYBRID WAR - THE RENAISSANCE OF CONTAINING RUSSIA



Mankind goes to generations of hybrid wars….



72. We have taken steps to ensure our ability to effectively address the challenges posed by hybrid warfare, where a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, are employed in a highly integrated design by state and non-state actors to achieve their objectives. Responding to this challenge, we have adopted a strategy and actionable implementation plans on NATO's role in countering hybrid warfare. The primary responsibility to respond to hybrid threats or attacks rests with the targeted nation. NATO is prepared to assist an Ally at any stage of a hybrid campaign. The Alliance and Allies will be prepared to counter hybrid warfare as part of collective defence. The Council could decide to invoke Article 5 of the Washington Treaty. The Alliance is committed to effective cooperation and coordination with partners and relevant international organisations, in particular the EU, as agreed, in efforts to counter hybrid warfare.

USA - pioneer of hybrid wars. General Mattis (US Secretary of Defense): How Marines are preparing for hybrid wars March 1, 2006

http://armedforcesjournal.com/how-marines-are-preparing-for-hybrid-wars/

U.S. Must Prepare for 'Hybrid' Warfare February 13, 2009

http://smallwarsjournal.com/blog/general-mattis-us-must-prepare-for-hybrid-warfare

?

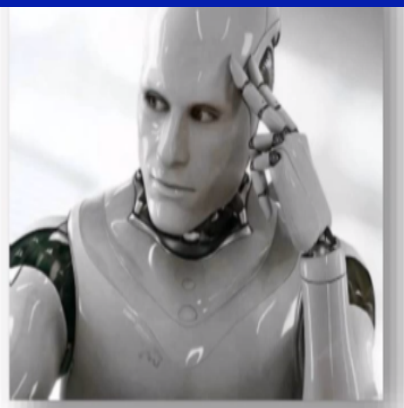
2003: U.S. Secretary of State Colin Powell holds up a vial that he described as one that could contain anthrax during his presentation on Iraq to the UN Security

США: роль ИКТ в «силовом» сценарии сдерживания РФ

- Решение Б.Обамы о закладке в КИИ РФ «кибербомб» (WP 23.6.17);
- Wikileaks: у ЦРУ есть СПО для атак под «чужим флагом» (03.2017)
- Доктрина нац.безопасности США (дек. 2017) содержит 45 раз термин «Кибер», противники: КНР, РФ, Иран, КНДР;
- Отказ США от создания группы по кибербезопасности на G 20 (2017)
- «CIOUD Act» (23.03.2018) доступ ФБР, ЦРУ и т.д. к инфо всех устройств, во всем мире (и РФ), вендоры которых фирмы США;
- закон №115-232 (13.08.2018) о военном бюджете: ст.1655 исключает фирмы, давшие исходные коды ПО для лицензий за рубежом
- 16.08.2018 - Трамп отменил указы Обамы о правилах кибератак
- 09.2018 - Стратегия кибербезопасности МО – преамбула кибервойны
- 09.2018 - Национальная киберстратегия – курс на кибернаступление
- 10.2018 – Создание Федерального агентства по кибербезопасности США

США: ГОНКА ЗА ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ (AI)

- 2016: **$26-39 млрд** ← Проект ИИ



- США

  50% инвестиций

  Рост 50% в год

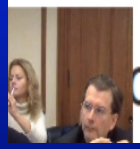
Проект Аполлон:
$146 млрд за 13 лет

- Китай:

  30% инвестиций

  ст 70% в год

Манхэттенский проект:
$21 млрд за 3 года

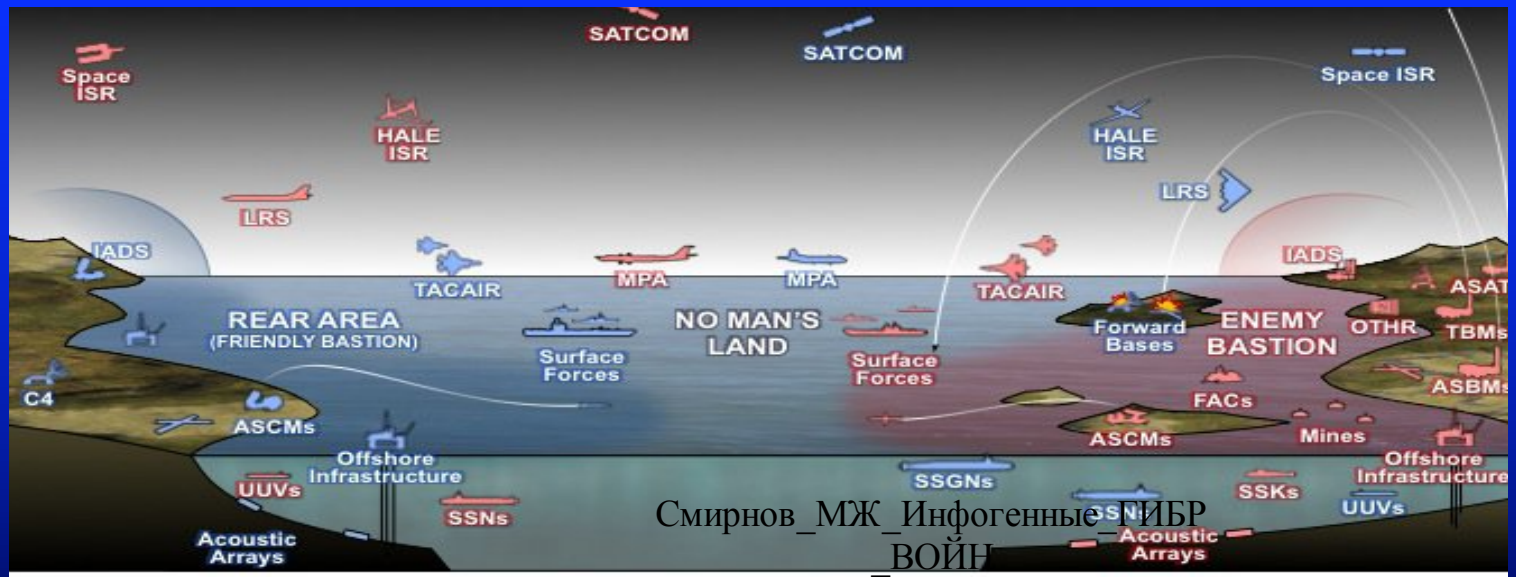


Угроза притязаний на глобальное лидерство с использованием Смертоносных автономных систем (САС) с применением ИИ

ГПЭ ООН по неконвенциальному оружию: САС обеспечат вооруженным силам технологический отрыв от соперников.

«Доминирование по полному спектру» (Full Spectrum Dominance) - способность контролировать любую ситуацию и победить противника во всем диапазоне военных действий.

Третья стратегия компенсации (third offset strategy): автономные роботы с ИИ смогут обеспечить военное доминирование на планете, заменив ядерное оружие и высокоточные боеприпасы.



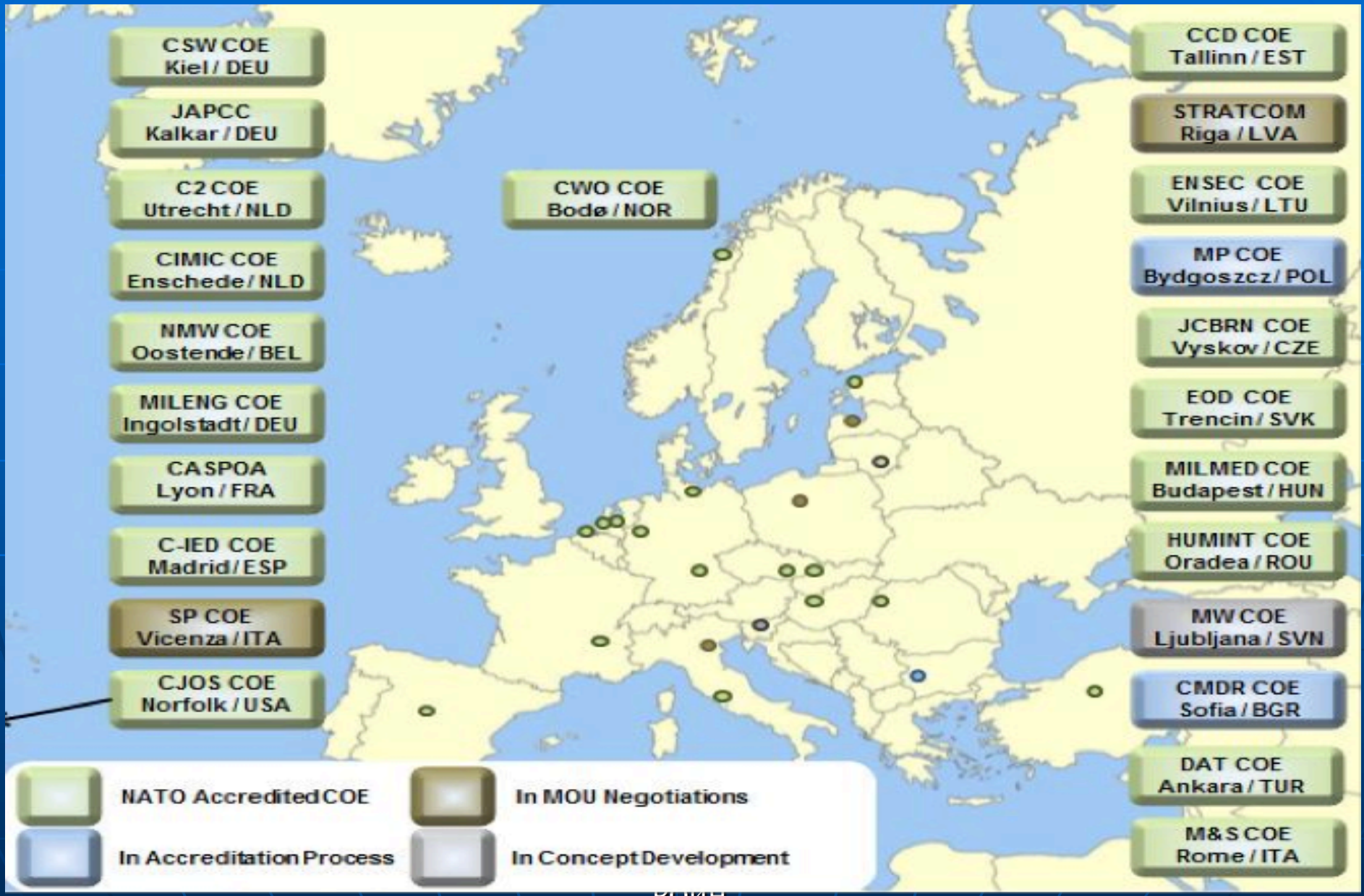
1950-е ЯО

1970-е Высокоточн.

2020-е Беспилотн. ИИ

НАТО: Центры передового опыта (на 2016 г)

http://www.eguermin.org/welcome/centre-of-excellence/



Объединенный центр кибероборонЫ НАТО в Таллине

Международно-правовая база для наступательной кибервойны

Создан в 2008 г.
задачи – консультирование, обучение специалистов и исследования в области кибербезопасности.

Санкционирует:
-применение кинетического оружия против киберугрозы;
-силовые действия военных в отношении гражданских;
-военные кибероперации, против КИИ

2013 г – Таллинское руководство по применению международного права к киберконфликтам – 95 правил;
2017 – Таллинское руководство 2.0 – 124 правила

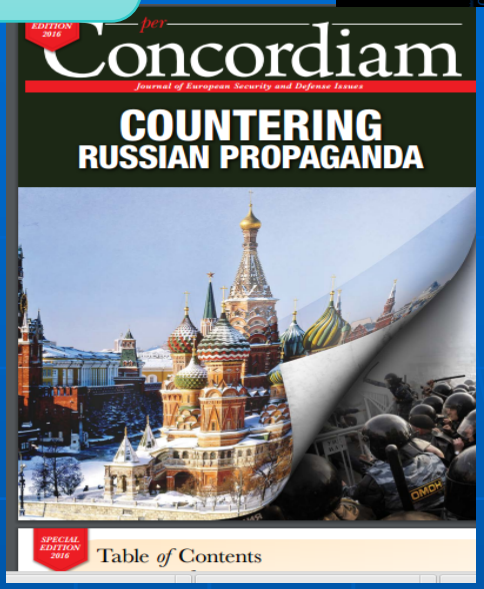
Cyber Conflict 2018

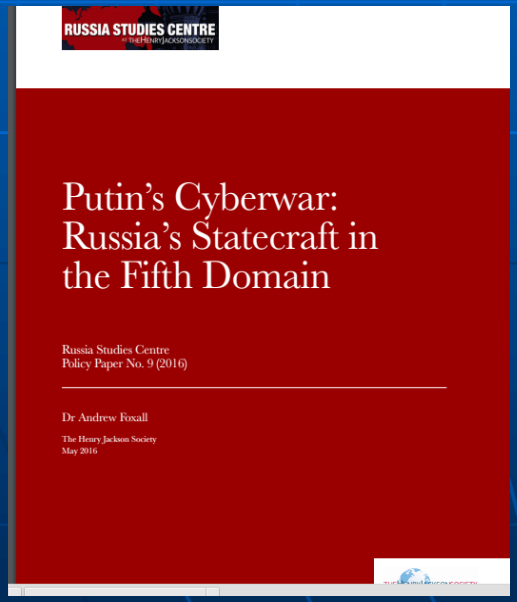
- 30.05-1.06.18 - 700 cyber experts from more than 40 nations.
- „CyCon, together with yesterday's Munich Security Conference Cyber Security Summit, turn Tallinn into a real Cyber Woodstock hosting discussions that shape the future of cyber security… Together we can maximise the effects of our efforts," said Merle Maigre, Director of the NATO-accredited cyber defence hub.
- The conference was opened by H.E. K. Kaljulaid, the President of Estonia. Other speakers include A.Stamos, CSO of Facebook; Dr. J. Zangardi, the CIO for the US DHS; Dr. A. Missiroli, NATO Assistant Secretary General; General R. Neller, Commandant of the Marine Corps, B. Schneier, internationally acclaimed cryptographer; C. François, Intelligence Director of Graphika; T. Dullien, Staff Software Engineer at Google Zero; Dr. K. Jones, Head of Cyber Security Architecture at Airbus; Dr B. M. Pierce, Director of the DARPA Information Innovation Office and many others… Cyber Conflict 2019: 28 - 31 May „Silent Battle"

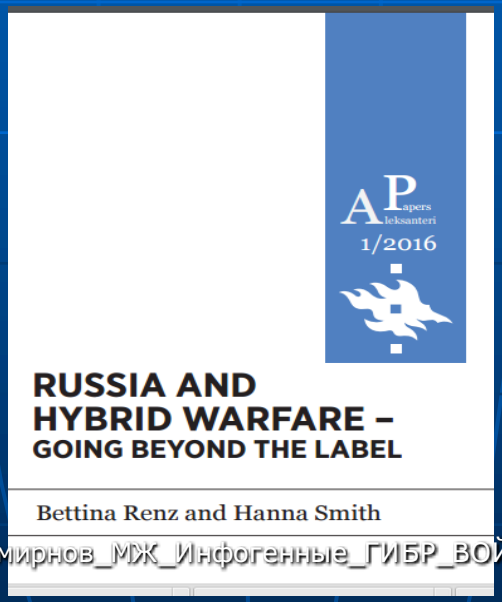
NATO Won Cyber Defence Exercise Locked Shields 2018

- 23-27.04.18 27 April 2018
- The team from NATO won the largest and most complex international live-fire cyber defence exercise (1000 experts from 30 countries)
- It was the first time NATO participated with a team representing different NATO agencies
- The exercise involved around 4000 virtualised systems and more than 2500 attacks altogether Protection of critical infrastructure is essential for ensuring the efficient operation of both military and civilian organisations…

NATO Strategic Communications Centre of Excellence and «cold war 2.0»







NATO Strategic Communications Centre of Excellence and «cold war 2.0»

Publications

Select ☐ Book ☐ Executive summary ☐ Journal ☐ Policy paper ☐ Manual ☐ Research ☐ Article

9th December 2018

The Role of Communicators in Countering the Malicious Use of Social Media

Type: Research

Download | Preview

9th December 2018

Industry Responses to the Malicious Use of Social Media

Type: Research

Download | Preview

9th December 2018

Government Responses to Malicious Use of Social Media

Type: Research

Download | Preview

25th September 2018

Russia's Arctic Strategy

Type: Executive summary

22nd November 2018

Robotrolling 2018/4

Type: Executive summary

26th September 2018

Arctic Narratives and Political Values

Type: Research

NATO: Look how close Russia put its country to our military bases!

The European Centre of Excellence for Countering Hybrid Threats of EU and NATO

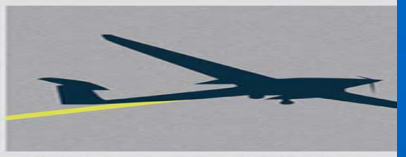
Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

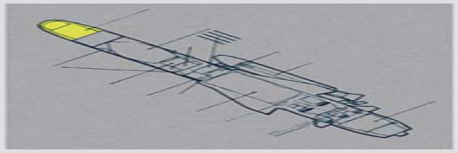
6 December 2016
Council of the EU and North Atlantic Council endorse
40 proposals in 7 areas


hybrid threats

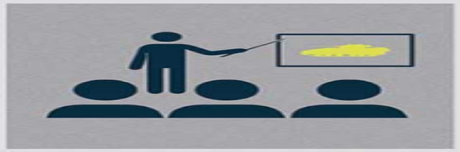

operational cooperation, including maritime issues

cyber security


defence capabilities


industry and research


exercises


capacity building

NEWS

November 21, 2018

Hybrid CoE presents the first year results in Brussels

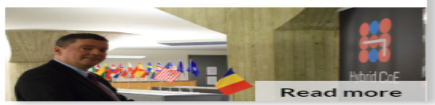
Today Hybrid CoE's two Communities of Interests (CoIs) presented the results of the fir...

Read more

November 14, 2018

Romania becomes a member of Hybrid CoE

H.E. Mr. Răzvan Rotundu, Ambassador of Romania to Finland, this afternoon signed a noti...



Read more

October 30, 2018

Canada joins Hybrid CoE

Today Colleen Merchant, Director General of the Canadian Cyber Security Centre gave a n...

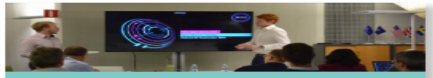
Read more

October 15, 2018

Call for Papers – Conference on 'Legal Resilience in an Era of Hybrid Threats'

The Exeter Centre for International Law is hosting a conference on the subject of¬...

Read more



October 10, 2018

Trainings on Open Source Material

In late September the European Centre of Excellence for Countering Hybrid Threats (Hybr...

Read more

October 4, 2018

Expert-pool trend mapping Western Balkans

This week the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) ...

Read more

September 28, 2018

Hybrid CoE Supports Informal NAC-PSC Discussion

This week the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) ...

Read more

Tweets by @HybridCoE

Hybrid CoE
@HybridCoE

Countering Disinformation will remain a clear focus for @HybridCoE in 2019. We will improve Member State capability by:
✅training stratcom experts and OSINT specialists from our 19 member states
✅bringing in private sector expertise
✅exercising journalists

Embed View on Twitter

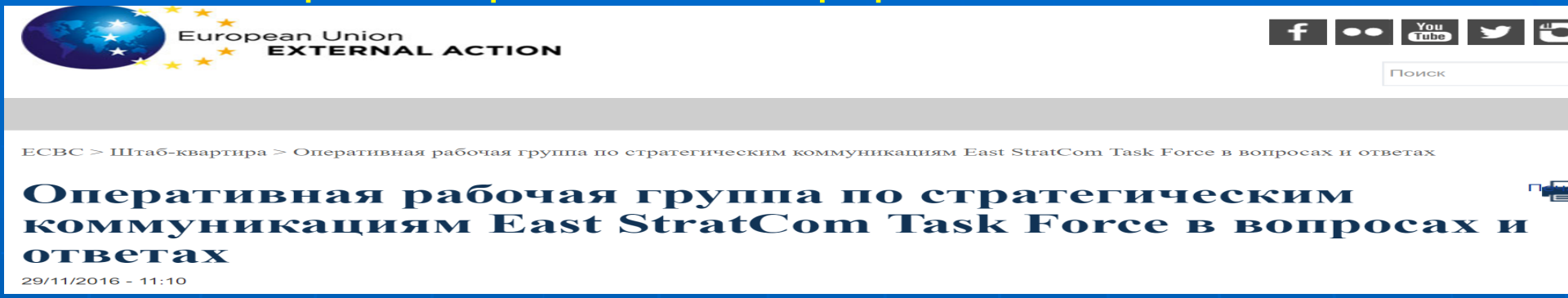
НОВЫЙ ЦЕНТР КИБЕРОПЕРАЦИЙ НАТО

Мы должны обеспечить в киберпространстве такую же эффективность, как и на суше, на море и в воздухе.

- Новый центр кибероперацийв г.Монсе(Бельгия) состоит из 70 экспертов, которые будут получать разведданные и информацию в режиме реального времени.
- Ранее генсек НАТО Столтенберг допустил возможность применения НАТО Статьи 5 о коллективной обороне в случае серьезных кибератак со стороны России

После Саммита НАТО в Брюсселе (июль, 2018): между НАТО и ЕС достигнуты соглашения по 74 направлениям сотрудничества, в т.ч. по кибербезопасности и военному сотрудничеству.

Оперативная рабочая группа по стратегическим коммуникациям ЕС – инструмент дезинформации и фальсификации – информационный спецназ!



В 2015 г. на основании решения ЕС о противостоянии дезинформации РФ создана служба для поддержки делегаций ЕС (во главе - британский дипломат Портмен).

В её составе 4 сотрудника ЕСВД и пять экспертов из Великобритании, Дании, Латв Чехии и Эстонии. И ГЛАВНОЕ: с ней сотрудничает около 400 журналистов и эксперто

В задачи службы входит разъяснение ключевых аспектов политики ЕС, создание его позитивного образа и противодействие дезинформации путем выпуска еженедельног бюллетеня «Обзор дезинформации».

При этом указанные «Обзоры» не могут являться официальнаой позицией ЕС. Их анализ показывает слабо аргументированный, подчас фейковый уровень и откровенную русофобию.

«ПРОДУКТ» РАБОЧЕЙ ГРУППЫ ЕС ОТ 12.12.2018

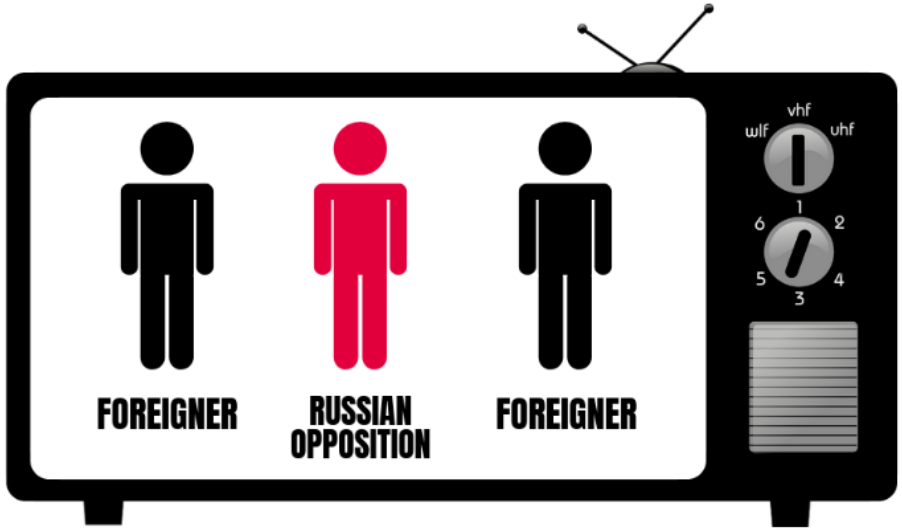
EU vs Disinfo

IN THE MEDIA SUBSCRIBE EN RU DE

NEWS AND ANALYSIS DISINFO REVIEW DISINFO CASES READING LIST ABOUT CONTACT US

"You Always Place Me Between Two Foreigners"

12 December 2018 | Fun, News and analysis, Top Story



What just happened? Did Russian state media decide to drop disinformation and replace it with

Latest news and analysis

"You Always Place Me Between Two Foreigners"
12/12/2018

Figure of the Week: 9
11/12/2018

Denigrating Ukraine With Disinformation
10/12/2018

Russian Independent TV vs. Kremlin TV: 3-0
05/12/2018

Figure of the Week: 12
04/12/2018

В ПРИНЯТОЙ ЕВРОПАЛАМЕНТОМ РЕЗОЛЮЦИИ 12.12.2018

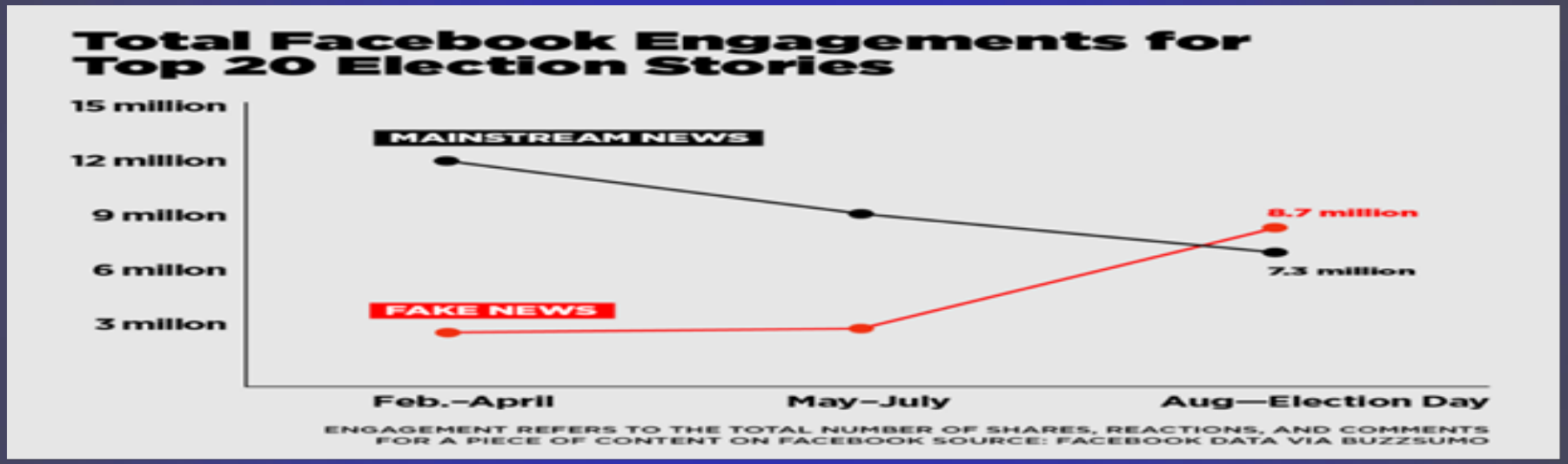
приоритетом ЕС признано противостояние киберугрозам из РФ

«Европейский союз должен быть более устойчив к внешнему вмешательству, особенно учитывая выборы в Европарламент 23-26 мая 2019 года. Евросоюз должен быть устойчивее перед угрозой террористических атак, <...> а также перед нелегальной миграцией, пропагандой, онлайн- и офлайн-кампаниями по дезинформации, российскими попытками осуществить кибератаки и другими гибридными угрозами, которые требуют быстрого и скоординированного ответа»

https://www.rbc.ru/politics/12/12/2018/5c115fb09a794727b2410bfe?from=newsfeed

С.В.Лавров (Мюнхен, 2017)

«… преодолеть период «post-truth», отбросить навязываемые международному сообществу истеричные информационные войны и перейти к честной работе, не отвлекаясь на ложь и вымыслы. Пусть это будет эпоха «post-fake».



Однако скандал с разоблачением «Cambridge Analytica» из-за участия в 200 зарубежных спецмероприятиях показали, что Запад (Англия) усиливает манипулирование общественным мнением многих стран, в т.ч. в ходе выборов,

При этом никаких санкций против Великобритании!!

Хакеры Anonymous выложили новые документы британского проекта Integrity Initiative

integrity initiative
Defending Democracy Against Disinformation

Цель проекта - противодействие пропаганде и гибридной войне РФ. За благородными намерениями Британия создала информационную секретную службу в Европе, США и Канаде из представителей политического, военного, научного и журналистского сообщества.

В файлах есть «поддельное доказательство» вмешательства РФ в референдум в Каталонии. Anonymous потребовали провести расследование. Первые документы проекта «для противостояния России» были обнародованы в ноябре с.г. и в ответ на ноту посольства РФ были признаны Форин Офисом .

ОПРОВЕРЖЕНИЯ ЗАРУБЕЖНЫХ ФЕЙКОВ НА САЙТЕ МИД РФ

16.11.18 13:16

О раскручивании датскими СМИ темы якобы тайных перевозок оружия российскими судами

14.11.18 13:47

Об инсинуациях черногорских СМИ на тему якобы вмешательства российских дипломатов в местные политические процессы

22.10.18 14:26

О статье в британском таблоиде The Sun на тему якобы российского вмешательства в Ливии

21.09.18 19:36

О публикации «Раскрыт секретный план побега Джулиана Ассанжа из Великобритании при помощи России» в газете «Гардиан»

12.09.18 15:27

О публикации американского телеканала NBC

7.09.18 13:29

О публикации кувейтской газеты «Аль-Анба»

РЕЗЮМЕ:

- Инфогенные угрозы трансформировались из технической сферы в один из ключевых факторов геополитического противоборства;
- В силу этого представляется правильным поддержать российскую резолюцию ГА ООН по МИБ, в т.ч. путем её всемерной медиатизации

- альтернатива иррациональна:

МГИМО УНИВЕРСИТЕТ

НАМИБ

НИИГлоБ
НАЦИОНАЛЬНЫЙ ИНСТИТУТ ИССЛЕДОВАНИЙ ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ
NATIONAL INSTITUTE FOR RESEARCH OF GLOBAL SECURITY

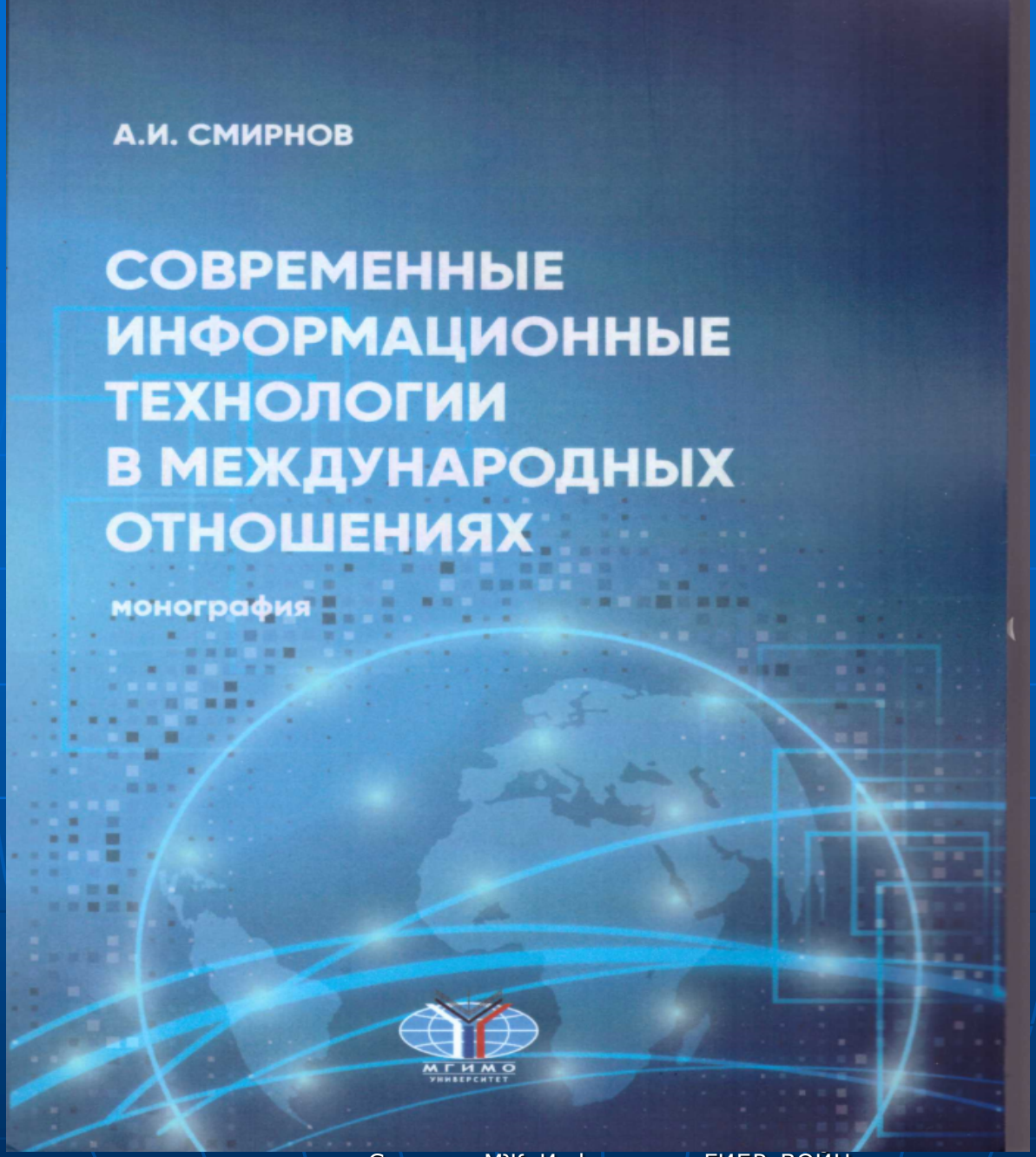
Thanks for attention!

ANATOLY I. SMIRNOV

Director General of the National Association of International Information Security, President of NIIGLOB,

Doctor of Historical Sciences, Professor, Chief Scientific Officer of MGIMO of the MFA of the Russian Federation

http://namib.online/



Смирнов_МЖ_Инфогенные_ГИБР_ВОЙН

В ДЕНЬ ДИПЛОМАТИЧЕСКОГО РАБОТНИКА 2008 г.

«Парижский призыв к доверию и безопасности в киберпространстве»

- На Форуме по управлению Интернетом (12-14.11.2018) Макрон анонсировал инициативу в области обеспечения МИБ
- К документу присоединились 51 государство, 50 международных региональных организаций, 170 компаний и корпораций.
- Основной посыл документа – обеспечить мир и безопасность в глобальной инфосреде – соответствует духу подходов РФ к обеспечению МИБ одобренных Первым и Третьим комитетами 73-сессии ГА ООН.
- В декларации присутствует ряд дискуссионных положений. Так, Конвенция Совета Европы по киберпреступности 2001 г. как «важнейший» международно-правовой инструмент, хотя эффектность её мер спорна.
- Мультистейкхолдеровый подход к цифровой среде уравнивает в правах государства и НГО размывает зону ответственности акторов.
- Ряд положений признают допустимость военнного исп.ИКТ-средь однако без уточнения мезанизма.
- Подтвержден тезис о применении к ИКТ-среде международного права, но остается неопределенным его механизм исппользован

Глобальная безопасность: госдолг США $21,82трлн. (на 4.12.18) (http://www.usdebtclock.org/) - 108% к ВВП **не покрыть без крупной войны (гибридной?)** (общий долг:1 квадрл). 4 киберстратегии 2018 г наряду с резким ростом расходов на оборону, спецмероприятия, в т.ч по сдерживанию, подрыву и смену режима в РФ, Иране, КНР…

П У Т Е М М Е Д И А Т И З А Ц И И П Р О Б Л Е М!!!)))

Международный стандарт ISO/IEC 27032:2012 Information technology Guidelines for cybersecurity. Соотношение Информационной безопасности и Кибербезопасности

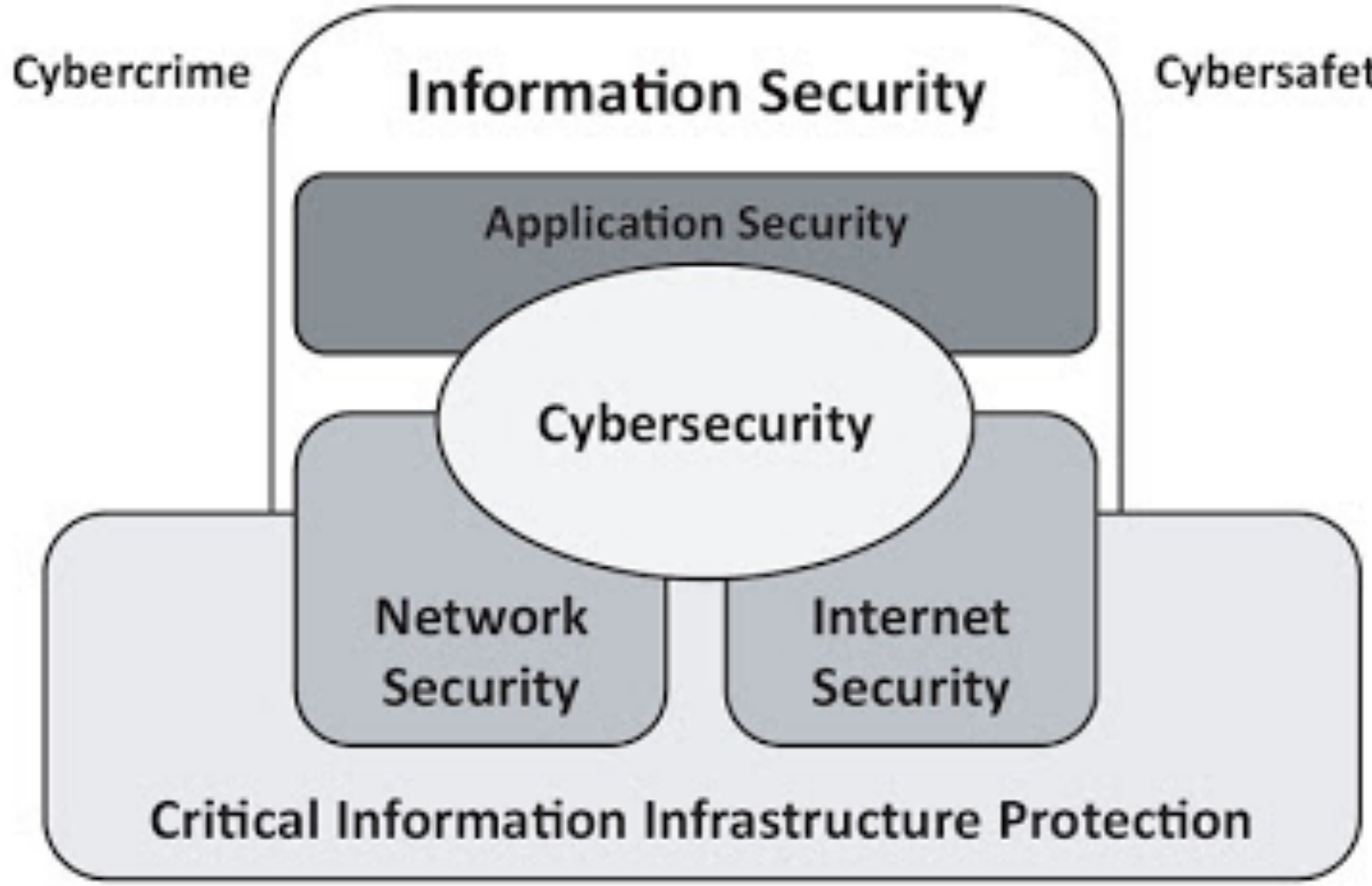


Figure 1 — Relationship between Cybersecurity and other security domains