Република България

Съвет по сигурност, Министерски съвет

Национална стратегия за кибер сигурност „Кибер устойчива България 2020” (2016)

www.cyberBG.eu

Националната стратегия по киберсигурността и е-управлението

Кръгла маса „Национални приоритети в развитието на е-управлението“
21 Април 2017 г., София

Dr. George Sharkov

National Cybersecurity Coordinator (Security Council), Adviser PM Office

g.sharkov@government.bg

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Lif

Tory Burch's New Store Is Her Clubhouse

When You Really Need to Attend That Conference

ADVENTURE & TRAVEL
The Ski Vacation That Should Be on Your ...

YOU ARE READING A PREVIEW OF A PAID ARTICLE. SUBSCRIBE NOW TO GET M

ESSAY

Why Software Is Eating The World

By MARC ANDREESSEN
August 20, 2011

This week, Hewlett-Packard (where I am on the board) announced that it is exploring jettisoning its struggling PC business in favor of investing more heavily in software, where it sees better potential for growth. Meanwhile, Google plans to buy up the cellphone handset maker Motorola Mobility. Both moves surprised the tech world. But both moves are also in line with a trend I've observed, one that makes me optimistic about the future growth of the American and world economies, despite the recent turmoil in the stock market.

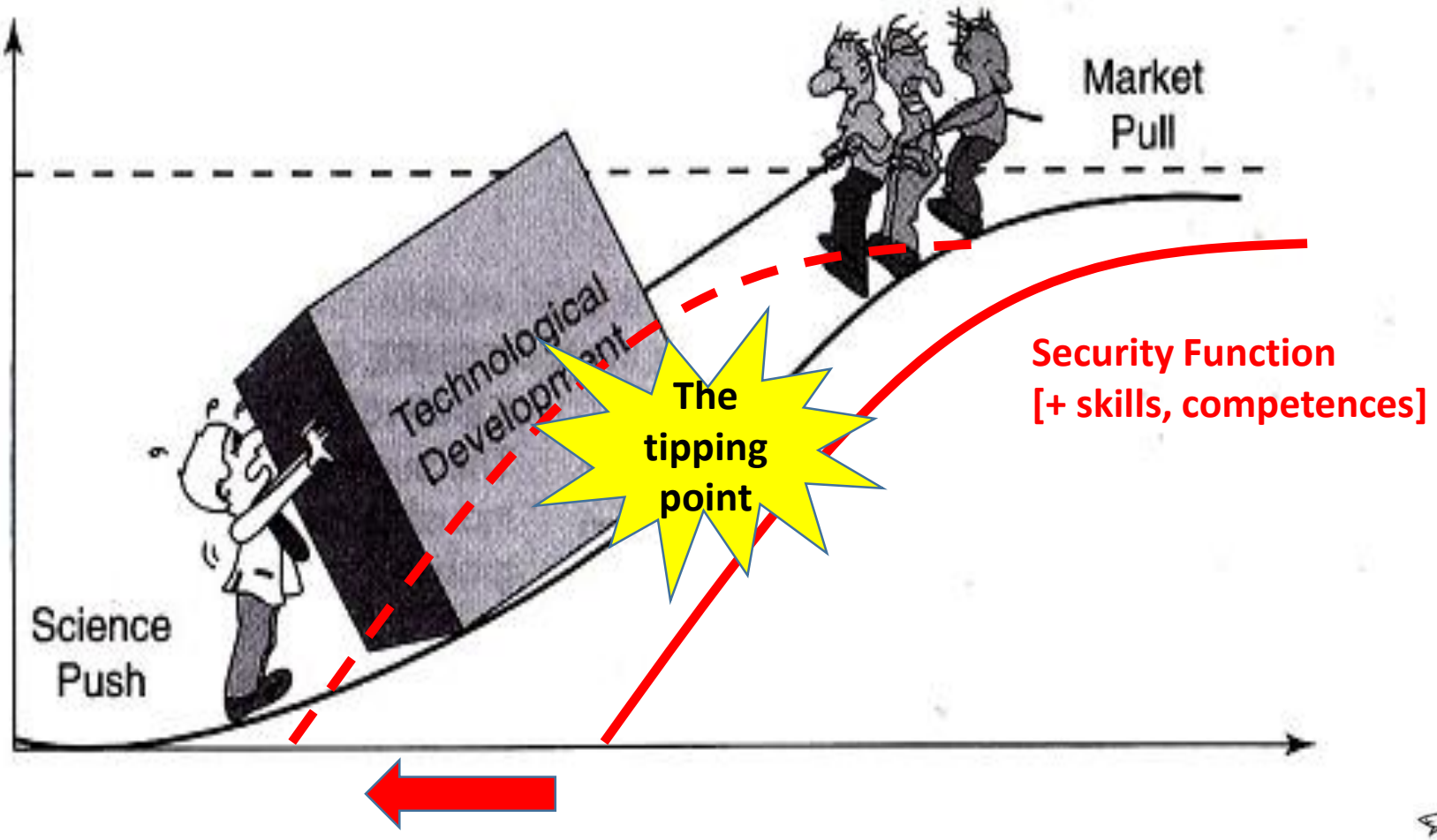
In an interview with WSJ's Kevin Delaney, Groupon and LinkedIn investor Marc

In short, software is eating the world.

More than 10 years after the peak of the 1990s dot-com bubble, a dozen or so new Internet companies like Facebook and Twitter are sparking controversy in Silicon Valley, due to their rapidly growing private market valuations, and even the occasional successful

Digital dependency:
If Software is eating the world,
are we safe ?

Ready for the Digital Dependency?



е-Управление

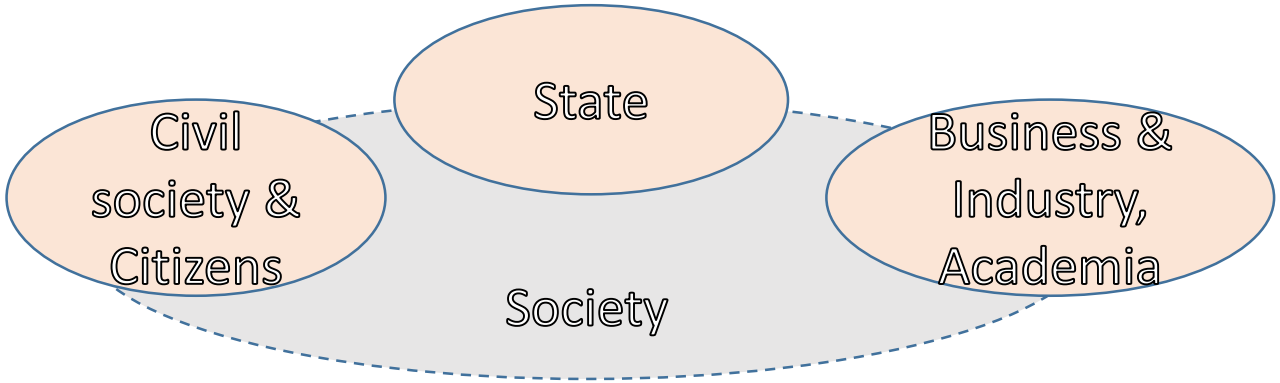
≠

е-Услуги

Сигурна, надеждна и устойчива дигитална екосистема (= кибер пространство)

National Cyber Security & Resilience: A multi stakeholder engagement

www.cyberBG.eu



National strategies
USA, UK,
Netherland, Finland…

Подход и принципи

- **Ангажиране на всички заинтересовани страни**

държавни, бизнес и индустрия, академична и изследователска общност, граждани и неправителствени организации

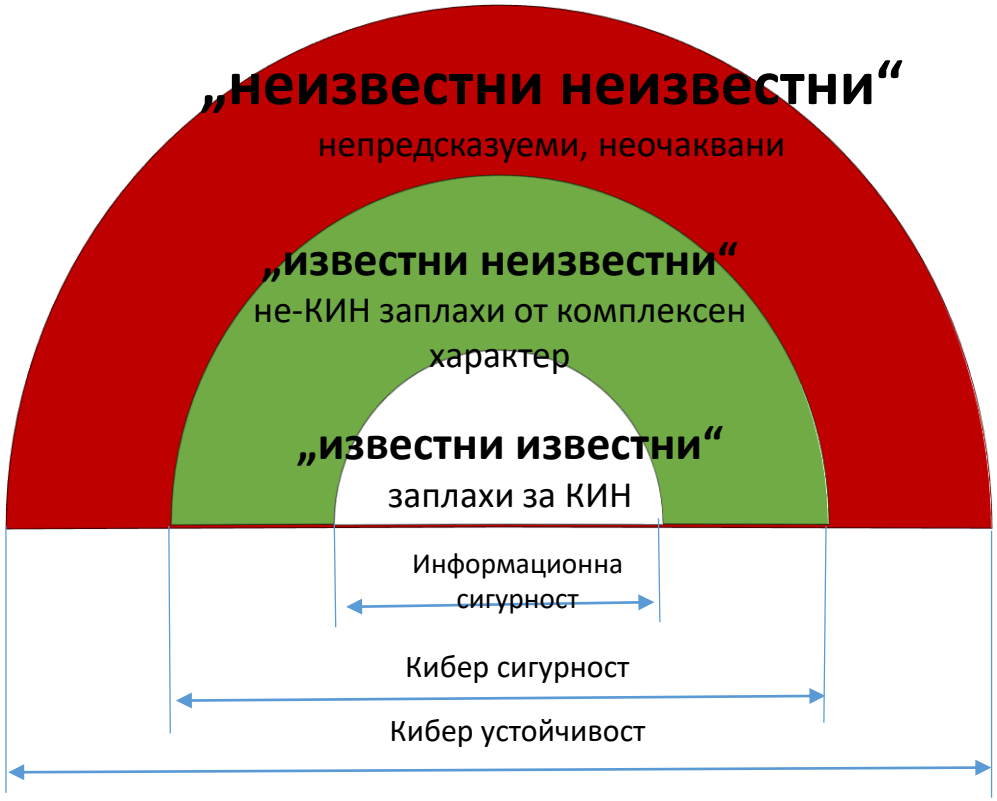
- **Стратегията следва методиките и зададените рамки от ЕС, НАТО и световните организации, международни стандарти;**
- **Визия за развитие на България до 2020 г на три етапа**

  От: Базова кибер сигурност и „кибер хигиена“ - преодоляване на основни уязвимости в критични за държавата и обществото КИС и изоставането в ЕС и НАТО

  До: Зряло състояние на кибер устойчивост (включително и срещу непознати атаки) и водеща и иновативна роля в няколко съвременни направления;

- Предложеният модел е съгласуван и подкрепен от водещи международни специалисти в областта на кибер сигурността и кибер отбраната, както и с партньорските организации от НАТО, ЕС и от държавите с най-развита система за кибер защита (САЩ, Нидерландия, Великобритания, Германия) - като основно негово предимство е признатата му функционална устойчивост на базата на мрежовия подход и разпределени ресурси, както и възможно най-бързото му реализиране и икономичност от гледна точка на финансови ресурси.

Готови за „неизвестното“ ?



Фигура 1: Контекст на кибер устойчивостта.
КИН: Конфиденциалност, Интегритет, Наличност

Визия: Кибер устойчива България 2020

Initiation
2016 -2017

Growth
2018 - 2019

Maturity & Leadership
2020 +

Обща структура

1 България в съвременното кибер пространство

- 1.1 Дигитална зависимост, заплахи и кибер сигурност
- 1.2 Предизвикателства, рискове и възможности

2 Визия „Кибер устойчива България 2020“

- 2.1 Стратегически цели
- 2.2 Фази
- 2.3 Подход - общо усилие, ориентирано към резултати
- 2.4 България – надежден международен партньор за сигурност и устойчивост на кибер пространството

3 Принципи

4 Области на действие, цели и мерки

5 Реализиране, контрол и актуализация

Приложение 1: SWOT анализ за състоянието и предизвикателствата пред България в кибер пространството

Приложение 2: Фази (и пътна карта) за реализиране на стратегията

Фаза 1: Инициране и постигане на базов капацитет за кибер сигурност (2016-2017г.)

Фаза 2: Развитие – от капацитет към способности (2018-2019г.)

Фаза 3: Зряло и кибер устойчиво общество (2020 + г)

Приложение 3: Речник

Области на действие, цели и мерки

4.1 Установяване и развитие на националната система за кибер сигурност и устойчивост

4.2 Мрежовата и информационна сигурност – фундамент на кибер устойчивостта

4.3 Подобряване на защитата и устойчивостта на дигитално зависимите критични инфраструктури

4.4 Подобряване на взаимодействието между държава, бизнес и общество

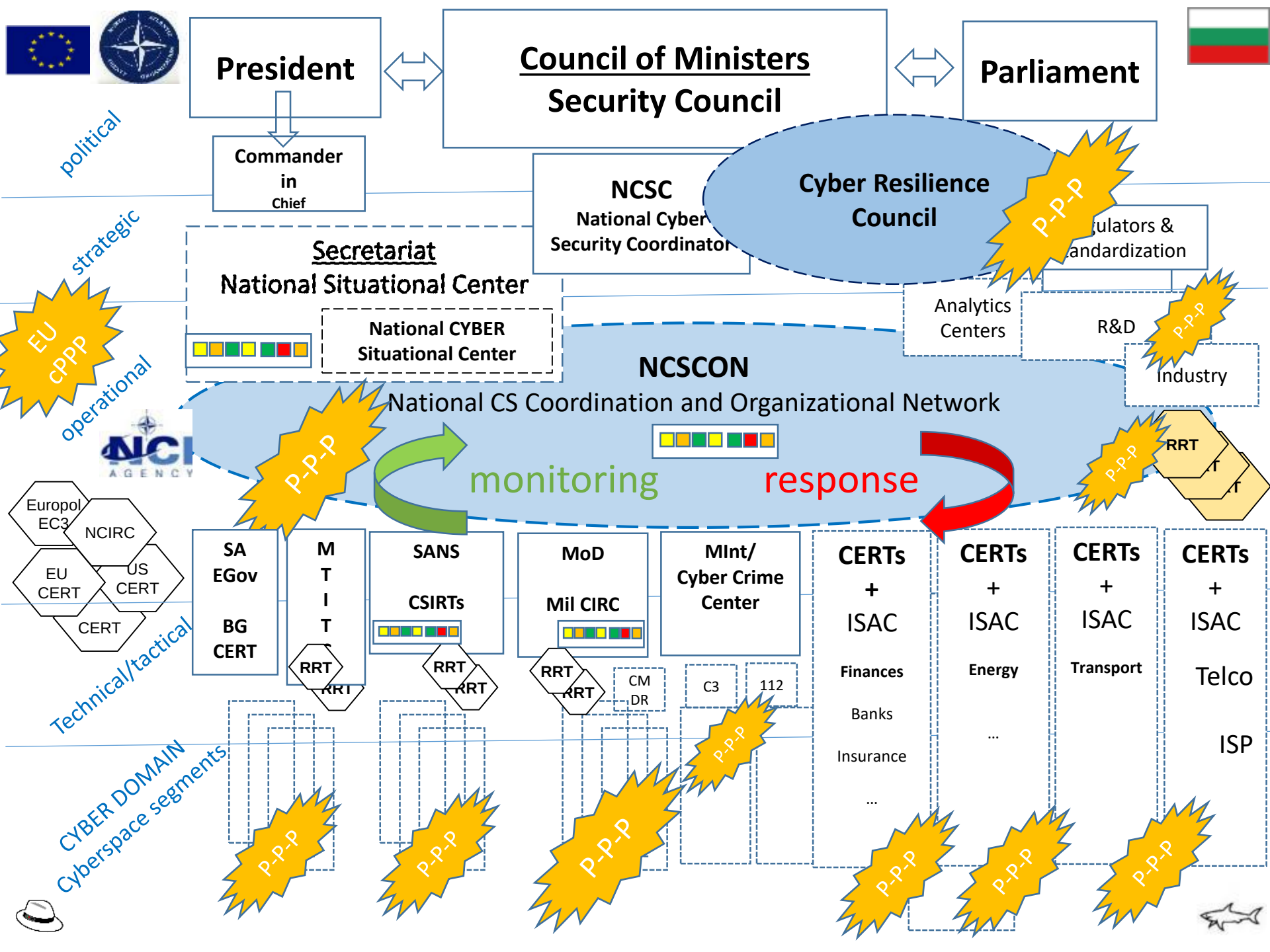
4.5 Развитие и подобряване на регулаторната рамка

4.6 Засилване на противодействието на кибер престъпността

4.7 Кибер отбрана и защита на националната сигурност

4.8 Повишаване на осведомеността, знанията и компетентностите и развитие на стимулираща среда за изследвания и иновации в областта на кибер сигурността

4.9 Международно взаимодействие


President
Council of Ministers
Security Council
Parliament
political
Commander in Chief
NCSC
National Cyber Security Coordinator
Cyber Resilience Council
P-P-P
strategic
Secretariat
National Situational Center
National CYBER Situational Center
Analytics Centers
R&D
Industry
EU cPPP
operational
NCSCON
National CS Coordination and Organizational Network
monitoring
response
RRT
Europol EC3
NCIRC
EU CERT
US CERT
CERT
Technical/tactical
SA EGov
BG CERT
MITI
SANS
CSIRTs
MoD
Mil CIRC
MInt/ Cyber Crime Center
CERTs + ISAC
Finances
Banks
Insurance
Energy
Transport
Telco
ISP
CM DR
C3
112
CYBER DOMAIN
Cyberspace segments

Области на действие, цели и мерки

4.1 **Установяване и развитие на националната система за кибер сигурност и устойчивост**

- 4.1.1 Национален Съвет по кибер устойчивост (СКУ)
- 4.1.2 Създаване на мрежа и структура за координация на оперативно ниво (НКОМКС)
- 4.1.3 Национален координатор по кибер сигурността (НККС)
- 4.1.4 Установяване на Национална система за управление при кибер кризи
- 4.1.5 **Повишаване на ролята и отговорностите на държавните органи и структури, и на всички заинтересовани организации и лица**

4.2 **Мрежовата и информационна сигурност – фундамент на кибер устойчивостта**

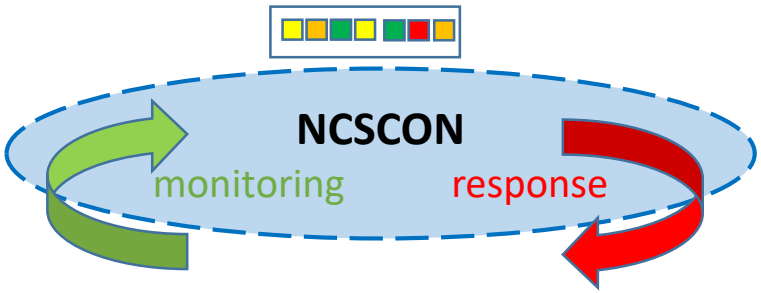
- **4.2.1 Постигане на високо общо ниво на мрежова и информационна сигурност**
- **4.2.2 Повишаване на сигурността на системите за електронно управление, комуникационните и информационни системи на държавните институции и администрация**
- **4.2.3 Ангажиране на частния сектор в подобряване на МИС**

4.3 **Подобряване на защитата и устойчивостта на дигитално зависимите критични инфраструктури**

- 4.3.1 Подобряване на взаимодействието между държавата и операторите на критични инфраструктури
- 4.3.2 Развитие и **модернизация** на системите за управление и защита на критични инфраструктури
- 4.3.3 Своевременно **разширяване на обхвата на действията за защита на новите области на кибер пространство**

e-Управление = система-от-системи

(национална) Система за киберсигурност = система-от-системи



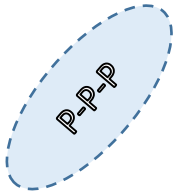
- Непрекъснат мониторинг на национална **кибер-картина (ситуационна осведоменост)** с проекция на кибер-състоянието във всички сегменти на управление и функциониране на държавата, икономиката и обществото;
- Оперативна оценка на **степента на заплаха** и осигуряване на **координиран отговор и превантивни действия**;
- Координирана защита и предотвратяване на **кибер кризи**, заплахи от **хибриден характер** (кибер или хибридни войни)
- Осигуряване на устойчивост на КИС/ИКТ системите за справяне с **кризисни и бедствени ситуации от различен характер**;
- **Разпределени отговорности, автономност, обединяване и споделяне на ресурсите**, включително и от неправителствени структури;

4.4 Подобряване на взаимодействието и споделянето на информация между държава, бизнес и общество

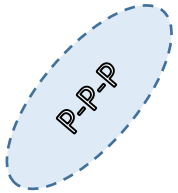
4.4.1 Установяване на ефективни механизми за споделяне на информация и ангажираност на всички заинтересовани лица

ISAC (Information Sharing and Analysis Centers/Organizations)

4.4.2 Развитие на индустриален технологичен капацитет и споделени способности

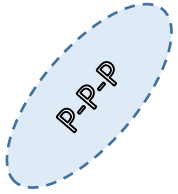


Създаване на ефективен механизъм за споделяне на ресурси, капацитет и способности между частния, публичен и академичен сектор на базата на взаимен интерес и обща визия и стратегия за развитие – отчитане на изпреварващата роля в технологично отношение на бизнеса и необходимостта за създаване на съответна среда за развитие и подпомагане от държавата и програмите за интелигентен растеж и развитие



4.4.3 Фокус върху малкия и среден бизнес

4.4.4 Установяване на обща комуникационна стратегия за информираност относно кибер въздействия и противодействия



4.4.5 Сигурна, свободна и надеждна интернет среда

NIS Directive (EU, EP)

ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза

EC Directive 2016/1148/EU – Network and Information Security

- Obligations for member states: adoption of a national strategy for NIS & identification of operators of essential services
- Obligations for operators of essential services and for digital service providers
- Implementation deadline: 9 May 2018

EU General Data Protection Regulation (GDPR)

May 2018

The Public-Private Partnership (PPP) on cybersecurity

To strengthen EU's cybersecurity industry, the European Commission will establish a contractual Public-Private Partnership (PPP) on cybersecurity, as envisaged in the Digital Single Market Strategy.

The aim of the PPP is to stimulate the European cybersecurity industry by:

- bringing together industrial and public resources to improve Europe's industrial policy on cybersecurity, focusing on innovation and following a jointly-agreed strategic research and innovation roadmap
- helping build trust among Member States and industrial actors by fostering bottom-up cooperation on research and innovation
- helping stimulate cybersecurity industry by aligning the demand and supply for cybersecurity products and services, and allowing the industry to efficiently elicit future requirements from end-users
- leveraging funding from Horizon2020 and maximizing the impact of available industry funds through better coordination and better focus on a few technical priorities
- providing visibility to European R&I excellence in cyber security and digital privacy.

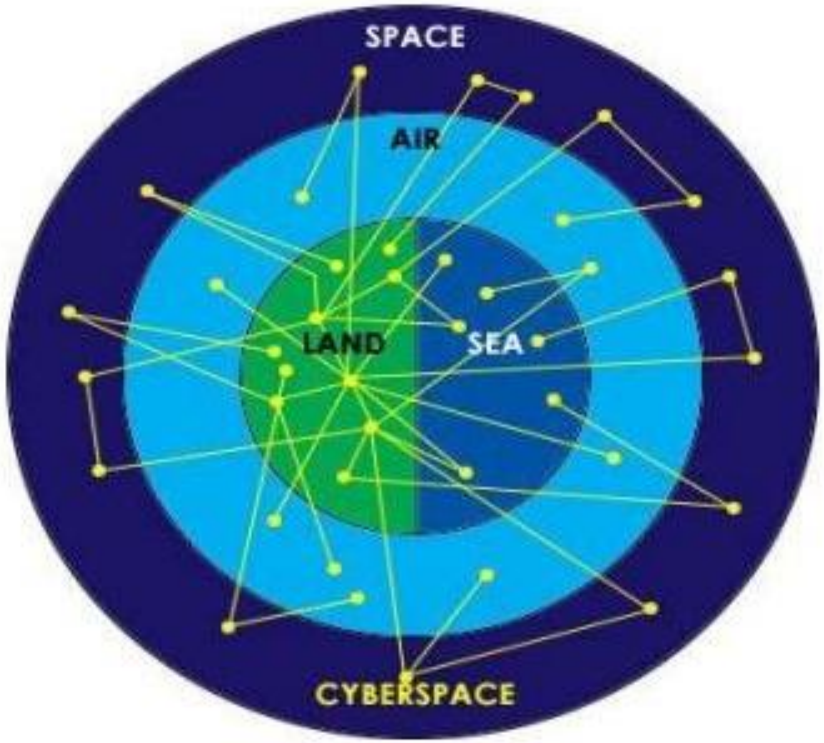
The PPP will build on the Strategic Research Agenda (SRA) in the area of secure information and communication technologies (ICT), developed by the NIS Platform and published in September 2015.

NATO
OTAN

Warsaw
Varsovie

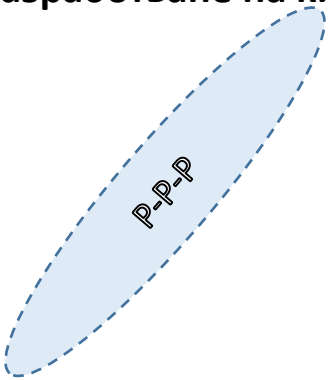
8-9 VII 2016

Summit | Sommet



4.8 Повишаване на осведомеността, знанията и компетентностите и развитие на стимулираща среда за изследвания и иновации в областта на кибер сигурността

Цел 1: висока **осведоменост на всички целеви групи и заинтересовани страни** и **еднакво разбиране и оценка за заплахите** във връзка с нарастващата всеобща дигитална зависимост и необходимостта от адекватни мерки на всички нива за постигане на информационна и кибер сигурност, развитие на обща кибер култура.
Цел 2: Включване на аспекти на киберсигурността и придобиване на адекватни компетентности във **всички нива и форми на образование и обучение** и създаване на специалисти, подготвени кадри и лидери за сигурно и устойчиво развитие на дигиталната икономика, общество и държавно управление в цифровата ера.
Цел 3: Създаване на благоприятна среда за развитие на изследванията и иновативни приложения и превръщането на България във **водещ център за разработване на кибер устойчиви системи на бъдещето**.



“If you are not part of the solution, you must be part of the problem”

Attributed to: Eldridge Clever (1969); African proverb, others

ПЛАН ЗА ДЕЙСТВИЕ: С ВАШЕТО АКТИВНО УЧАСТИЕ!

www.CyberBG.eu

Dr. George Sharkov

National Cybersecurity Coordinator (Security Council BG), Adviser MoD

g.sharkov@mod.bg ; g.sharkov@government.bg

ESI CEE Director, CyResLab gesha@esicenter.bg