Strategic and Political Dimensions of Cyber Security - Lessons from Bulgaria"

Valeri R. RATCHEV

Strategic context

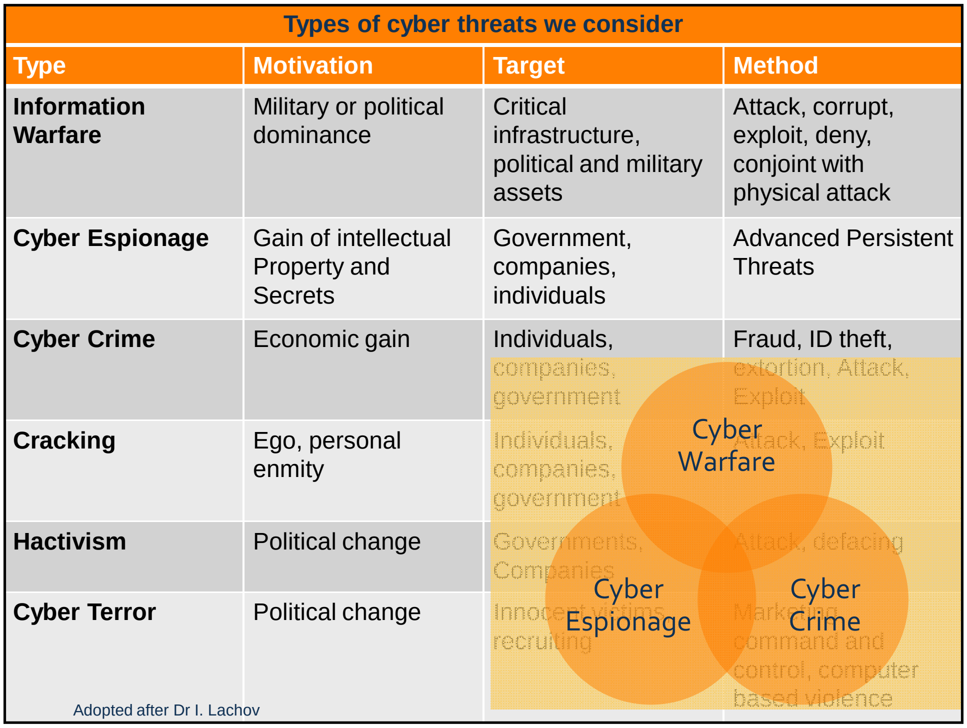
+ **BULGARIA'S VARIABLES IN CYBSEC CONTEXT:**
  - **Geopolitically** vulnerable – cyber conflict mirrors fighting on ground
  - Extremely "**open**" as economy, access, traffic, communications
  - Best in **services and tourism** that depend on infonetworks;
  - With **dominant private sector** but mostly **internationally owned**;
  - With internationally deployed **criminal sector**;
  - **Active at the international scene**;
  - With **still developing** IT sector; critical delays are in the e-government and inclusiveness of rare country areas;

The use ICT is a source of national competitive advantage!

Strategic context

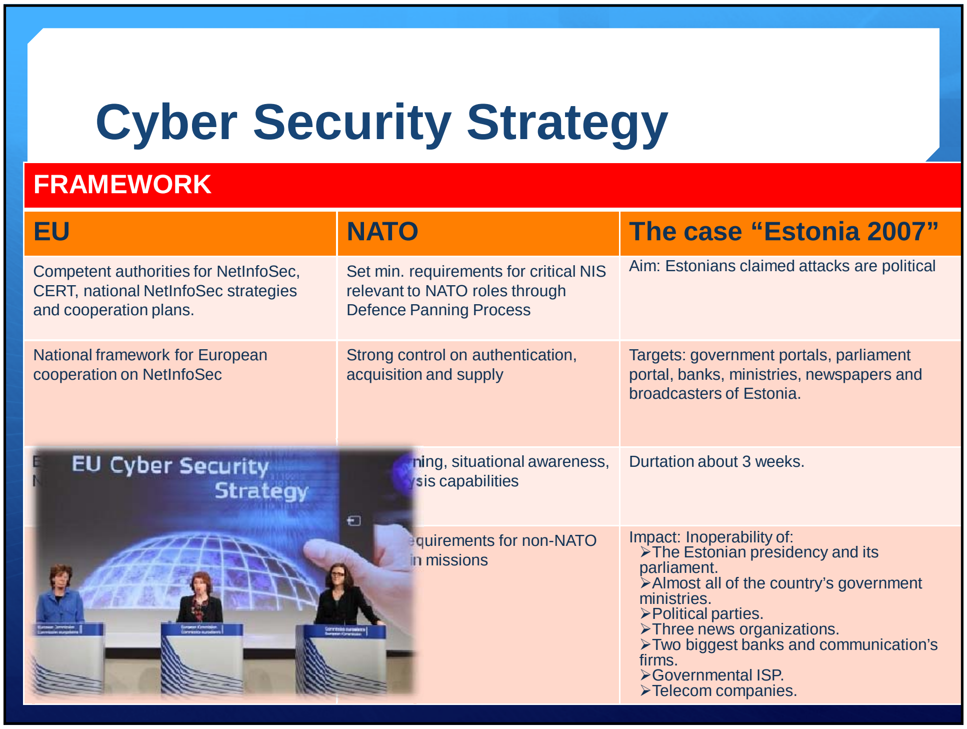
+ **VULNERABILITIES:**
  - **The Bulgarian state looses some control** over the cyber domain and conflict
  - **Old** international norms and rules does not work properly; **national are still in discussion**
  - EU and NATO frame the strategic approach,

    but **initiative and responsibility remains national**
  - Two strategic perspectives – **development** and **security** within the cyber domain
  - In BG cyber space: **variety of actors with different motivation; "unknown** unknowns"



Types of cyber threats we consider			
Type	**Motivation**	**Target**	**Method**
Information Warfare	Military or political dominance	Critical infrastructure, political and military assets	Attack, corrupt, exploit, deny, conjoint with physical attack
Cyber Espionage	Gain of intellectual Property and Secrets	Government, companies, individuals	Advanced Persistent Threats
Cyber Crime	Economic gain	Individuals, companies, government	Fraud, ID theft, extortion, Attack, Exploit
Cracking	Ego, personal enmity	Individuals, companies, government	Attack, Exploit
Hactivism	Political change	Governments, Companies	Attack, defacing
Cyber Terror	Political change	Innocent victims, recruiting	Marketing, command and control, computer based violence

Adopted after Dr I. Lachov

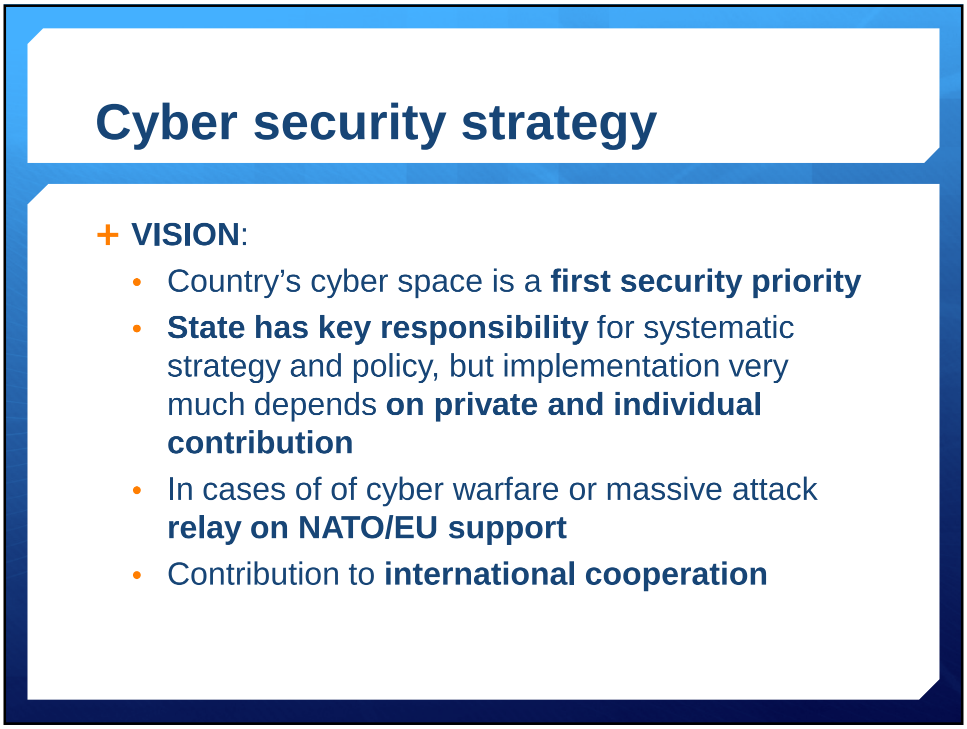


Cyber Security Strategy

FRAMEWORK

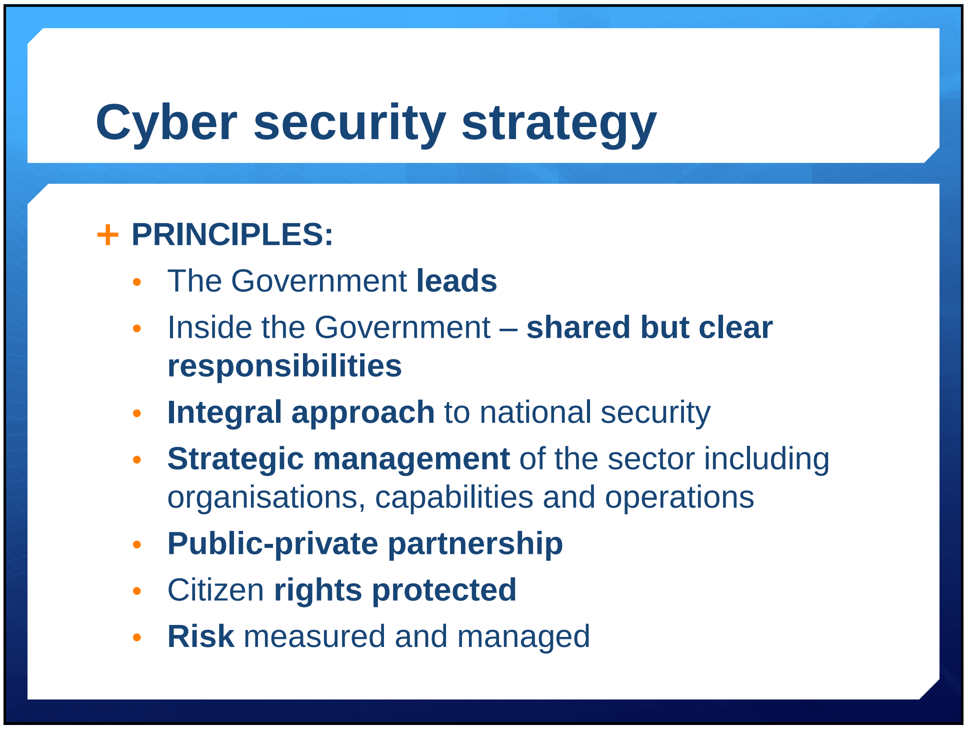
EU	NATO	The case “Estonia 2007”
Competent authorities for NetInfoSec, CERT, national NetInfoSec strategies and cooperation plans.	Set min. requirements for critical NIS relevant to NATO roles through Defence Panning Process	Aim: Estonians claimed attacks are political
National framework for European cooperation on NetInfoSec	Strong control on authentication, acquisition and supply	Targets: government portals, parliament portal, banks, ministries, newspapers and broadcasters of Estonia.
E N	ning, situational awareness, ysis capabilities	Durtation about 3 weeks.
	equirements for non-NATO in missions	Impact: Inoperability of: ➢The Estonian presidency and its parliament. ➢Almost all of the country’s government ministries. ➢Political parties. ➢Three news organizations. ➢Two biggest banks and communication’s firms. ➢Governmental ISP. ➢Telecom companies.

EU Cyber Security
Strategy



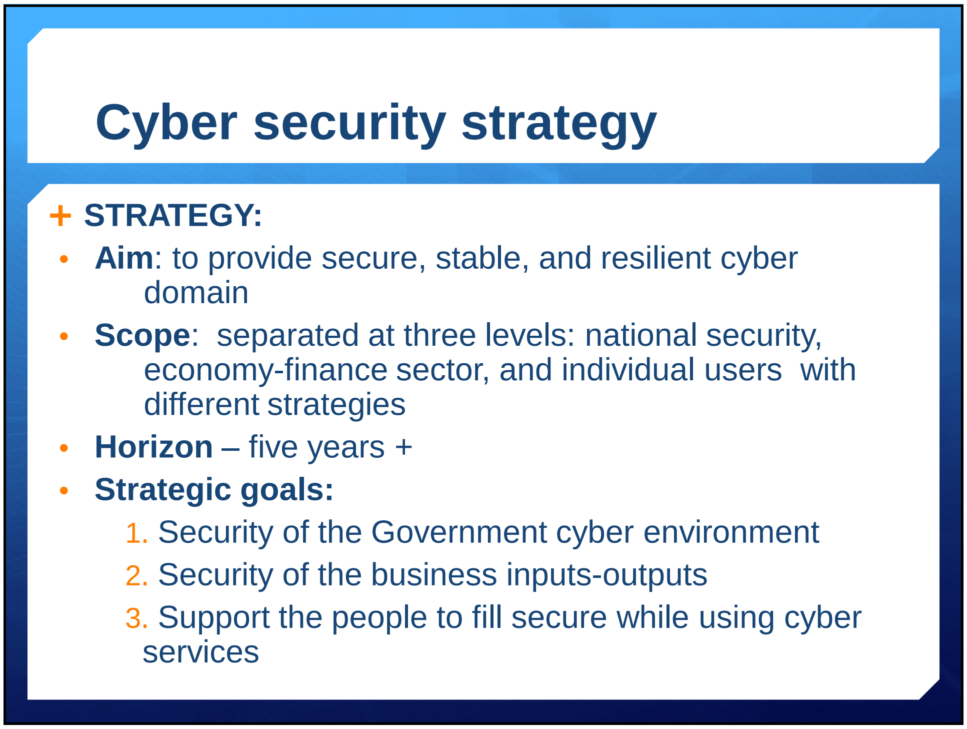
Cyber security strategy

+ **VISION**:
  - Country’s cyber space is a **first security priority**
  - **State has key responsibility** for systematic strategy and policy, but implementation very much depends **on private and individual contribution**
  - In cases of of cyber warfare or massive attack **relay on NATO/EU support**
  - Contribution to **international cooperation**



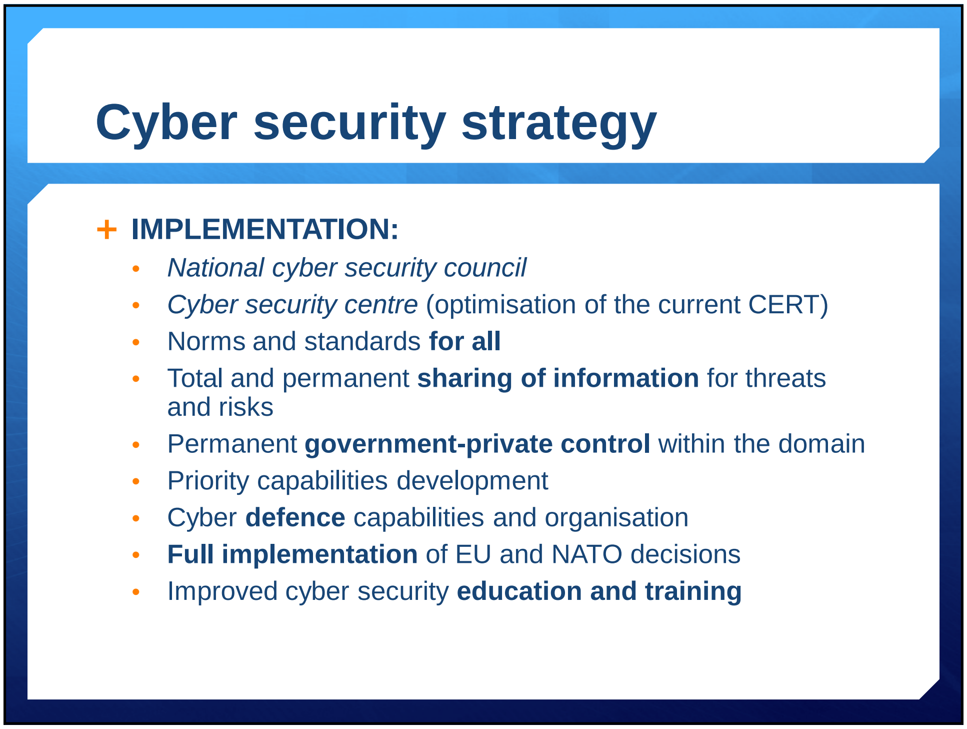
Cyber security strategy

+ **PRINCIPLES:**
  - The Government **leads**
  - Inside the Government – **shared but clear responsibilities**
  - **Integral approach** to national security
  - **Strategic management** of the sector including organisations, capabilities and operations
  - **Public-private partnership**
  - Citizen **rights protected**
  - **Risk** measured and managed



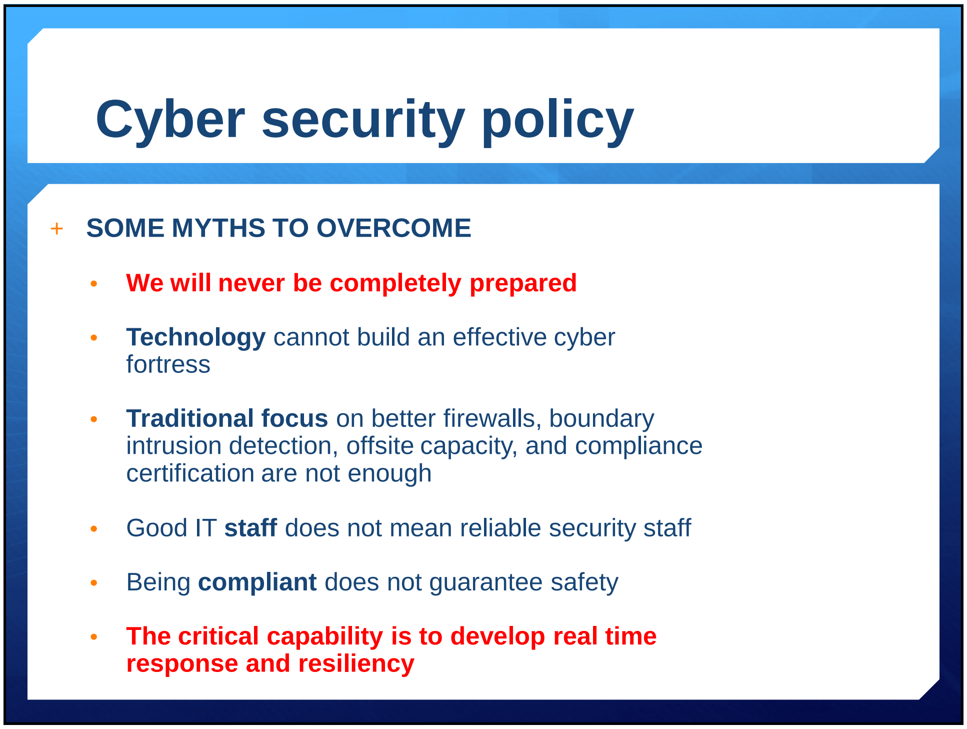
Cyber security strategy

+ **STRATEGY:**
- **Aim**: to provide secure, stable, and resilient cyber domain
- **Scope**: separated at three levels: national security, economy-finance sector, and individual users with different strategies
- **Horizon** – five years +
- **Strategic goals:**
  1. Security of the Government cyber environment
  2. Security of the business inputs-outputs
  3. Support the people to fill secure while using cyber services



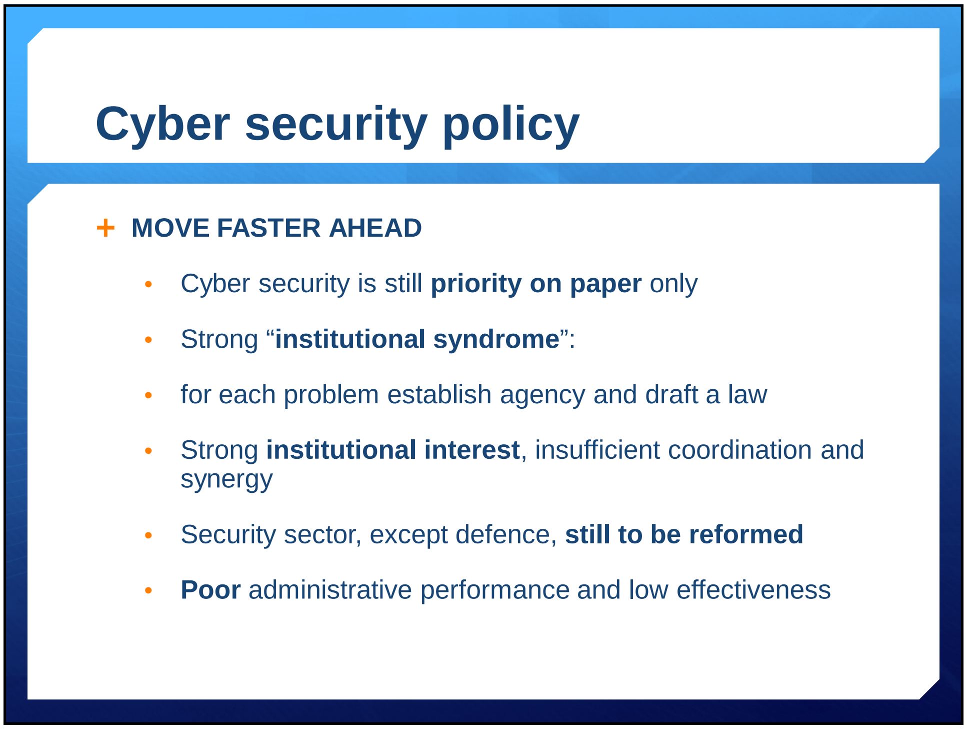
Cyber security strategy

+ IMPLEMENTATION:
  - *National cyber security council*
  - *Cyber security centre* (optimisation of the current CERT)
  - Norms and standards **for all**
  - Total and permanent **sharing of information** for threats and risks
  - Permanent **government-private control** within the domain
  - Priority capabilities development
  - Cyber **defence** capabilities and organisation
  - **Full implementation** of EU and NATO decisions
  - Improved cyber security **education and training**



Cyber security policy

+ SOME MYTHS TO OVERCOME
  - **We will never be completely prepared**
  - **Technology** cannot build an effective cyber fortress
  - **Traditional focus** on better firewalls, boundary intrusion detection, offsite capacity, and compliance certification are not enough
  - Good IT **staff** does not mean reliable security staff
  - Being **compliant** does not guarantee safety
  - **The critical capability is to develop real time response and resiliency**



Cyber security policy

+ **MOVE FASTER AHEAD**
  - Cyber security is still **priority on paper** only
  - Strong “**institutional syndrome**”:
  - for each problem establish agency and draft a law
  - Strong **institutional interest**, insufficient coordination and synergy
  - Security sector, except defence, **still to be reformed**
  - **Poor** administrative performance and low effectiveness