From Cybersecurity to Collaborative Resiliency

George Sharkov
National Cybersecurity Coordinator
Ministry of Defense
6 Diakon Ignatii Str., Sofia, Bulgaria
+359 888 808485
g.sharkov@mod.bg

ABSTRACT
This paper presents the holistic approach to cyber resilience as a means of preparing for the "unknown unknowns". Principles of augmented cyber risks management and resilience management model at national level are presented, with elaboration on multi-stakeholder engagement and partnership for the implementation of national cyber resilience collaborative framework. The complementarity of governance, law, and business/industry initiatives is outlined, with examples of the collaborative resilience model for the Bulgarian national strategy and its multi-national engagements.

Keywords
Cybersecurity; business resilience; collaborative frameworks; systems of systems; public-private partnership; national cybersecurity strategy; unknown unknowns; cyberspace.

1. INTRODUCTION
Our modern societies rapidly evolve from "technological" through "information" and "knowledge-based" into conceptually new, "cyber society". Digital infrastructures have become the backbone, or a fundamental critical factor, for the management and normal functioning of all resources and systems of national importance, of present-day innovative economy, transparent governance, of modern and democratic civil society. The individuals and the community rely on trustworthy and reliable information in the online environment but they also expect somehow trusted data sources, confidence and protection of personal data and their digital e-self, along with adequate respect for human rights and liberties in cyberspace. After certain hesitation, states and politicians literally jump in Internet as a channel for the delivery of information and services to citizens and businesses and for fast, almost instantaneous, transparent and extensive contact with the community. Through e-governance states irreversibly migrate activities and services into digital only form.

Cyberspace offers virtually infinite opportunities for development to the society and businesses but the augmenting and irreversible digital dependency of the main functions and activities of the society in generates new compelling risks and threats. The "knowledge economy" not only depends on, but also introduces, with a long-term perspective, new aspects related to the intensive use of information systems, software management systems and effective processes based on digital infrastructures. Supply chains (or more general - value chains) operate and deliver on the basis of the established virtual digital channels via their information systems and through the internet. Thus, the business risks expand with some new "embedded" cyber risks of crucial importance, ignoring which would have catastrophic implications.

Various standards, models and guidelines address different aspects of cyber security, business and services continuity, risk management, disaster response and recovery, and since recently – the resilience of organizations. The enterprise focus on resiliency at the very high level is not only competitive advantage, but is vital for business sustainability and growth. The holistic approach requires stronger alignment and convergence of previously "siloed" activities and led to evolution and convergence of respective models and standards. Not surprisingly for the digital era we live in, the common ground for this convergence is the information, technology (ICT) and respective digitized business processes and ecosystems. One of the recent meta-models to manage as a whole operational risks and resiliency in the digitized world was introduced exactly from the "cradle" of the malware counter fighting – the CERT at Software Engineering Institute, Carnegie Mellon University [2]. Applying such a holistic approach, modern organizations are already building a new culture on the top of cyber security, and target a healthier status of "cyber resilience".

Today, the real challenge is how to move from those segmented and therefore not so efficient resilience-focused programs to a nation-wide, sponsored from the highest possible level program which involves and engages all major stakeholders. Most countries have introduced and implemented national strategies for cyber security, some are already upgrading them towards resiliency as a focus (like US, Netherland, Germany, UK, etc.). Higher level international policies are being developed at EU, NATO and regional levels. The UN International strategy for disaster risk reduction is also constructed around "disaster resilience" for risk assessment and mitigation. However, the key after agreeing on the goals (or "what to do") at a strategic level is how to "translate" them into effective measures, or "how to-s". What model for coordinated collective activities should be deployed to prepare and meet a cyber crisis at national or higher level, how to build joint capacity and capabilities, how to assess the "collective" risks, how to increase simultaneously the awareness and responsibilities of different actors and stakeholders from public and private sector and at the end transform and defend the cyber space as the fifth domain we live and rapidly develop in. This talk presents the Bulgarian approach to design such an ambitious roadmap in the recently adopted National cybersecurity strategy, focused on "Cyber Resilient Bulgaria" [1].

SafeConfig'16, October 24, 2016, Vienna, Austria.
ACM ISBN 978-1-4503-4566-8/16/10.
DOI: http://dx.doi.org/10.1145/2994475.2994484

2. FROM CYBERSECURITY TO CYBER RESILIENCY

Although the cyber security concept was born back in nineties mainly from the two complementary fields - information security and ICT security, the new "cyber domain" context required new understanding of cyber to address the resilience (of organizations and nations) in the digital age and digitized ecosystems.

To structure the basis for objectives and actions when developing the Bulgarian national cybersecurity strategy [1] we found helpful to utilize and align the following two well-known aspects:

- implementation of the fundamental "triad" from information security – Confidentiality, Integrity, Availability (the CIA triad);
- extent of our knowledge on risks and threats – adapting the "known unknowns" classification, coming from the financial world and structured in Black Swan theory of Nassim Taleb [11], but also used in other fields, including national security and cyber.

The references to CIA-triad and the scheme (Figure 1) were inspired by the use in Eurocontrol manual for national air-traffic management security oversight [5], where the scope of information security is outlined as dealing with "known CIA" risks, the cyber security - with "known non-CIA" and cyber resilience as "unknown, unpredictable, uncertain, unexpected".

From the risk management perspective, those associations naturally map to the second perspective and extrapolate to "known knowns", "known unknowns" and "unknown unknowns" respectively.

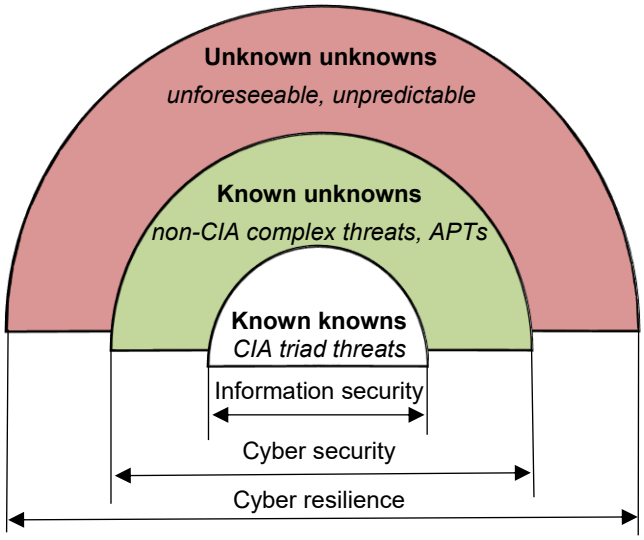

Figure 1. Cyber resilience context.

CIA: Confidentiality, Integrity, Availability

2.1 Prepare Organizations and Nations for "Unknown Unknowns"

The two aspects allow structuring of goals and measures at three levels and introduce them as a generalized "label" to express kind of maturity levels not only of the organizations, but also of the state, ecosystems, community and nation. Figure 1 illustrates these three nested levels – information security (which also embeds the ICT security), cyber security and cyber resilience. The threats, goals and measures are outlined as follows:

- *"known knowns"* – goals and measures to defend and protect information assets and communications infrastructure against known vulnerabilities, threats and breaches having to do with the fundamental information security concept – the CIA triad;
- *"known unknowns"* - dealing with combined threats related information security, ICT, communication and information systems (CIS), the variety of advanced persistent threats (APTs), attacks against the reputation of organizations and people, disinformation campaigns, and other unpredictable consequences of the mass migration of our activities to cyberspace, extremely large-scale CIA breaches (on a national, regional, and global scale), requiring enhanced and systematic application of the CIA concept to all assets of the digital ecosystem – information, technologies, people and facilities – an informal description of the cyber security;
- *"unknown unknowns"* – preparing for the unknown: unforeseeable, unexpected threats in cyberspace, dynamically changing risks and complex impacts with unpredictable implications demanding flexibility and resilience of the systems, organizations, and processes, as well as introduction of appropriate requirements when developing and deploying systems and processes - the essential characteristics of the status of cyber resilience.

Just to complete the four quadrant picture of uncertainties [11], we may name some of the recent APTs as *"unknown knowns"* (or our "blind spot"). For example, some "spying" stealth malwares which literally "annihilate" after time and we may eventually detect that "something was there, but we don't know what, how and for how long". Therefore, the damage is yet to come, with possible direct or maybe indirect impact, and others ("bad guys") will know it, use it or exploit the hidden vulnerability before us detecting it.

These "unknown unknowns" represent a type of uncertainties known as "ontological", or the events that have not been thought of, and therefore are not assessed or managed [9]. The rapidly increasing digital dependency of the economy and society and the agility (but also fragility) of the growing new fifth cyber domain with respective digitized ecosystems and their "unknown unknowns" made some market watchdogs predict that the next Black Swan event will come from cyber space [7].

2.2 Why Traditional Risk Management Is Not Enough

When evaluating and assessing the viability and resilient capabilities of complex, composite and adaptive systems such as the state with national governance and operational models, we need to go beyond the traditional risk-based approaches such as continuity of operations and disaster risk reduction processes. As described in [10], we should develop augmented risk approaches which incorporate methodologies grounded in socio-ecological system resilience principles for improving the abilities to assess and manage both known and unknown risks. New models, such as the illustrated in [10] Military Installation Resilience Assessment (MIRA) model, apply risk and resilience principles to evaluate whole systems, focusing on interconnections and their functionality in facilitating response and adaptation. These

principles and models are designed and applied successfully in complex organizational or enterprise systems, but the real challenge is to extend them to the higher, national level. At this complex level we should consider models like system-of-systems which handle interconnectivities and dependencies that are not steady and fixed upon time. In practice, those complex and interconnected systems (actually, the backbones of the entire associated ecosystems) could be disrupted and turned to unpredictable and nondeterministic behavior though unthinkable scenarios, thus generating or opening unidentifiable and also unpredictable vulnerabilities which by nature would be easier exploitable with potential cascade or catastrophic effect. Instead of over-engineering the risk management, the impact assessment should be based on the cost and consequences of failure of mission-related core services and operations of different organizations in the context of the entire ecosystem. Although various methods offer quantification of cyber-associated risks, still the major impact of control and information systems disruptions or failures, data and information breaches is largely difficult to quantify. Especially considering the prolonged hidden ("stealth") time, the APTs, sophistication, agility and self-adaptiveness of campaigns with unrecoverable and unimaginable factors of damage in virtual or physical space.

Elaborating an augmented risk management and resilience management model at national level will enable adaptation to the situation and therefore coordinated response to unknown threats associated with different disruptions - climate change and disasters of various nature, financial or budgetary crises, terrorism, cyber-attacks, and other unpredictable disruptions of "hybrid" type. However, it requires a higher level coordination framework among players that would have also unified understanding and sufficient implementation level of those extended risks and resilience management requirements for the entire ecosystem they operate in.

3. ORGANIZATIONAL AND NATIONAL RESILIENCE

The achievement of the strategic goal: cyber resilient society and state, requires a systematic and consistent policy and implementation effort in all areas comprising the status of cyber resilience in its entirety, which is characterized generally by the following:

- Effective protection and adequate comprehensive response to threats and destructive impacts in cyberspace, even to threats and impacts not previously known or of complex (hybrid) nature, and occurring in various spheres of the digital ecosystem;
- To the greatest extent possible, preserve and maintain continuity of function of vital activities and services, minimizing of harmful effects;
- Prompt and timely recovery to normal life (operations).

Or shortly, the "protect and sustain" functions as described in CERT-RMM for organizations [2], but applied to the entire national ecosystem.

3.1 Coordination at National Level: Multi-Stakeholder Approach

The collective (or national) resilience is a result of organizational resilience plus effective coordination mechanisms at the national level on all three layers – strategic, operational, and tactical/technical (last engaged in crisis situations via multisector rapid reaction teams, RRTs). It should be noted that the coordination at national level is mainly for information sharing and general operational situation analysis with alert levels attribution, and coordinated actions of organizations. Typically, it does not include or deploy specific dedicated technical resources, as they are usually located in the sector specific teams. However, there are two capabilities that are essential to develop at national level – procedures and mechanism to deploy cross-sectoral RRTs, and validation mechanism for collective capabilities (combined exercises on hybrid scenarios, including generic "red teams" with cross-sectoral profile).

The accomplishment of the objectives is based on the identification, inclusion and active involvement of all stakeholders, the multi-stakeholder approach. Following the example of advanced countries (such as USA, UK, Netherlands and other EU member states), it should be the initiative of the Government to establish the national cybersecurity system concept with a multi-stakeholder cooperation and engagement framework, which is also considered as a sign of mature governance of the state. The institutionalization of multi-stakeholder engagement is through various formats of public-private partnerships (PPP). The successful deployment and development depend on balanced and distributed participation, responsibilities, and investment, in collaboration with business, academic, and non-governmental organizations. In many areas it is the industry that assumes the leading role with its capacity and resourcefulness, and that is the more active element in public-private partnership models. It is essential to clearly define the roles of the relevant stakeholders with regard to assets, systems and business processes – owners, managers, operators, users/customers, providers, then assess the degree of current and future digital dependency, responsibilities, requirements, and recommendations to achieve cybersecurity and resilience.

More and more services, systems and resources become critical in the digital space. Connected means vulnerable to virtual attacks and unknown attackers. A particularly important issue stems from the increased tying of information and communications systems with such critical infrastructure sectors and systems as energy, transport, finance, healthcare, telecommunications, food and water supply, defense. Many new areas are added to the list as "essential services", some of the "e-" type (like e-health, e-commerce, internet search engines, etc.), see [4] and [6]. Most of them operate under specific ICT and control systems (ICS, SCADA), services, networks and infrastructures form the core of the economy and society either providing vital products and services or being themselves the main platform of other critical infrastructures (CI) allowing us to exercise our rights and liberties as citizens. The communication and information systems (CIS) are also considered as critical communications and information infrastructures (CCII), including those serving the public administration and state, since their disruption or destruction may lead to major disturbances and disruption of the state and society. Many governments are concerned about the ability of the private sector with a rapidly increasing role as "operators of essential services" to provide acceptable level of security without governmental intervention. This lead to several proposals on mandatory reporting of security incidents and obligations to share information, security standards and compliance procedures (some already introduced by the EU NIS Directive in [4]). However, the main principle for building trust between industry and governments is keeping the balance between regulation and self-

regulation, bottom-up voluntary approach for collaboration with more and heavier regulations.

3.2 Engaging the Business: Value Chains and Shared Risk

The approach we consider to engage more naturally the business and industry in building the collective cyber security and resiliency is derived from the standard Porter's business value chain analysis [8]. Value chains (or value streams) provide a logical scheme to identify and engage the interconnected businesses through their normal business dependencies, roles and channels and then add the underlying digital dependency and the associated shared cyber risks. In addition, the value chains approach would allow joint and collaborative involvement and engagement of "small" and "big" businesses, based on the natural business logic and clustering not necessarily driven by ICT aspects. This allows revealing of various "hidden" threats and digital dependencies with significant potential impact on business continuity and resilience. There is no small or big in the value chain from a cyber security perspective – as "small" data breaches of essential data could jeopardize the entire chain. Moreover, within the chain this would be of the type of "insider threat" but without means for forensics, intel or other attribution techniques, a kind of "man in the business value chain". An increasing number of cases utilize weaknesses in the alignment of value chain business processes and practices and managing the interdependencies.

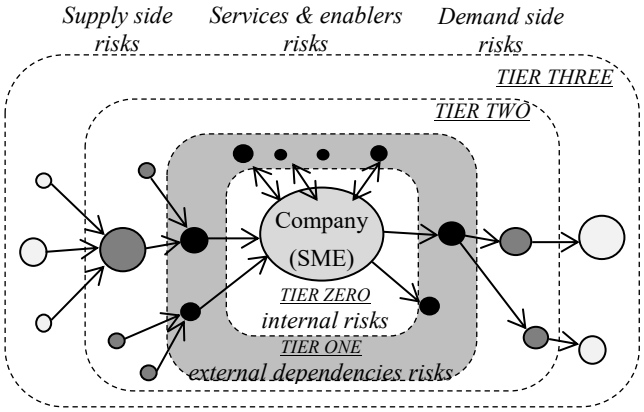

Figure 2. Shared cyber risks over value chain dependencies.

The goal is to create a sustainable and growing "appetite" of CEOs and leaders (including in small businesses, SMEs) for revealing cyber risks by exploiting the dependency chains, both on supply and demand side, but also including external services (see Figure 2). The key for spreading such appetite, like a "good virus", is in sharing with first tier partners (i.e. the first layer of connected businesses around the particular company), and this way propagating the initiative through the connected business from both demand and supply side direction (method, derived from Social Network Analysis and combined with gamification techniques). Such gamified approach will pave the way for implementation and compliances with specialized standards (such as ISO/IEC 27036). Value stream mapping was used to address also "insider threats" (this is "tier zero" on Figure 2), and risks at "tier one" shared with enablers and external services (providers of outsourced services, such as legal, payroll or bookkeeping, computer and ICT maintenance, etc.).

3.3 Cyber Picture and National Situational Awareness

To address the cyber security and resilience at the national level, first we need a holistic view on the situation - monitor the status and condition of the cyberspace within the country, accompanied with summary information and indication of the status and proper functioning of the communications and information systems (including electronic communications systems, transmission networks, and national and international information connectivity). This dynamic view is also referred to as the "national cyber picture" (e.g. in the National cybersecurity strategy of Austria). The intent is to construct and maintain a cyber picture which is as relevant and comprehensive as possible, at national level. To this end, standardized information exchange protocols and unified alert levels status codes need to be established (consistent with already established conventional crisis codes, as well as with those of the EU, NATO, and partner networks). The elaboration of such national-specific protocol scheme is based on the approach of OASIS Cyber Threat Intelligence Technical Committee and open standards, such as STIX (Structure Threat Information Expression), TAXII (Trusted Automated Exchange of Indicator Information), CybOX (Cyber Observable Expression). That approach allows to develop standardized representations for campaigns, threat actors, incidents, tactics techniques and procedures, indicators, exploit targets, observables, and courses of action and develop own standard-based sharing architecture at national level.

The cyber picture is essential part of the general status of the country, and the institution that monitors the cyber picture (National cyber situational center) will operate closely with the general national situational center (which in the case of Bulgaria is under the Security Council). The real value of the picture is to consider it in the context, or aligned with the general picture and cover potential hybrid crisis. For example, a terrorist attack on civil or industrial object. The attribution is difficult, and even qualifying the observed a "terrorist act" is difficult. Could be due to malfunction of a system, accident, hacker attack over the control system (ICS, SCADA), negligence, or just bad coincidence of several smaller factors. An essential rule here would be that whatever accident happens, the "cyber alert" or color-code status of the respective domain/sector should be elevated. Because if it was really cyber we need to act quickly, so we better assume it is cyber or at least it might have a cyber component. Second – attribution in cyber is extremely difficult, so we would need eventually some additional relevant artefacts (of non-cyber nature).

4. COLLABORATIVE CYBER RESILIENCY

The establishment of a viable national cybersecurity system requires an introduction of organizational model for collaboration between public and private entities with different level of maturity and capabilities, furnished by appropriate technical platform with the following main characteristics:

- Maintain a "live" national cyber picture - situational awareness at national level, a generalized view based on info sharing on the status of organizations (or cyberspace segments), ongoing disruptions with expected impact assessed and dynamically updated;

- Ensure common and comprehensive understanding of the situation (or "status of alert" with respective levels, for example color codes) by all the players;
- Coordinated response with feedback on efficiency of measures (including preventive ones, not only reactive);
- Establish time limits for reporting, response, reaction, closure, etc. and maintain a method to dynamically adapt them to the situation and capabilities of the organizations;
- Continuous improvement – validation and verification, info sharing protocols and systems evolution, security and protection (of the framework), international harmonization and compliances, trainings, lessons learned.

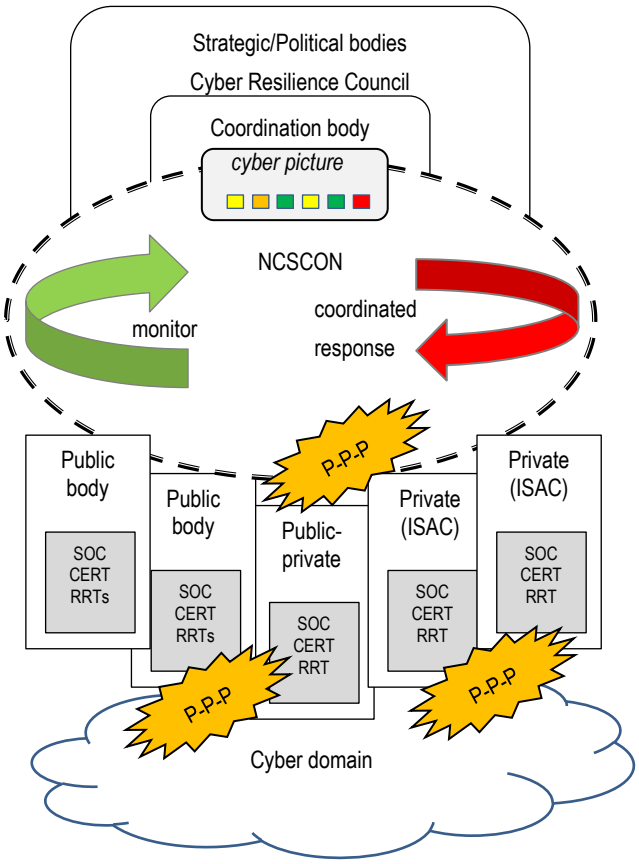

Figure 3. Collaborative framework for national cyber resilience.

4.1 National Collaborative Network

To provide operational coordination at national level, we have designed and are in the process of setting up an organizational framework with technical platform - National Cyber Security Coordination and Organizational Network (NCSCON) with the following general functions:

- Construct, maintain and broadcast (share) the national cyber picture;
- Coordinated response and operational interaction and collaboration in the event of massive incidents, complex attacks and crises: performed with organizational and technical means and based on the current cyber picture, status analysis, and, by means of a technical protocol and organizational measures, provision of status information at national level, possible combined threats and hybrid impacts, potential kinetic and cascade ("domino") effect, and recommendations for preventive action at operational and tactical/technical level, activation of cyber defense plans and actions, mobilizing experts and forming cross-sectoral reaction groups.

As outlined in Figure 3, the NCSCON is the "neural system" of the national cybersecurity system and is built and developed on the basis of the public-private partnerships (PPP) model, engaging all relevant stakeholders from the public and private sectors. The initiation and core development of NCSCON is provided by the state organizations and bodies directly engaged with national security systems (and with cyber security). NCSCON is designed "open" for inclusion of organizations representing the main cyber resilience stakeholders (state, business, non-governmental), but compliant to both technical and organizational requirements.

The participating organizations operate in interactive collaboration, continuously emitting information on their cyber status with sufficient details to build the national cyber picture, the purposes of national monitoring and, in turn, receiving the current cyber picture with level of details they are authorized to view, including the operational evaluation of the overall situation, guidance and recommendations for coordination and interaction with other organizations. NCSCON normally operates as a coordination platform and collaboration network with a coordination body, not a centralized "command and control center". It is the obligation of each participating entity to act immediately and autonomously within its competences, plans, and capabilities (implemented by CERT/CSIRT, or more advanced Security Operations Centers – SOC, with respective permanent or ad-hoc Rapid Reaction Teams – RRT). However, on the basis of the overall assessment of the situation and the cyber picture, their actions are further adapted, enhanced, and coordinated with other centers and organizations. All participating entities take preventive actions and dynamically increase their state of readiness based on their own analyses and assessments, but adapted to the context of the national cyber picture and the recommendations of the coordination body or other special analytical and/or research bodies, connected also to NCSCON. Based on the cyberspace governance roles, different connected bodies may have different structure and responsibilities. Public bodies (ministries, agencies) typically have legally defined responsibilities and a mandate for specific sectors with roles from the national security programs and system. Private bodies could represent associations, clusters or other formats of information sharing and engagement gatherings, which qualify for membership. As shown in Figure 3, different forms of public-partnerships are applicable at operational level (e.g. for the NCSCON itself), and more technical level (for CERTs/CSIRTs).

The usual collaborative behavior turns into more centralized mode of operations in case of a national crisis (code "red") or state of emergency is declared, not necessarily of a cyber type, as previously described in 3.3. However, the contingency plans and procedures need to be fully adapted to the digital context in advance, and exploit to full extent the power and services of NCSCON, but in predefined and elevated "emergency mode".

The NCSCON architecture and operating model are based on the principle of a virtual collaboration network and follows the proven, working, and flexible service-oriented model. The network will be built logically and technically in different layers

(rings) with corresponding levels of protection and resilience. Parts of the information, in the appropriate form, may be shared via additional expanded channels on the basis of a tailored standard for sensitive information sharing in public-private communities and organizations.

Looking from a system theory perspective, NCSCON falls in the category of complex interoperable systems and applicable models are like system-of-systems for service oriented collaborative architectures [3]. From the engineering perspective, each of the member bodies govern and operate based on its own layer of complex and interconnected systems, with own implementation principles and architecture, technical solutions, level of maturity and interoperability, legacy, reaction latency, etc. To achieve the operability and resilience of NCSCON, each of the member systems must be autonomous, self-sufficient, self-maintained or self-healing, etc. To ensure that, additional and heavier requirements to those systems are already defined (of the type "security by design", "resilience by design"), both to public and private participating bodies.

4.2 Information Sharing and Public-Private Collaboration

Cooperation and collaboration are based on implementing trusted information sharing principles, organizational engagement models and secure channels. Participation and engagement of the major relevant stakeholders at all levels - strategic, operational and technical require implementation of efficient information sharing mechanisms. Technically, this is provided by platforms such as NCSCON and the compliance to them could be assessed and granted. However, the organizational perspective requires formalized and institutionalized grouping which guarantee sufficient level of trust between public and private bodies and organizations. To provide that, we have foreseen a structured approach to forming platforms such as ISAC (Information Sharing and Analysis Centers) that are institutionalized by respective formats of public-private partnerships (PPP).

4.2.1 From information sharing to collaboration

The classical ISACs and CERTs information style is based on TLP (Traffic light protocol). It has more informative, kind of "food for thought" or knowledge sharing nature, and does not imply some specific actions. At least the action part would be a full responsibility of separate members. As we consider ISACs as bodies that plug in the national collaborative network NCSCON, there are few additional aspects. First, there is a need to formalize to some extent this information sharing between public and private bodies, or within the PPPs as well. This will need to harmonize with existing regulations, legal and business specific norms (such as electronic communications ordinance, classified information law, compliances with international regulations, etc.). When necessary, they need to be modernized appropriately and timely. Second, the TLP need to extend with an "action" type information attributes. The basic "need to know" principle therefore extends with "need to share", and further to "responsibility to share", and even "obligation to respond/provide/act". This is more than messaging protocol issue (as described in 3.3), as it requires evolution of organizational and governance frameworks of public, private and clustered public-private bodies.

At the level of NCSCON itself, also a PPP model is considered, that requires much stronger regulation. On the top, we should guarantee a unified view on information value perception, collaborative risk management and trust [12], [13]. The basis for such coherent information sharing network is that all members have a common understanding of the information to be shared with respect to its perceived value, purpose and meaning (or the "sense-making"). Or we need to ensure that "green-s", "yellow-s", "orange-s" and "red-s" mean same to all players and decision makers.

4.2.2 When two "yellow-s" become "orange" or "red"

When we look at the color-code alert levels at the national cyber picture we should always bear in mind that they represent an aggregated and summarized common state of the underlying cyber segment (i.e. the respective systems, networks, communication channels, etc.). Among the main purposes of the national cyber picture is the combined view and the ability to re-assess the general state and occasionally some of the "segments" alert levels having the global view. In particular, this means that only at that higher level we could consider aggregated risks and identify to what extent they are "coincident" (simultaneous, but from different causes), "related" (based on common cause) or "interconnected" (that are related by their generic characteristics). Aggregated risks usually result in larger impacts, so several "yellow-s" may turn jointly to "orange", or even "red". Some organizations (like DHS in USA) moved already from fixed level color schemes to more advanced quantitative/qualitative expressions, which allow deployment of advanced qualitative reasoning and decision-making methods, known from the field of Artificial Intelligence (AI).

4.2.3 Public-private partnerships in action

Various public-private collaboration schemes are known from practice. A recent study by ENISA [4] determines three types:

- "leadership type" – lead and run by one of the members (most frequent);
- "coordinated" - run by a coordinating entity, a specifically created body (less frequent);
- "democratic" - peer or democratic collaboration (rare).

The PPP model for the implementation of the national collaborative framework NCSCON is of "coordination" type (Figure 3), with a specific government created body at operational level (the National Cyber Situational Center), and at the strategic level – the Cyber Resilience Council (a specific "format" of the Security Council) and the function of the National Cyber Security Coordinator.

The ISACs and CERTs (if implemented by, or related to some PPP) typically organize through the "leadership" model. That is valid for the public CERTs (Gov CERT, mil CIRC, Critical Infrastructure CSIRTs). Business driven ISACs (like a Financial ISAC with a specialized CERT) would go for "democratic" or "coordinated" type. Clusters could serve de-facto as ISACs (like "Cyber Defense" or "Cyber Resilience"). Another public-private partnering model dedicated to joint resources and capability development is the "Cyber Reserve" instrument, which binds a public body (MoD), private body (software/IT companies), and people (professionals). At international level (EU) a new PPP mega-body was just recently established (named a "contractual PPP" European Cyber Security Organization, ECSO).

5. A ROADMAP TO COLLABORATIVE RESILIENCY

Cyber resilience at national level is a conceptually new status, or "maturity level" label for the country. It requires systematic,

planned and coordinated activities of all major stakeholders, lead but not ruled by the state, progressing at a synchronized pace.

In Bulgarian National Cybersecurity Strategy [1] we have outlined three phases (following the classics in improvement programs development), which illustrate the "maturity levels" approach applied at national level:

- *Initial - Cyber secure institutions (phase 1):* introducing multi-stakeholder approach, obtain common understanding and commitments on the priorities of the National strategy and the Action plan, adopt a coordinated approach and set up a common national cybersecurity system framework, define the main structures and core capacity, institutionalize the development processes and principles with the key stakeholders, align with NATO and EU, and ensure baseline cybersecurity, define and implement minimum requirements for security of network and information systems (as in EU NIS directive [5]), achieve cybersecurity at the level of the individual organization, implement a cyber security public-private partnership at national level, etc. ;

- *Development - Cyber resilient institutions and cyber secure society (phase 2):* "from capacity to capabilities" - unite the capacity, built at initial level and work on resilience of individual organizations (public and private), as well as capabilities for coordinated response to cyber crises, organize prevention activities and institutionalize the collaboration, extend the coverage of the national cyber picture, improve capabilities for operational and strategic analysis, and international operational and technical collaboration (EU, NATO, region);

- *Maturity/Leadership - Cyber resilient society (phase 3):* effectively collaborate at the operational and strategic levels at a national and international scale (EU & NATO), based on the model and commitment of all stakeholders, develop capabilities, both in public and private and research sectors, in identified niches, in order to secure leading positions in the region and specialize in cybersecurity and resilience partner networks.

6. ACKNOWLEDGMENTS

This work summarizes the contributions and final agreements of the Interagency Expert Working Group (established in 2015 by order of the Prime Minister of the Republic of Bulgaria) on principles and approach for the development of the National cybersecurity strategy "Cyber Resilient Bulgaria 2020".

Short Bio

George Sharkov obtained his PhD in Artificial Intelligence, with specialization in applied informatics, biophysics, thermography and genetics, enterprise intelligent systems. Since 1994 he was leading international software projects and companies for banking and financial systems, e-business, online markets and innovative e-trading solutions. Since 2003 he is managing the regional center for Eastern Europe of the European Software Institute. He is trainer and appraiser for software engineering quality management, resilience management. Lecturing software quality, cybersecurity and business resilience. Since 2014 George is appointed as a National cybersecurity coordinator for the Bulgarian Government, and is leading the development and implementation of the National cybersecurity strategy.

7. REFERENCES

[1] Bulgaria 2016. National Cyber Security Strategy "Cyber Resilient Bulgaria 2020". Council of Ministers (July, 2016). http://www.cyberbg.eu

[2] Caralli, R., Allen, J. and White, D. 2011. *CERT Resilience Management Model (CERT-RMM)*. SEI Series in Software Engineering, Addison-Wesley Professional.

[3] Cámara, J., Moreno, G.A., Garlan, D. and Schmerl, B. 2016. Analyzing Latency-Aware Self-Adaptation Using Stochastic Games and Simulations. *ACM Trans. Auton. Adapt. Syst.* 10, 4, Article 23 (January 2016), 28 pages. DOI= http://dx.doi.org/10.1145/2774222

[4] ENISA 2012. *Cooperative Models for Effective Public Private Partnerships. Desktop Research Report*. http://www.enisa.europa.eu/act/res/other-areas/national-public-private-partnerships-ppps/desktop-reserach-on-public-private-partnerships/at_download/fullReport

[5] EUROCONTROL 2012. *Manual for National Air Traffic Management Security Oversight* (1st Edition). European Organisation for the Safety of Air Navigation, Brussels.

[6] European Union 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union* (Volume 59, 19 July 2016 http://data.europa.eu/eli/dir/2016/1148/oj

[7] Herbolzheimer, C. 2016. Preparing for a Black Swan Cyberattack. *Harvard Business Review* (September, 2016) https://hbr.org/2016/09/preparing-for-a-black-swan-cyberattack

[8] Porter, M. E. 1985. *The Competitive Advantage: Creating and Sustaining Superior Performance.* NY: Free Press

[9] Sheffi , Y. 2015. *The Power of Resilience: How the Best Companies Manage the Unexpected*. MIT Press.

[10] Sikula, N.R., Mancillas, J.W., Linkov, I. and McDonagh, J.A. 2015. Risk management is not enough: a conceptual model for resilience and adaptation-based vulnerability assessments. In *Environ Syst Decis* (2015) 35: 219-228. http://dx.doi.org/10.1007/s10669-015-9552-7

[11] Taleb, N.N. 2010. *The black swan: the impact of the highly improbable*. Random House Inc, New York

[12] Tropina, T. 2015. Public-Private Collaboration: Cybercrime, Cybersecurity and National Security. In *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*, Tropina T., Callanan C., Springer Briefs in Cybersecurity, 1-41. http://dx.doi.org/10.1007/978-3-319-16447-2_1

[13] Vazquez, D.F., Acosta, O.P., Brown, S., Reid, E., Spirito, C., 2012. Conceptual framework for cyber defense information sharing within trust relationships. In *Proceedings of 2012 4th International Conference on Cyber Conflict,* C. Czosseck, R. Ottis, K. Ziolkowski, Eds. NATO CCD COE Publications, Tallinn. https://ccdcoe.org/cycon/2012/proceedings/d2r2s3_vazquez.pdf