Information & Security: An International Journal

T. Tagarev & G. Sharkov, v.34:1, 2016, 59-68

https://doi.org/10.11610/isij.3404

MULTI-STAKEHOLDER APPROACH TO CYBERSECURITY AND RESILIENCE

Todor TAGAREV and George SHARKOV

Abstract: Identifying and involving all relevant stakeholders in national cybersecurity strategy (NCSS) development is key for defining the scope, setting the goals and approaches, and the roadmap to achieve targeted maturity levels. It is more than involving the three groups (government, private sector, academia) and requires a holistic approach towards security and resilience of all interconnected segments of national and international cyberspace. The paper presents the approach to making the Bulgarian NCSS (BG-NCSS). Different aspects of stakeholders' involvement and engagements are considered: for identifying the scope and developing the strategy, defining the responsibilities and engaging with the development of a national collaboration operational network, strategy implementation and the roadmap to a resilient society, and collaboration to achieve operational cyber resiliency. As a collaboration mechanism, applications of public-private partnerships at different levels are envisaged.

Keywords: multi-stakeholder approach, cybersecurity strategy, cyber maturity, organizational framework, collaborative networks, organizational model, stovepipes, intelligent complex adaptive system, public-private partnership

Introduction

In the globalized, digitalized, and interconnected global economy and society, more and more activities move to that virtual and man-made space - cyberspace. It is more than the Internet and interoperable systems – an entirely new domain in addition to the four physical domains (land, sea, air, and space). And there is a joint agreement that fostering a free, open, and secure cyberspace requires a multi-stakeholder approach to capacity building and suitable governance models. Developing a national cybersecurity strategy (NCSS) lies at the core of these efforts. By providing a comprehensive framework for prevention, preparation, response, and incident recovery, the NCSS represents a critical element of a country's cybersecurity maturity and readiness. A large variety of measures could be taken to implement the NCSS—legislative, institutional, technical, or others—aimed at reducing the scale of cyber threats and cyberattacks, as well as minimizing their impact. It is, however, more than mitigating the new emerging

risks coming from the pervasive digital transformation and the growing new dependencies. Cybersecurity, however, is not solely an issue for governments and ensuring a free, open, and secure cyberspace is not the preserve of any single stakeholder group. Cybersecurity is a shared responsibility requiring coordinated efforts by government authorities, the private sector, and civil society. The key to success is effectively involving all relevant stakeholders in developing, implementing, and reviewing a country's NCSS. However, if the value of such an inclusive approach to cybersecurity, implementing it is not straightforward. It requires dedicated effort and appropriate leadership, specialized skills and knowledge development, and practical guidance for implementing the NCSS and continuously improving it. Also, the NCSS lifecycle refers to the series of stages with different roles and responsibilities of the stakeholders involved. The general instrument to achieve collaboration and synergy is through public-private partnerships. These lifecycle stages are typically: *Initiation > Stocktaking and Analysis > Production of the NCSS > Endorsement and Implementation > Monitoring and Evaluation.*

The two practical benefits of engaging a broader range of stakeholders are:

- Achieve well-informed and evidence-based policy outcomes, aggregating the diverse experience and areas of expertise of different stakeholders. The majority of this is unlikely to exist within the government structures only. The private sector would better understand the cyber threats faced by businesses and society and the products to monitor and preserve cybersecurity.[1] Civil society organizations provide extensive expertise in the human rights implications and specific cybersecurity threats to different groups, also as experience in working directly with individuals
- More effective implementation of the NCSS and achieving the country's cyber maturity levels.

Guidance and Recommendations Followed

Practically all guidance documents on developing NCSS emphasize the critical importance of involving and engaging a broader range of relevant stakeholders. During the development of the first Bulgaria National Cybersecurity Strategy "Cyber Resilient Bulgaria 2020" (BG-NCSS),[2] we have studied and followed the recommendations from a broader range of international sources: ITU, Commonwealth Telecommunications Organization,[3] ENISA, NATO, and lessons learned from countries with more advanced strategies, and even several improved versions already (like USA, UK, Netherlands, Austria, others). At the international level, ITU [4] first started with the Global Cybersecurity Agenda (GCA) in 2011 as a framework for international multi-stakeholder cooperation on cybersecurity. It aimed to build synergies with current and future

initiatives and partners toward a safer and more secure information society. GCA defined five pillars: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation. An international multi-stakeholder approach has been established and maintained at the global Internet level for the international domain names and Internet governance (ICANN).[5]

To identify the list of relevant stakeholders, ITU followed the proposed one by the Carnegie Mellon team led by John Haller [6] in the report "Best Practices for National Cybersecurity," which include: Executive Branch of the Government; Legislative Branch of the Government; The Judiciary; Law Enforcement; Intelligence Community; Critical Infrastructure Owners and Operators; Vendors; Academia; Foreign Governments; Citizens. ITU further elaborated on the type of entities of each category, which we briefly present in Figure 1 below.

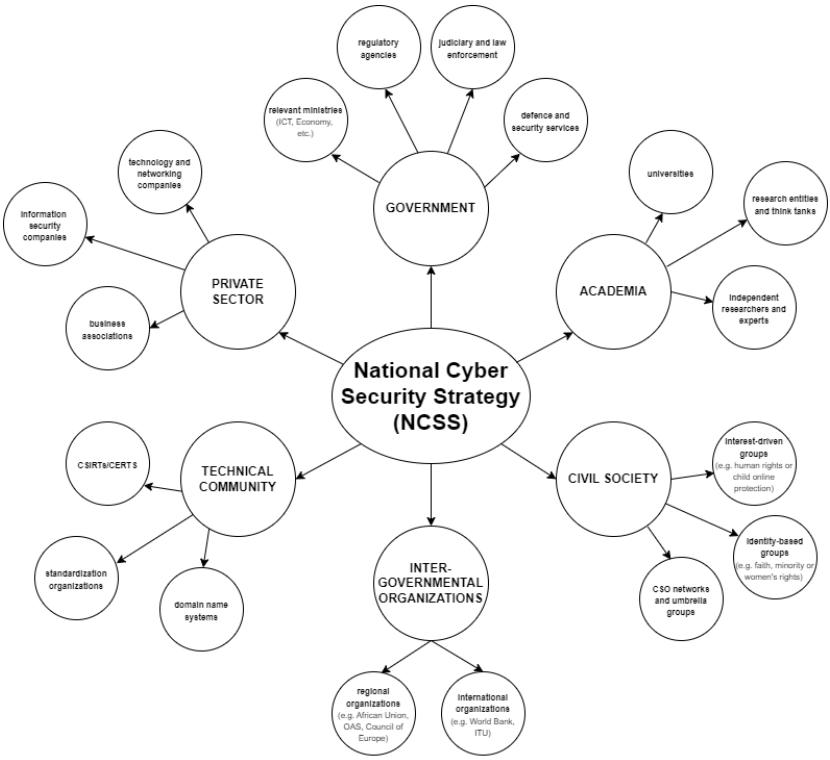

Figure 1: Multiple stakeholders and entities involved in NCSS (based on ITU list).

ENISA (the European Network and Information Security Agency) published its first National Cyber Security Strategy Good Practice Guide in 2012. In 2016, ENISA prepared an updated version of the guide, following the updates and lessons learned from EU Member States and EFTA countries when developing and implementing their National Cybersecurity Strategies (NCSS).[7] The ENISA guide presents the status of the implementation of NCSS among EU Member States and identifies gaps and challenges such as:

- Establish effective cooperation between public stakeholders
- Establish trust between public and private stakeholders
- Ensure adequate resources
- Promote a common approach and awareness for privacy and data protection
- The implementation of vulnerability and risk analysis.

Among the good practices, the guide also provides valuable insights for the stakeholders involved in the lifecycle of the strategy, such as private, civil, and industry stakeholders. In "Recommendation 6," the advice is to "Approach and involve stakeholders at an early stage of (strategy) development." It also advises "Establishing a public-private partnership." The involvement and engagement of all relevant stakeholders in provisioning the NIS Directive into the NCSS and national legislation, prioritizing specific critical sectors (operated mainly by private organizations), and extending the scope of international cooperation beyond international exercises (where academia and industry play an essential role).

Another key advice is to "Set a clear governance structure." Such a governance framework must define all relevant stakeholders' roles, responsibilities, and accountability. Two types of governance structures are used: centralized approach with a central cyber security authority with broad responsibilities and competencies across sectors, and decentralized approaches – based on a strong degree of cooperation between public agencies and motivated by the principle of subsidiarity. Countries have also developed different relationships with the private sector. Some countries have established co-regulation in cyber security through institutionalized forms of cooperation such as public-private partnerships. Other countries have created new dedicated laws to regulate the private sector. Among other recommendations concerning the central role of Critical Information Infrastructure Protection (CIIP) in the digitalized economy and society the enhancement of capabilities of both public and private actors, with the focus on CIIP and other priority critical sectors (essential, as outlined in the NIS Directive).

Multi-Stakeholders and Challenges of Formulating BG-NCSS

In addition to the known global challenges, we have faced some specific issues:

- Cyber threats don't fit nicely with the remit of any existing organization
- Defining the scope –the risk of incompleteness or over-complicating
- Anecdotal evidence and unpredictability
- Limited ability for objective assessment of alternatives
- Propensity for and readiness to innovate.

The organizational framework and existing players in the field are not well established and defined. Various ad-hoc initiatives, palliative measures, or isolated capacity development mini-projects are in place. The status could also be characterized in the following way:

- Stovepipes with limited cooperation and lack of coordination
- Search for either a "lead" or a "super (supra)" cybersecurity agency
- Multiple stakeholders not collaborating or engaged at the national level, fragmented capacity in the private sector and academia.

Also, modernization lags modern trends in the security sector, and digital transformation is critically delayed, as well as capabilities development.[8] The concept of cyberspace as a domain of military and defense operations [9] and preparing for the new type of ongoing cyber war in cyberspace has not been addressed.

The main groups of identified stakeholders, following the recommendations by ITU and ENISA, as presented above and in Figure 1, have been further detailed with particular entities and organizations in a general "stakeholders map," as shown in Figure 2. Their roles and level of engagement (strategic, operational, tactical) are also indicated, plus the partnerships envisaged with international organizations.

Coordinated Efforts of a Broad Range of Stakeholders

After several failures to agree on the mechanism of developing an NCSS in Bulgaria and the leadership role, the practical work started in late 2014, which resulted in a comprehensive and very detailed final proposal (in 2015-16). Among the key factors for this successful and relatively fast production, we may outline:

- Establishing the role and appointment of a National Cybersecurity Coordinator, and a broader working group involving not only relevant ministries and agencies but also representatives of academic and industry organizations
- The leadership and commitment of a strategic government policy structure (Ministry of Defense, support by the Prime Minister's office)
- Setting cybersecurity as a priority element of the National Security Strategy, and support by the Security Council, the Secretary and designed as a new component integrated into the "National Situational Centre"

- Anticipating the challenges and the legal context at the EU level (NIS Directive) and NATO (Cyber Defense Capabilities, Cyber domain as the 5th domain – Wales 2014, Warsaw 2016).

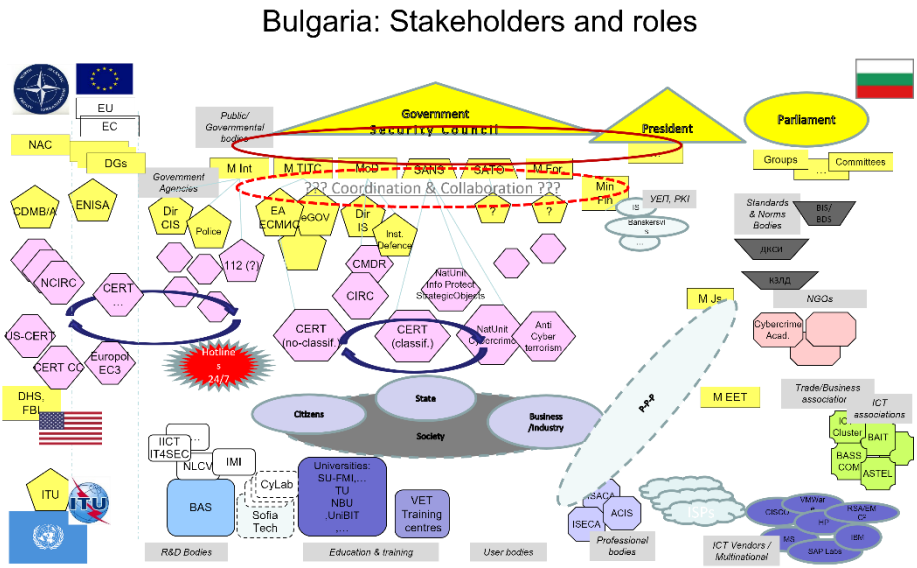

Figure 2: The stakeholders' map and international collaboration bodies (BG-NCSS).

Stakeholders in Operationalizing the strategy BG-NCSS

Regarding the organizational structure which would provide the best matching opportunities for engaging the stakeholders in Bulgaria, we decided that the legacy strict hierarchies and stovepipes, exclusively governmental structures, are a thing of the past. These models cannot provide the necessary flexibility, scalability, and adaptiveness to new challenges and do not sufficiently engage the private sector and academia. Networked and distributed models have been considered at the organizational collaboration level (process-oriented) and communication and interoperability networks (system level). Various 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 holistic approach requires stronger alignment and convergence of previously "siloed" activities and leads to the evolution and convergence of respective models and standards. One of the recent meta-models to manage as whole operational risks and resiliency in the digitized world was introduced by CERT at Software Engineering Institute as CERT-RMM (Resilience Management Model).[10] We have referred to this model to define cyber resilience at a higher national level and to set goals and cyber maturity levels to achieve.

Public-Private Partnerships – an Instrument for Stakeholders Engagement

Following the ENISA [11] "Practice Guide on Cooperative Models for Effective Public Private Partnerships (PPPs)," we have identified the main components and players to achieve security and resilience at the national level. As an example within the strategy and the implementation guidelines, we have provided details about the five questions we need to answer and identify relevant components and stakeholders (Why, Who, How, What, and When). The involvement of Small and Medium Enterprises (SMEs) in the process of PPP building is also crucial since they are the backbone of the European economy. We have also followed the saucerful models and guidelines for setting PPP of more advanced nations.[12]

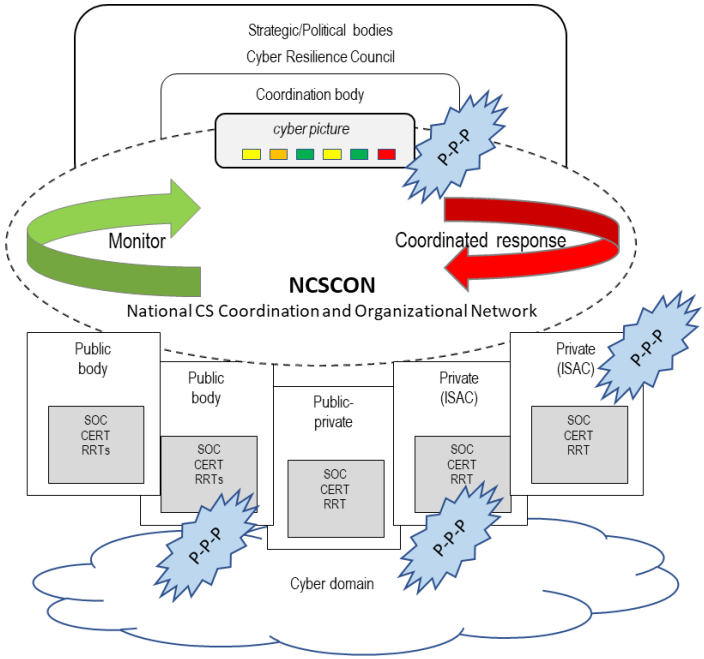

Figure 3: Stakeholders engagement in organizational and operational cybersecurity framework (Bulgaria, National Cybersecurity Strategy). P-P-Ps indicated.

The Collaborative Model for National Cybersecurity

The organization model envisaged for the national collaboration network is based on the theory of system-of-systems (SoS), which at a higher national level, would provide interoperability and collaboration between systems and organizations that operate different types of essential services, critical infrastructure or other sectors and business areas of national importance. The concept of the "intelligent complex adaptive system"

(ICAS) was also introduced. This collaboration scheme and the role of different stakeholders are shown in Figure 3. Some options for PPPs are also indicated.

However, the organizational perspective requires formalized and institutionalized grouping, which guarantees a sufficient level of trust between the 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 public-private partnerships.

The Roadmap to National Cyber Resilience and the Role of Stakeholders

Achieving cyber resilience at a national level is a conceptually new status, or "maturity level," or a "label" for the country. It requires systematic, planned, and coordinated activities of all major stakeholders led but not ruled by the state, progressing at a synchronized pace. In the proposed GB-NCSS we have agreed on three main stages:

- *Initial: Cyber secure institutions.* Introducing a multi-stakeholder approach, obtaining a common understanding and commitment to the priorities of the National Strategy and the Action plan, adopting a coordinated approach and setting up a common national cybersecurity system framework, defining the main structures and core capacity, institutionalizing the development processes and principles with the key stakeholders, align with NATO and EU, and ensure baseline cybersecurity, define and implement minimum requirements for the security of network and information systems (as in EU NIS directive), achieve cybersecurity at the level of the individual organization, implement a cyber security public-private partnership at the national level, etc.
- *Development: Cyber resilient institutions and cyber secure society*. Following the principle "from capacity to capabilities" – unite the capacity, built at the initial level and work on the resilience of individual organizations (public and private), as well as capabilities for a 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*. 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.

For each stakeholders group different engagements are detailed in the strategy, related to their role in defining the goals and initiating projects and initiatives, but also in implementing them, as well as the collaboration partners expected at national and international level. For example, the engagements of "Academic stakeholders" are defined as: Technical knowledge (threats, identification of protective measures, implementation); Decision support (strategy, policies, organizational arrangements, business processes, procurement decisions and project management); Education and training; Focus research areas; Knowledge sharing, dissemination

Conclusion

Involving a broader range of relevant stakeholders in the making of a national cybersecurity strategy (NCSS) is not enough for the success of this endeavor. It is important to obtain their engagement and commitment to implement the strategy. The instrument to do that is through various types of public-private partnerships. These are the main lessons learned when we were leading the development of the Bulgarian NCSS "Cyber Resilient Bulgaria 2020." To achieve the targeted cyber maturity levels, collaboration and stronger commitment by all stakeholder groups are essential.

References

[1] Scott J. Shackelford, Timothy L. Fort, and Jamie D. Prenkert, "How Businesses can Promote Cyber Peace," *University of Pennsylvania Journal of International Law* 36, no. 2 (2014): 353-431.

[2] *National Cyber Security Strategy "Cyber Resilient Bulgaria 2020,"* Council of Ministers (final draft, in Bulgarian), available at http://www.cyberbg.eu.

[3] Commonwealth Telecommunications Organisation, *Commonwealth approach for developing national cybersecurity strategies* (2015).

[4] Frederick Wamala, "ITU National Cybersecurity Strategy Guide", International Telecommunication Union, 2011, available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

[5] Lennard G. Kruger, "Internet Governance and the Domain Name System: Issues for Congress," *CRS Reports* R42351 (Washington, D.C.: Congressional Research Services, 2014).

[6] John Haller, Samuel Merrell, Matthew Butkovic, and Bradford Willke. *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0* , CMU/SEI-2011-TR-015 (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2011), available at https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9999.

[7] ENISA, *NCSS Good Practice Guide. Designing and Implementing National Cyber Security Strategies.* (ENISA, 2016) available at https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[8] Todor Tagarev, "Capabilities-based Planning for Security Sector Transformation," *Information and Security: An International Journal* 24 (2009): 27-35, https://doi.org/10.11610/isij.2404.

[9] Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014).

[10] Richard Caralli, Julia Allen and David White, *The CERT Resilience Management Model: a Maturity Model for Managing Operational Resilience (CERT-RMM)*, SEI Series in Software Engineering (Addison-Wesley Professional, 2011).

[11] ENISA, *Cooperative Models for Effective Public Private Partnership (PPP)* (ENISA, 2011), available at https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperative-models-for-effective-ppps.

[12] Max Manley, "Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership," *Journal of Strategic Security* 8, no. 5 (2015): 85-98, https://doi.org/10.5038/1944-0472.8.3S.1478.

About the Authors

Todor TAGAREV is Professor at the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences and Head of its IT for Security Department and Centre for Security and Defence Management. A security and defence planner combining governmental experience with sound theoretical knowledge and background in cybernetics, complexity, and security studies, he has been specializing in security sector reform and institution building, primarily from organizational management perspective. Prof. Tagarev was defence minister in Bulgaria's Caretaker Government, March-May 2013. E-mail: tagarev@bas.bg

Dr. George SHARKOV is adviser to the Bulgarian Minister of Defense and National Cybersecurity Coordinator. He is a director of the European Software Institute CEE since 2003 and Head of the Cybersecurity Lab at Sofia Tech Park. *E-mail:* gesha@esicenter.bg