ALTERNATIVE MODELS OF NATIONAL CYBERSECURITY ORGANIZATION: COMPARATIVE EVALUATION

Todor Tagarev, Institute of Information and Communication Technologies
Vasil Rizov, "G.S. Rakovski" National Defense College

ABSTRACT

The provision of cybersecurity requires diverse capabilities, typically provided by several main organizations plus numerous other public, private, and societal actors. This article explores alternative ways of organizing these capabilities at a national level and attempts to define a 'best' model. For that purpose, the authors outline six alternative models positioned along two dimensions according to the degree of coordination among main cybersecurity contributors and the degree of centralization. These alternative models are evaluated vis-a-vis five criteria—Effectiveness, Efficiency, Resilience, Agility, and Cooperation—using the analytical hierarchy process and interviewing 88 experts from the public administration, academia, and the business sector. The results indicate a clear preference for robust operational cooperation and coordination in the development of cybersecurity capabilities. They can serve as evidence in the search for the best organizational arrangements. The findings are context-specific and reflect the Bulgarian culture. Yet, the methodology is applicable in any context, and the results might be of interest to cybersecurity policymakers globally.

Keywords: Cybersecurity, Strategic Management policy organizational Models, Cooperation, Effectiveness, Efficiency, Resilience; Agility, Co-Operation, Coordination, AHP.

INTRODUCTION

Advanced information and communication technologies provide abundant rewards in terms of competitiveness, political engagement, security capabilities, and social interaction. Yet, numerous actors are willing to and already exploit the opportunities provided by increased connectivity to gain political (Hare, 2019; Paterson & Hanley, 2020; Gunneriusson, 2021) and military (Libicki, 2020; Sotelo Monge & Maestre Vidal, 2021) advantages, access classified or other sensitive information (Greiman, 2018; Cunliffe, 2021), promote terrorist agendas (Haberl, 2020), disrupt critical infrastructures and the delivery of essential services (Weiss & Biermann, 2021), receive ransom or other financial or material gains (Paşca & Simion, 2020), indulge in illegal behavior (Quayle, 2020), or just to demonstrate their attack capabilities.

The attackers have the advantage of selecting a target and the timing of their cyberattack. On the other hand, the defending side needs to be able to protect any potentially vulnerable asset, react to limit the immediate impact of the cyberattack and restore the functionalities of critical systems, and manage the consequences. In addition, a smart defender will attempt to mitigate risks, predict a cyberattack, foresee the evolution of the cybersecurity landscape and adapt accordingly.

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

These, however, are daunting tasks. Even at the level of an individual organization, the senior management has to understand at least the vulnerabilities of IT infrastructure to cyberattacks, their criticality for the organization's functioning, the potential impact of a possible cyberattack, and the technological and procedural solutions available to reduce the cyber risk. On that basis, organizations develop cybersecurity policies and invest in new procedures, training, and technological solutions. Some national and international standards already assist in identifying and managing cybersecurity risks in a consistent framework (e.g., NIST, 2018), thus facilitating the establishment of the organizational cybersecurity policy.

The assignment of roles and responsibilities and resourcing the involved actors, i.e., organizing for cybersecurity, is part of the strategic management of cybersecurity. Establishing a policy for a sector or broad security area, e.g., defense, law enforcement, (counter)intelligence, or critical infrastructure protection, is certainly more complex than for an organizational policy. To take cyber defense as an example, there are significant differences in priorities, concepts of operations, and consequently, in organizing the armed forces and other contributing players. The studies of cyber defense policies of Germany (Leinhos, 2020), the United Kingdom (Lester & Moore, 2020, and Israel (Tabansky, 2020) demonstrate how important national specifics can be. Hence, every organizational decision is specific as well.

Finding the best organization at national-level cybersecurity is even more challenging. The European Union Cybersecurity Agency (ENISA), for example, published a good practice guide for designing and implementing a national cybersecurity strategy. The guide recommends to *"set a clear governance structure,"* tasks to be considered in the process, and outlines three high-level options for the national governance structure (ENISA, 2016), but does not advise on adopting one or the other of those *"structures."*

Hence, it is up to each country to find a model that best suits the specific cyber vulnerabilities and threat landscape, the general administrative arrangements, public-private and societal relations, and the available human and technological capacity. However, several issues complicate the problem of devising such a model:

- Hackers use more sophisticated tactics, techniques, and procedures with higher negative impact; hence the need for a timely and effective response;
- Some of the attacks target new, not properly protected assets in sectors for which the national responsibilities are not clearly defined;
- The effects of some cyberattacks tend to propagate across sectors, while others may have transversal effects (Pappalardo et al., 2020);
- The threats from cyberspace continue to diversify and thus require a continuous adaptation of the cybersecurity system;
- Cybersecurity experts are in high—and increasing—demand, and the national capacity is often insufficient to meet the demand for expertise.

New technological or societal developments, such as artificial intelligence and the Covid-19 pandemic, add attack vectors to the threat landscape and another layer of complexity in searching for effective cybersecurity solutions.

In summary of the discussion so far, the elaboration of a national cybersecurity strategy is highly context-specific. Any decision on policy and strategy, including organizational arrangements, should consider existing responsibilities and relations between the leading security institutions and is inevitably influenced by the balance of power among the key players with interests in cybersecurity.

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

The study presented here intends to promote rationalism in discussions on organizing cybersecurity at the national level. The article is structured as follows. Section 2 presents the authors' motivation to embark on this study. Section 3 describes the methodology, including the design of alternative organizational models and the set of criteria for their evaluation, and the selected method for their expert assessment – the analytical hierarchy process (AHP). The results are presented in Section 4 and discussed in Section 5. The article concludes with a short discussion on the current status and ideas for follow-on research.

Motivation

In the early 2010s, senior Bulgarian officials recognized the need for a national-level cybersecurity strategy to guide the preparation of the country to counter threats from cyberspace. As a result, a draft of the first related strategic document appeared in 2012. It focused entirely on an organizational solution, proposing the creation of a new state agency to deal with cybersecurity matters. In the spring of 2013, one of the authors of this article (T.T.) was in a position to influence the fate of this draft and, instead of promoting it further, decided to launch a new process, involving all relevant ministries and agencies in the elaboration of a national cybersecurity strategy, the organizational arrangements being just one of the aspects to be discussed.

The primary rationale for the selected course of action stemmed from the earlier experience of this author in organizing the system for civil protection and transposing the European Union (EU) Directive for critical infrastructure protection (Council Directive, 2008/114/EC). At the turn of the century, Bulgaria's leading civil protection organization underwent several transformation rounds, turning it from an entirely military service to a civilian agency directly subordinated to the Council of Ministers (Tagarev & Ratchev, 2018). Some senior governmental executives thought that that arrangement was inadequate and tasked a Bulgarian Academy of Science team to conduct a comparative study of alternative organizational models. The study concluded that no significant organizational changes are needed, and priority should be assigned to enhancing the mechanisms for cooperation and coordination among key actors in crisis and disaster management, with the civil protection agency as its core (Shalamanov et al., 2005). Notwithstanding this research-based advice, in 2005, it was decided to create a new ministry, first called Ministry of Disasters, and later renamed Ministry of Emergency Management. It was soon realized that adding a new administrative layer without any substantial increase in the capacity to perform disaster management operations does not solve any of the underlying problems. Interagency rivalries persisted and, after a change of the party in power in 2009, the Ministry of Emergency Management was closed down, and the civil protection agency was placed under the Ministry of the Interior.

The case of transposing Directive 2008/114 into the national legislation was somewhat different. The directive covered two sectors of critical infrastructure – energy and transport, while Bulgaria designated a point of contact for operational exchange at the EU level in the Ministry of the Interior. This decision reflected nothing else but the power relations in the ruling elite in 2010.

In 2014, after another change in Government, the process of drafting the national cybersecurity strategy was relaunched. Both authors were included as members of the Interagency Expert Working Group (IEWG) tasked to draft the strategy. After intensive and often heated debates, IEWG came up with a document preserving the distributed cybersecurity

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

architecture and focusing on mechanisms for operational cooperation and coordination of the plans of all key players for developing their cybersecurity capabilities, as well as the infrastructure for cooperation and coordination. The strategy was approved by the Council of Ministers in the summer of 2016 (National Cybersecurity Strategy, 2016).

The approved strategy envisioned the design of a plan with a roadmap and their implementation in three phases until the end of 2020. Particularly strong were the expectations to invest in the development and testing of procedures and creation of the technical infrastructure allowing smooth and effective cooperation among all key players. Instead, the focus of the political leadership shifted to the implementation of the EU network and information systems security directive, known as the NIS Directive (Directive 2016/1148), through the introduction of a new cybersecurity law. The new law was expected to reassign cybersecurity responsibilities and, respectively, to shift the balance between key institutions. However, evidence and rational arguments were again in low demand, which led to our decision to perform this study.

RESEARCH METHODOLOGY

The methodology implemented in this study includes three steps: (1) design of a set of criteria for assessment of organizational arrangements; (2) design of alternative cybersecurity organizational models at national level; and (3) conducting interviews with experts to solicit their pairwise evaluation of criteria and alternatives. Each of these steps is presented in a sub-section below, while Section 4 presents the aggregated results from the expert assessment.

Criteria for Assessing Cybersecurity Organizational Models

Cybersecurity systems need to respond to diverse requirements. For example, a parallel study identified 33 groups of requirements to cybersecurity collaboration just from a governance perspective (Tagarev, 2020). On the other hand, and given the limitations of the memory capacity of a person, researchers recommend using between five and nine criteria in the AHP implementation (Mu & Pereyra-Rojas, 2017a). On that basis, the authors came up with an initial proposal for the set of evaluation criteria that was discussed with researchers during a workshop and consequently refined. As a result, our decision was to use five criteria in this study, described below.

Effectiveness

This criterion allows evaluating the extent to which a particular model of national-level cybersecurity organization allows to achieve:

- The necessary degree of situational awareness;
- Protection from cyber attacks;
- Capacity for early warning;
- An adequate response to an attack;
- Consequence management and recovery
- Forensics capacity, allowing to identify the reasons for a particular effect on the IT infrastructure and attribute an attack;
- Capacity for managing the core processes in the provision of cybersecurity;
- Planning and allocation of cybersecurity resources.

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

Of particular importance for the effective provision of cybersecurity, and in particular for achieving situational awareness, is the readiness of key actors to share information (Pala & Zhuang, 2019) and assist each other in response to a cyberattack. As Pöyhönen & Lehto (2020) pointed out, essential in that respect is the level of trust among cooperating organizations.

Efficiency

The inclusion of the Efficiency criterion affords to take into account the ratio between the expected results and the invested human, financial and material resources. More efficient is an organizational model that allows achieving a better result given a certain amount of allocated resources or, alternatively, to achieve a set result by minimizing costs. A particular consideration here is to avoid unnecessary duplication of capabilities provided by participating organizations.

Resilience

This criterion allows evaluating the capacity of a certain model of the national cybersecurity system to retain at least partly its functioning under a massive and partially successful cyberattack and recover its full functionalities and the functioning of the protected assets quickly. To be resilient, an organizational model needs to be dispersed and include some redundancies and backups while at the same time providing connectivity for flexible redirection of information and capabilities (Simon & de Goede, 2015). In addition, a highly resilient model would provide for self-organization and survival under heterogeneous attacks (Petrenko & Vorobieva, 2019).

Agility

This criterion allows evaluating the capacity of the national cybersecurity system to adapt in a timely manner to changes in the environment, including new threats, implementation of emerging technologies, economic, demographic, and educational shifts, etc. An agile model is prone to innovation and will allow to quickly identify the need for and fill in capability gaps.

Cooperation

The fifth and final criterion, used in the study, allows evaluating the capacity of a certain organizational model to provide for cooperation and collaboration between and among actors, specializing in cybersecurity, other organizations in the system for national security, allies, public and private actors. Of particular interest is the capacity to respond cooperatively to 'borderline' problems, such as the protection of critical infrastructures, countering hybrid threats, including online propaganda, combatting terrorism and radicalization, protection of the banking and financial system, etc.

Alternative Organisational Models

The possible models of the national cybersecurity system differ mainly along the level of coordination among the main contributing organizations and the degree of centralization (or distributed nature of the system). Initially, the authors developed several alternative organizational models that were then discussed at the same workshop discussing the set of

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

criteria for their evaluation. As a result, it was decided to develop and use in the assessment six basic models, designated respectively as:

1. Current Model;
2. Operational Cooperation
3. Coordinated Capability Development
4. SA *"Cybersecurity"*
5. SA *"e-Government & Cybersecurity"*
6. *"National Champion."*

Before describing the models, it is necessary to explain the current arrangement in Bulgaria and what precisely is meant by 'cooperation' and 'coordination.' In the current arrangements, the Ministry of Defense is responsible for countering external threats, including threats from cyberspace, and operations in cyberspace supporting other military activities. As a member of NATO, Bulgaria accepts the Alliance view that cyberspace is the fifth domain of operations. The Ministry of the Interior is the primary law enforcement agency. It has the lead responsibility for countering all types of cybercrime. The State Agency (SA) *"National Security"* is the national counterintelligence organization tasked to counter cyber espionage and threats to *"strategic assets."* The State e-Government Agency (SeGA) has the lead responsibility for network and information security. The national CERT is part of SeGA. However, SeGA has no functions related to the protection of classified information used by the other three agencies. The State Commission on Information Security has this responsibility, a fact that turns it into an important cybersecurity actor. Bulgaria does not have a State Agency *"Cybersecurity,"* hence model D is notional.

As for terminology, the coordination among cybersecurity stakeholders is examined at two levels:

- First, it can be *operational* when the organizations with cybersecurity responsibilities share available resources and capabilities in monitoring cyberspace, early warning, protection of assets, response to attacks, recovery, and mitigation of the consequences of a cyberattack, forensics, attribution, etc. This type is designated here as 'operational cooperation';
- At the second level is the coordination in the development of cybersecurity capabilities by using the available and newly provided human, material and financial resources, introducing standard operating procedures, standards and other common requirements to the required competencies, procurement of technical means and systems, education, training and exercises, etc. This level is designated as *"coordinated (capability) development."*

The six models are called *"basic"* since they are described only through some of their main characteristics. To be implemented, the chosen model needs to be developed in detail and adapted to the respective normative, organizational and cultural context. It can be assumed that each model will include some type of public-private partnership, will seek ways to counter hybrid and other threats, etc. Such details were not examined in the study.

Model A: Enhancement of the Current Model

Model A reflects the current cybersecurity architecture (prior to the implementation of the cybersecurity law). Key cybersecurity responsibilities are assigned to existing organizations, e.g., the Directorate for Countering Organised Crime at the Ministry of the Interior leads in countering cybercrime as well. The model evolves in time and improves, for example, by

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

developing and agreeing on procedures for the exchange of information between two or more of the agencies with cybersecurity responsibilities, introducing common qualification requirements for positions in the administration, supporting education programs in universities, organization of training courses and exercises, certification of key personnel, etc.

Model B: Operational Cooperation

Model B reflects the current national cybersecurity organization amended with mechanisms for operational coordination, envisioned in the national cybersecurity strategy and the cybersecurity law. The organizations with key responsibilities for different sectors of interest (defense, law enforcement, etc.) interact continuously and coordinate their activities for monitoring and maintaining a common picture of the cyberspace, early warning, coordinated reaction in a cyber incident or crisis, consequence management, investigation of incidents and identification of the culprits. A National Cyber Situation Center is established to support operational cooperation.

Model C: Coordinated Capability Development

Model C builds upon Model B, adding to the operational cooperation the coordinated use of agency and common resources for creating the spectrum of needed cybersecurity capabilities. That may include investments in the research and development capacity, the application of technical measures and procedures for better protection of networks and information resources, testing, certification, qualification, joint exercises, and other measures.

This model envisions establishing a National Coordinating Cybersecurity Network, which formulates and suggests to the ministerial-level Security Council (or a Cybersecurity Council, not existing at current) common measures, priorities, and policies covering, among others, budgeting and investment issues.

In both Model B and Model C the national-level cybersecurity architecture remains distributed, but the degree of coordination between responsible agencies is increased. A small administrative unit—the National Cyber Situation Centre—is created in Model B, while model C adds a consultative body – a National Coordinating Cybersecurity Network.

The following two alternatives envision increased centralization.

Model D: State Agency *"Cybersecurity"*

Model D foresees the creation of a new state agency focused entirely on cybersecurity. It will support the Security Council (an executive body chaired by the Prime Minister) in formulating national cybersecurity policies, will coordinate and perform activities for the implementation of such policies. This agency will have both operational and oversight functions in the provision of cybersecurity, including in countering cybercrime and cyber espionage, cyber defense activities and the protection of critical infrastructures and strategic assets, and cryptographic security.

This agency will bring together the best experts in the administration on information, network, communication, and cryptographic security. It will perform the functions of a national incident response center (CIRC) and maintain a response team (CERT) servicing all organizations in need.

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

Model D builds on the evolution of the national-level cybersecurity architecture towards centralization, paralleled with specialization on all security issues related to cyberspace. The agency will be clearly positioned as a component of the national security system.

Model E: State Agency *"e-Government & Cybersecurity"*

According to Model E, the existing State e-Government Agency will perform, in addition to its *"civilian"* responsibilities, the functions of the agency in Model D. New units will be added to its current organizational structure, and they will undertake the new functions and tasks.

In this model, the best IT specialists in the administration will be concentrated in one agency performing both *"civilian"* tasks and functions for the protection of national security.

Model F: Outsourcing to a Lead Company (*"National Champion"*)

The performance of the main functions in guaranteeing cybersecurity is assigned to a lead company with highly qualified and cleared personnel (i.e., having access to classified information). It will support all leading cybersecurity players. At the same time, the company applies its expertise to support policy-making and the decisions on allocating budgetary resources for investments in the development of cybersecurity capabilities.

Ranking the Alternatives

The Analytic Hierarchy Process (AHP), developed by Thomas L. Saaty in the 1980s (Saaty, 2010), was selected for evaluation of the alternative architectures. AHP represents a model of natural human reasoning in ranking and selecting one among a number of alternative options. It has been used widely in sociological, ecologic, economic, and security studies.

Individual expert evaluations are used to rank the basic alternative models. To solicit the expert views, we used a nine-degree scale for pairwise comparison of criteria and alternative models. First, for each of the five criteria, the expert presented his or her preferences for each pair of alternative architectures. Then we asked the interviewees to assess the degree of importance in each pair of criteria.

An interview lasted between 45 and 75 minutes, depending on the interest of the respondent. A four-page summary of the purpose of the study and descriptions of alternative architectures and criteria for their evaluation were e-mailed to the expert in advance. During the interview, conducted *in vivo* or via phone, the interviewer was filling in the response in an Excel file and tracking at the same the consistency of the assessments calculated automatically via the maximum eigenvalue of the matrix of comparisons (Mu & Pereyra-Rojas, 2017b).

In total, 88 experts were interviewed. Thirty-nine of them came from the administration, 29 from academia, and 20 from the business sector. The following section presents a summary of the results.

RESULTS

The section presents first the ranking of the criteria, followed by the ranking of alternative organizational models for each criterion, and finally, the overall ranking of the models based on the expert assessments.

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

Ranking the Criteria

In the average evaluation of the criteria's importance, Effectiveness and Resilience come on top, with a slight preference for Effectiveness (Figure 1). Agility comes third with a weight of 18 percent, followed by Efficiency and Cooperation with roughly 14 percent each.

The ranking of the criteria among the groups of experts does not differ much (Figure 2). It can be noted nevertheless that the experts from the administration give relatively higher importance to Efficiency, researches underline Resilience and Agility, while the business sector clearly prefers Effectiveness.

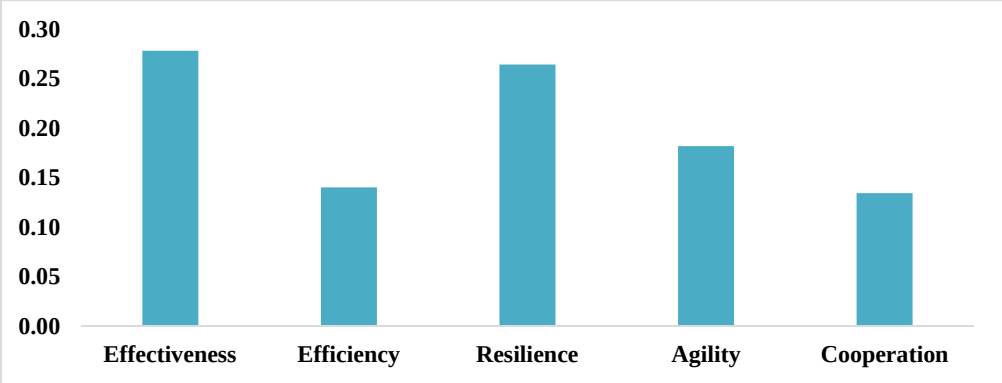
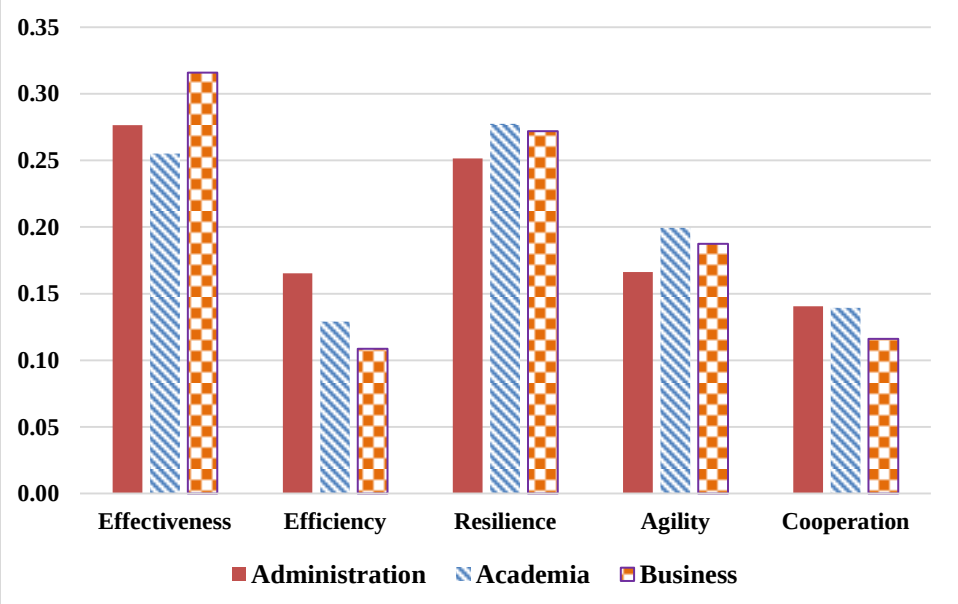


FIGURE 1
OVERALL RANKING OF THE CRITERIA



Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

FIGURE 2
RANKING OF THE CRITERIA BY GROUPS OF EXPERTS

Ranking the Alternatives per Criterion

Figure 3 presents the relative ranking of the alternative cybersecurity models along each of the five criteria. Model C of coordinated capability development ranks highest according to all criteria, and the current organizational arrangement (Model A) has the lowest ranking. Not surprisingly, the organization centered on outsourcing cybersecurity capabilities to a *"National Champion"* (Model F) ranks rather high in terms of agility.

If we combine the ranking of the cooperation-oriented models (B and C) on the one hand and the centralization-oriented models (D and E) on the other, the centralization-oriented ones rank a little higher in terms of effectiveness. However, the cooperation-oriented models exceed along the other four criteria respectively by 7.6, 7.9, 3.5, and 5.3 percentage points.

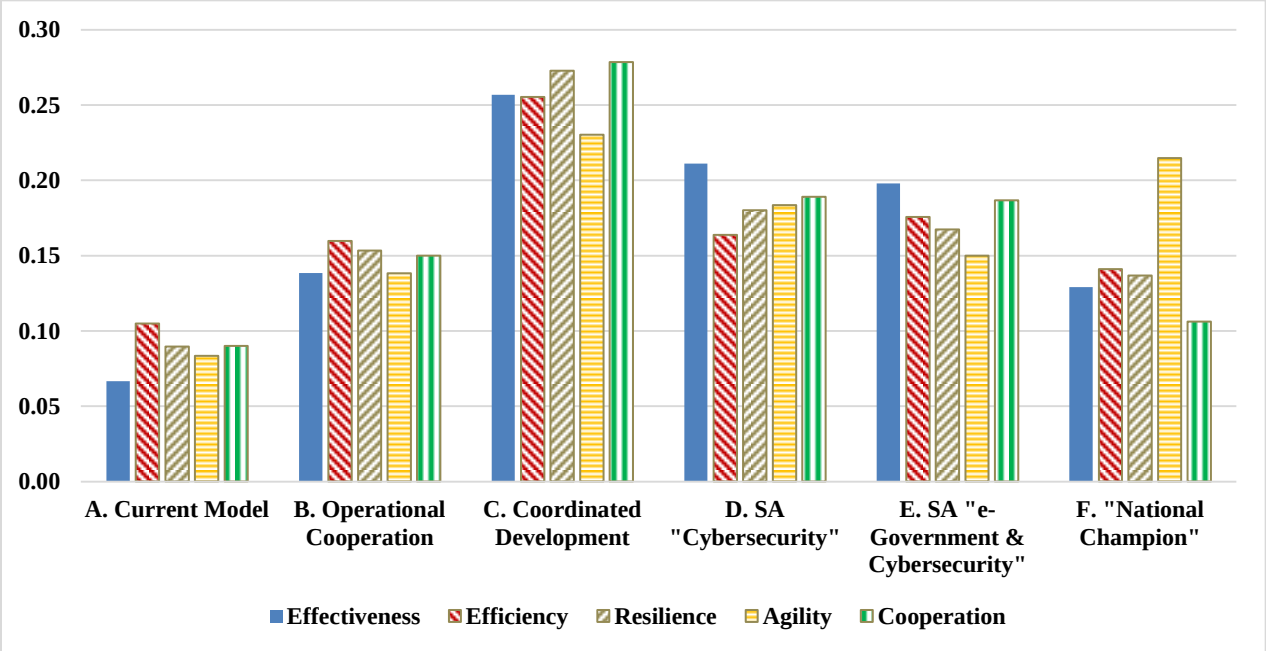


FIGURE 3
RANKING OF ORGANIZATIONAL ALTERNATIVES PER CRITERION

Overall Ranking of the Alternative Architectures

The overall ranking based on averaging the assessment of all interviewees is presented in Figure 4. Model C clearly exceeds all other alternatives, with Model D coming second. The combined ranking of the cooperation-oriented models surpasses that of the centralization-oriented models by 4.6 percentage points.

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

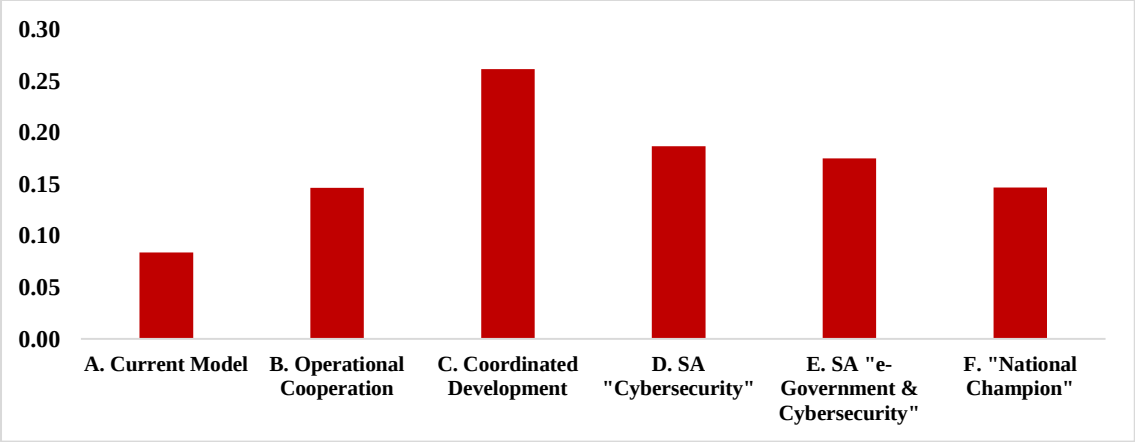


FIGURE 4
OVERALL RANKING OF THE ALTERNATIVE ARCHITECTURES

There are no substantial differences in the ranking of the alternatives by the three groups of experts. It is worth noting that experts from the administration rank Model E relatively high, primarily at the expense of Model F. The latter observation is indicative of the experts' anxiety related to corruption risks – a point that came up repeatedly during the interviews.

DISCUSSION

The application of the AHP method provided the statistical significance of the results that allows drawing some conclusions.

First, in almost all individual assessments, the current cybersecurity architecture of loosely coordinated players is the least preferred. The views on the current architecture express frustration among the experts due to significant gaps in the cooperation among the main actors and the persistent rivalries between them.

Second, Model C, which combines operational cooperation with coordination among all key players in developing cybersecurity capabilities, is clearly the most preferred. It ranks highest in the evaluations of all groups of experts.

Third, among the architectures involving increased centralization, a slight preference is given to Model D, i.e., the creation of a cybersecurity agency. The possible creation of a mega-agency (Model E), combining the development of online public services with cybersecurity responsibilities, worries many of the senior experts.

Fourth, the cooperation-oriented models are preferred even when the rankings of models B and C, on the one hand, and D and E, on the other, are combined. This preference is strongest in evaluating their potential contribution to cyber resilience, which is in the focus of Bulgaria's cybersecurity strategy (Sharkov, 2016).

Finally, the views of the interviewed experts are aligned with the national cybersecurity strategy that prescribed mechanisms for operational cooperation and coordination in the development of cybersecurity capabilities with the least administrative burden.

A question of particular interest is, *"why then the implementation of the strategy stalled?"* The answers may be in the lacking traditions of transparent discussions involving all

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

main stakeholders and evidence-based decision making, as well the more general national culture.

According to Geert Hofstede's six-dimensional model of defining national cultures (Hofstede et al., 2010), Bulgaria ranks rather high in two dimensions. First, it scores 70 along *"power distance,"* which means that centralization is popular, hierarchies are seen as reflecting inherent inequalities, and the people accept a hierarchical order where everybody knows and accepts their place and without requiring further justification. The second dimension of interest is *"uncertainty avoidance,"* where Bulgaria gets a very high score of 85. This indicates that people are generally intolerant of unconventional ideas and tend to resist innovation (Hofstede Insights, 2021).

These cultural specifics have already impacted the search for national cybersecurity arrangements and most likely will affect the future evolution of the cybersecurity organization at the national level.

The Jury is Still Out

The first national cybersecurity strategy, *"Cyber Resilient Bulgaria 2020,"* approved by the Council of Ministers in 2016, is one of the first such documents with a focus on cyber resilience at organizational, sectoral, and national levels envisioning mechanisms for comprehensive cooperation and coordination among all stakeholders. Experts from the US, UK, Israel, and other countries assessed advanced drafts of the document as mature and sophisticated (Interview, 2021).

The strategy was officially approved in 2016. It envisioned a rigorous transition to a higher level of maturity of the national cybersecurity and resilience (Sharkov, 2020), achieved to a large extent through the cooperation and coordination among institutions with distinct yet overlapping responsibilities and capabilities. However, instead of implementing the strategy, soon the focus shifted to the elaboration of a new cybersecurity law, which largely mimicked the EUNIS Directive.

In parallel, the function of the national cybersecurity coordinator was transferred from a member of the political cabinet of the defense minister to a senior officer from the Countering Organised Crime Directorate of the Ministry of the Interior, and then to the Deputy Chair (currently Chair) of the State e-Government Agency.

These facts indicate that institutional rivalries are alive and strong, while it is hard to note any significant advances in practice. Two examples support the latter statement.

At the time of finalizing this article, Bulgaria launched its regular census. The most recent census, conducted in 2011, provided an opportunity for online participation, and it was met with significant interest. The expectation is that the majority of citizens will use the online option during the 2021 census. Yet, the dedicated server of the National Statistical Institute (NSI), https://census2021.bg/, was attacked on the first day of the census. This attack was officially denied by the State e-Government Agency (Economic.bg, 2021); yet, on the next day, NSI admitted that the online platform is under DDoS attack and *"in the next hours, the access [to the platform] will be difficult or impossible"* (Dnevnik, 2021).

The attack against the census platform is just one among numerous cases and not the most severe one. In 2019, hackers penetrated the databases of Bulgaria's National Revenue Agency (NRA) and stole personal, income, and related data of nearly all adult citizens of Bulgaria. Noisy arrests and accusations followed, but two years later, the arrested have been set

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

free, no accusations have been raised, and no responsible officials have been identified (Georgiev, 2021). The case became known as *"NRA-leaks"* and demonstrated the gaps in the capacity of national institutions to protect sensitive information and properly investigate cyber incidents.

CONCLUSION

In the authors' opinion, Bulgaria has not yet reached the decision on a stable national-level cybersecurity organization. The search for a *'best'* model has not been subject of interest by the political elites. An inquiry of one or more cyber incidents, possibly set under rigorous parliamentarian scrutiny, can trigger the necessary interest.

The study presented in this article can provide a foundation for a substantive discussion and the selection of the organizational model of the national cybersecurity system deemed most suitable. Further studies of this type may help policymakers delve into the details of the selected model and decide on the most appropriate organizational cybersecurity arrangements.

ACKNOWLEDGEMENTS

This study was supported by the National Scientific Program *"Information and Communication Technologies for a Single Digital Market in Science, Education, and Security (ICT in SES),"* financed by the Ministry of Education and Science of the Republic of Bulgaria. The authors gratefully acknowledge the contribution of researchers and experts who participated in discussions of alternative cybersecurity organizational models and the criteria for their evaluation, and in particular that of Associate Prof. Velizar Shalamanov, Institute of Information and Communication Technologies, Bulgarian Academy of Sciences; Associate Prof. Dimitrina Polimirova, National Laboratory of Computer Virology, Bulgaria; Associate Prof. Nikolai Stoianov, Bulgarian Defence Institute; and Dr. George Sharkov, European Software Institute – Center Eastern Europe, Sofia. Furthermore, this study would not have been possible if dozens of senior professionals from the public administration, academia, and the business sector had not dedicated precious time for the interviews.

REFERENCES

Cunliffe, K.S. (2021). Hard target espionage in the information era: new challenges for the second oldest profession. *Intelligence and National Security*, in press.

Dnevnik. (2021). The Electronic Census Temporarily Stopped, 8 September 2021. Retrieved September 19, 2021, from https://www.dnevnik.bg/bulgaria/2021/09/08/4251244_elektronnoto_prebroiavane_vremenno_spria

Economic.bg. (2021). SeGA denied the Hacker Attack against Census 2021, 7 September 2021. Retrieved September 9, 2021, from https://www.economic.bg/bg/a/view/daeu-otreche-hakerskata-ataka-sreshtu-prebrojavane-2021-g

ENISA. (2016). European Union Agency for Network and Information Security. NCSS good practice guide: Designing and implementing national cyber security strategies. Luxembourg: Publications Office of the European Union.

Georgiev, M. (2021). Reprimanded for "NRA-leaks"? Forget It! *Sega*, 23 Match 2021. Retrieved September 19, 2021, from https://www.segabg.com/category-observer/nakazani-za-napliyks-zabravete

Greiman, V. (2018). Cyber espionage: The silent crime of cyberspace. *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018*, 245-251.

Gunneriusson, H. (2021). Hybrid warfare: Development, historical context, challenges and interpretations. *Revista ICONO 14*, *19*(1), 15-37.

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

Haberl, F.J. (2020). The weapons of choice: Terrorist armament culture and the use of firearms in online propaganda and identity-building through cyberspace. *Proceedings of the European Conference on Information Warfare and Security, ECCWS*, 126-135.

Hare, F.B. (2019). Privateering in cyberspace: Should patriotic hacking be promoted as national policy? *Asian Security*, *15*(2), 93-102.

Hofstede Insights (2021). What about Bulgaria?. Retrieved September 9, 2021, from https://www.hofstede-insights.com/country/bulgaria

Hofstede, G., Hofstede, G.J., & Minkov, M. (2005). *Cultures and organizations: Software of the mind* (Vol. 2). New York: Mcgraw-hill.

Interview (2021). Dr. George Sharkov, national cybersecurity coordinator (2014-2017) and chair of the interagency expert working group tasked to develop Bulgaria's cybersecurity strategy, September 7, 2021.

Leinhos, L. (2020). Cyber defence in Germany: Challenges and the way forward for the Bundeswehr. *Connections: The Quarterly Journal*, *19*(1), 9-19.

Lester, P. & S. Moore (2020). Responding to the cyber threat: A UK military perspective. *Connections: The Quarterly Journal*, *19*(1), 39-44.

Libicki, M.C. (2020). Correlations between cyberspace attacks and kinetic attacks. *Proceedings of the International Conference on Cyber Conflict, CYCON*, 199-213.

Mu, E., & Pereyra-Rojas, M. (2016). *Practical decision making: an introduction to the Analytic Hierarchy Process (AHP) using super decisions V2*. Springer.

Mu, E., & Pereyra-Rojas, M. (2017). Understanding the analytic hierarchy process. In *Practical decision making* (pp. 7-22). Springer, Cham.

National Cybersecurity Strategy "Cyber Resilient Bulgaria 2020", approved by a Decision of the Council of Minister, 13 July 2016. Retrieved September 10, 2021, from http://www.cyberbg.eu/

NIST. (2018). *Framework for improving critical infrastructure cybersecurity*, ver. 1.1. Gaithersburg, MD: National Institute of Standards and Technology.

Pala, A., & Zhuang, J. (2019). Information sharing in cybersecurity: A review. *Decision Analysis*, *16*(3), 172-196.

Pappalardo, S.M., Niemiec, M., Bozhilova, M., Stoianov, N., Dziech, A., & Stiller, B. (2020). Multi-sector assessment framework–a new approach to analyse cybersecurity challenges and opportunities. In *International Conference on Multimedia Communications, Services and Security* (pp. 1-15). Springer, Cham.

Paşca, V.R., & Simion, E. (2018). Challenges in cyber security: Ransomware phenomenon. In *Cyber-Physical Systems Security* (pp. 303-330). Springer, Cham.

Paterson, T., & Hanley, L. (2020). Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'. *Australian Journal of International Affairs*, *74*(4), 439-454.

Petrenko, S.A., & Vorobieva, D.E. (2019). Method of ensuring cyber resilience of digital platforms based on catastrophe theory. In *2019 XXII International Conference on Soft Computing and Measurements (SCM))* (pp. 97-101). IEEE.

Pöyhönen, J., & Lehto, M. (2020, June). Cyber security: Trust based architecture in the management of an organization's security. In *ECCWS 2020 20th European Conference on Cyber Warfare and Security* (p. 304). Academic Conferences and publishing limited.

Quayle, E. (2020). Online sexual deviance, pornography and child sexual exploitation material. *Forensische Psychiatrie, Psychologie, Kriminologie 14*, 251-258.

Saaty T.L. (2010). *Mathematical principles of decision making: The complete theory of the analytic hierarchy process*. Pittsburg, PA: RWS Publications.

Shalamanov, V., Hadjitodorov, S., Tagarev, T., Pavlov, N., Stoyanov, V., Geneshky, P., & Avramov, S. (2005). Civil security: Architectural approach in emergency management transformation. *Information & Security: An International Journal*, *17*.

Sharkov, G. (2016). From cybersecurity to collaborative resiliency. *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig'16)*, 3-9.

Sharkov, G. (2020). Assessing the maturity of national cybersecurity and resilience. *Connections: The Quarterly Journal*, *19*(4), 5-24.

Simon, S., & de Goede, M. (2015). Cybersecurity, bureaucratic vitalism and European emergency. *Theory, Culture & Society*, *32*(2), 79-106.

Sotelo Monge, M.A., & Maestre Vidal, J. (2021). *Conceptualization and cases of study on cyber operations against the sustainability of the tactical edge.*

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.

Tabansky, L. (2020). Israel defense forces and national cyber defense. *Connections: The Quarterly Journal, 19*(1), 45-62.

Tagarev, T. (2020). Towards the design of a collaborative cybersecurity networked organisation: Identification and prioritisation of governance needs and objectives. *Future Internet*, *12*(4), 62.

Tagarev, T., & Ratchev, V. (2018). Evolving models of using armed forces in domestic disaster response and relief. *Information & Security: An International Journal*, *40*, 167-180.

Weiss, M., & Biermann, F. (2021). Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform*, 1-18.

Citation Information: Tagarev, T., & Rizov, V. (2022). Alternative models of national cyber security organization: Comparative evaluation. *Academy of Strategic Management Journal, 21*(1), 1-15.