A Framework of Partnership

Professor Jim Q. Chen, Ph.D.

ABSTRACT

The persistent engagement strategy in cyberspace requires partnership between the public and private sectors. This whole-of-society approach is greatly needed, as cyber threats are holistic. Partnership can yield a number of good outcomes that all parties seek to achieve. However, having truly productive partnership requires a significant amount of time and effort. There are different partnership methods that ask for different amount of time, effort, and resources. Hence, it is crucial to have a better understanding of the requirements of each partnership method. To this end, this article proposes a framework that incorporates various partnership methods with aims to achieve various goals. It demonstrates that this framework can provide guidance for selecting an appropriate partnership method based on specific conditions, needs, and requirements.

I. INTRODUCTION

In an interview with the *Joint Force Quarterly*, U.S. Cyber Command Commander General Paul Nakasone[1] emphasizes the importance of partnership in persistent engagement strategy. He states that "enabling our partners is two-thirds of persistent engagement. The other third rests with our ability to act – that is, how we act against our adversaries in cyberspace. Acting includes defending forward." Likewise, U.S. Presidential Policy Directive 41 (PPD-41)[2] specifically addresses coordination in dealing with cyber incidents, especially coordination between and among federal agencies as well as coordination between the public and private sectors. It directs inclusion of critical private-sector stakeholders within Cyber Unified Coordination Groups (UCG) when significant cyber incidents occur.

Without a doubt, partnership effort is needed for successful cyber defense, including forward defense, because cyber threats are threats to the society as a whole. Victims of cyber attacks range from government agencies to private companies and individual citizens. In order to disrupt or halt malicious cyber activity at its source and degrade said activity before it can reach its intended victim, all relevant parties should be engaged. This common defense calls for partnership across all sectors of society, but especially between the government and the private sector. The efforts from the government and the private sector are complementary. No effort from any party will lead to the failure of the overall defense.

Partnership, especially partnership between the government and the private sector, is the key to enhance capability and provide resilience in cyber defense. However, it is always a challenge to establish and maintain partnership because partnership is built on trust, which requires time. The unique relationship between the two sides also needs to be maintained. Both sides should "give" in order to "take," as partnership ought to have proportional investment from both sides. Before entering into a partnership relationship, both sides should have a clear understanding of the types of methods and the relevant effort required. In this way, both sides know what is expected in this relationship. As a matter of fact, there is no structured guidance to nurture such an effort. This article attempts to bridge this gap by proposing a framework that incorporates various partnership methods between the government and the private sector. It assumes that these methods sit on varied points of a partnership spectrum to support varied goals. This framework helps to address the following questions: What are the different types of partnership methods? What is involved in each method? How can an effective partnership between the government and the private sector be developed? Ultimately, this framework provides guidance for the selection of an appropriate partnership method in a specific environment. The guidance provided is based on specific conditions, needs, and requirements.

In the following sections, an analysis is performed, revealing what is missing in the current approach to partnership. Then, a framework that consists of a spectrum of various partnership methods such as cooperation, collaboration, and integration is proposed. The advantages of this new approach are discussed, and future research is also recommended.

2. ISSUES

The public-private partnership has been a cornerstone in the U.S. national cybersecurity strategy for the most recent administrations[3, 4, 5, 6] as well as in the U.K. national cybersecurity strategy[7]. As mentioned by Carr[8], the public-private partnership has also been included in national cybersecurity strategies in many other countries in the world. This shows the importance of the public-private partnership and the emphasis that many governments have placed on it.

There are several reasons for the promotion of the public-private partnership. At least the following three reasons have to be mentioned: (1) Critical infrastructure is mainly owned, managed, and operated by the private sector in the U.S. and in some other countries. In an environment like this, the government has to work closely with the private sector, i.e. the owners, the managers, and the operators, in order to protect critical infrastructure. U.S. Presidential Policy Directive 21 (PPD-21)[9] identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems. These sectors are mainly owned, managed, and operated by the private sector. (2) Victims of cyber attacks are from all walks of life. The whole-of-society strategy requires all sectors of society be engaged in cyber defense, both public and private. Absence of one sector may lead to some unexpected consequences. (3) The government may possess specific information on threats and vulnerabilities. Sharing this information with the private sector may help enhance its specific defense posture before real attacks occur. The private sector may also hold some specific pieces of information about attacks for the compromised networks that it owns and manages. Sharing these with the government may help the government gain a comprehensive view of cyber attacks in its country, allowing for effective countermeasures at the national level to be designed and launched. In this respect, the exchange of information may benefit both sectors in enhancing cyber defense posture.

However, it is never an easy task to implement a public-private partnership. As mentioned by Blacker[10], "national cybersecurity guidance mandates collaboration, but does not speak to (nor should it) how to actually collaborate." Besides, there are some issues in the current approach to a public-private partnership. These issues are examined below.

First, responsibility and accountability are not clearly defined. As a result, mutual trust is difficult to maintain, and chaos may occur time and again. Without appropriate coordination, one side may accidentally step on the toes of the other side, and both sides may flinch at performing a task at another time. What is worse, both sides may refuse to accept any responsibility when something goes wrong. At the end, it becomes hard to hold anyone accountable, and the partnership may collapse.

Second, the common ends, ways, and means of a partnership are not often considered. Consequently, the partnership becomes aimless. No good strategy is figured out. Neither side knows why, how, or what should be done in order to make the partnership work successfully.

Third, the differences between the two sides are not well considered, not mentioning the different goals that the two sides have. Without reconciling these goals, it is difficult to build a shared work platform. As pointed out by Carr[11], the government is politically focused, as it is more concerned about the common public good and national security. It employs a hierarchical, or vertical, management structure. However, the private sector is more concerned about profits for enterprises. The private sector has full ownership of enterprises. To achieve its business goals, i.e. to make business efficient and profitable, a horizontal management structure is employed. In Wettenhall[12]'s term, a horizontal management structure is characterized by consensual decision-making, while a hierarchical management structure is characterized by having one side in a controlling role.

To summarize, the current approach to the public-private partnership lacks responsibility and accountability; lacks common ends, ways, and means; and lacks effective modes of reconciliation. The issues are associated with "a persistent ambiguity with respect to the parameters of such a partnership," just as Carr[13] states. As neither side has a clear view of what should be the give and take, the partnership becomes an ad hoc endeavor. As a consequence, the partnership cannot achieve what it is expected to achieve.

To deal with these issues, the scope of involvement in a partnership should be explicitly defined. In the next section, a framework comprised of various partnership methods is proposed, and each method is explored.

3. A FRAMEWORK OF PARTNERSHIP METHODS

The framework of partnership proposed here should be able to address the three issues discussed above, so that each side knows what is expected of them before it enters into a partnership. The framework consists of a spectrum containing various partnership methods, such as cooperation, collaboration, and integration. Each method is associated with different roles and responsibility as well as ends, ways, and means. The framework helps to understand the give and take of each method.

There exist many partnership methods. Here, in this research, three major ones are focused on. These are: cooperation, collaboration, and integration. These three methods sit on varied points on a partnership spectrum. Within this spectrum, cooperation requires the least effort from both sides, while integration requires the most effort from both sides.

The high-level representation of the spectrum is displayed in Figure 1 below:

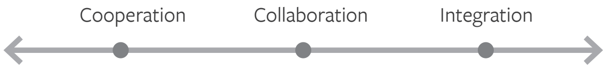

Figure 1. Spectrum of different partnership methods

In a cooperative relationship, a horizontal management structure is maintained. Both sides are independent from each other, even though they have a common task to accomplish. No roles or responsibilities are clearly assigned to relevant team members. No formal procedure is followed. There is no special budget for a task in most cases. Both sides may put resources together whenever needed. The relevant people from both sides work together in an informal environment whenever needed. This relationship is symbolically represented below:

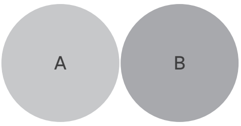

Figure 2. Cooperation

A voluntary, cyber-related, information-reporting mechanism is an example of cooperation. A government agency may acquire a critical piece of information from a private-sector company, which, in return, may receive useful pieces of advice for cyber defense from a government agency. Both sides may benefit from this mechanism, but neither side is in absolute control. Besides, neither side needs to have a big investment for the use of this mechanism.

In a collaborative relationship, a horizontal management structure is maintained. Both sides remain independent from the other while they take on a common task. They select people from both sides to form a special group to work together on a particular task. Both sides are in charge. Roles and responsibilities may or may not be assigned. People from both sides form a group and work together in an informal environment. A special budget may or may not be allocated. Both sides may put resources together whenever needed. This relationship is represented below:

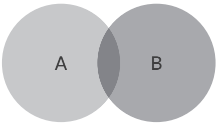

Figure 3. Collaboration

An active threat intelligence-sharing group is an example of collaboration. It involves stakeholders and participants, such as national security agencies, law enforcement agencies, cybersecurity industry companies, non-cybersecurity commercial companies, and other relevant actors. Well-established, cyber-focused, public-private collaboration in current practice includes, but is not limited to, Information Sharing and Analysis Centers (ISACs), automated indicator sharing though Structured Threat Information Expression (STIX), Trusted Automated Exchange of Indicator Information (TAXII), and the Cyber Information Sharing and Collaboration Program (CISCP). Personnel and resource investment is required to support these efforts, which are beneficial for all stakeholders and participants.

The true public-private collaboration in Healey[14]'s framework falls into this category, as joint governance is guaranteed and personnel exchange is supported.

In an integrative relationship, one side absorbs the other side into its organization. Now, one side is in total control. A horizontal management structure changes into a hierarchical management structure. Those who work on a task form a special unit of the organization. They work in a formal environment. A formal procedure is followed. A special budget is allocated. Resources are provided. Bureaucracy may be developed in some cases. This relationship is represented below:

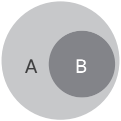

Figure 4. Integration

Having groups of employees from the private sector embedded into a government cyber operation organization as individuals or as new units is an example of integration. In this environment, employees from the private sector have to strictly follow the instruction of the government organization in order to support the mission.

The government-led approach in Healey[14]'s framework falls into this category as the government maintains the total control. Private-sector employees who join the government efforts are compelled to follow all government policies and regulations. All the maneuvers are orchestrated in order to accomplish missions.

Likewise, the private-led approach in Healey[14]'s framework also falls into this category. In this environment, one private-sector company is taking the lead. It thus has full control and final say in operations.

Several factors have to be considered when analyzing these partnership methods. One factor is the promotion of trust. Any relationship will not last if there is no mutual trust. Osborne[15] is an advocate for trust. He maintains that trust can help to develop a "mutual belief in the positive gains of both partners." This belief can serve as the motivation for partnership efforts. Manley[16] echoes the same view. He takes one step further and makes trust the foundational level for his proposed public-private partnership model.

Another factor is the assignment of responsibility. If specific roles and responsibilities are not assigned to relevant people, the leadership of a group cannot be empowered; communication within the group cannot be enhanced; relationships inside the group cannot be improved; reliability cannot be guaranteed; and accountability cannot be assured when something goes wrong.

Still another factor is the employment of checks and balances. If a task is led by one entity, checks and balances are seldom conducted. However, if it is led by two entities, while one entity performs the task, the other entity can play the role of checks and balances. These roles are interchangeable while the function of checks and balances is still maintained. Meanwhile, transparency and due process or fairness should be guaranteed.

In Eichensehr[17]'s assertion, without "accountability, transparency, and due process or fairness," the partnership effort will fall short of "public law values."

One more factor is the adoption of the bottom-up approach, which encourages voluntary partnership and should be utilized. It is the opposite of the top-down approach. As pointed out by Osborne[15], the top-down approach, which is the "rigid set of formal partnership" set up on strict "legal binding contract(s)" and mainly controlled by one side, discourages teamwork and reduces efficiency. This approach, which may be used in integration, is not suitable for cooperation and collaboration.

Still one more factor is the allocation of a dedicated budget. Without sufficient funding and resources, it is hard to get a task completed. In an integrative environment, there is one budget authority. Hence, the decision-making is relatively less complicated. As long as there is a budget available and the priority is set for a task, the task will be funded and relevant resources will be accessible. However, in a cooperative environment or a collaborative environment, there are at least two budget authorities. Each entity may have different budget rules and regulations to follow. Consequently, having the task funded from two sides is not an easy undertaking at all.

These are just some of the factors that ought to be considered in deciding how to structure a partnership venture. In the following discussion, these factors and other relevant factors are analyzed. When all these factors are compiled into a set of features, the differences among various types of partnership methods are easily seen. Below is the list of the factors: the type of trust, the type of organizational structure (org structure), whether the leadership or the command and control (C2) for partnership is established, whether the responsibility is assigned, whether the liability of partnership is made known, the type of relationship endorsed, the type of communication used, whether the checks and balances are employed, whether a dedicated budget is allocated, whether relevant resources are made available for partnership effort, the type of approach taken, whether a common process is utilized, whether a dedicated team is set up, whether a common goal is clearly known by everyone involved, whether a shared strategy is formulated, and whether some dedicated tools are identified and utilized. In the table below, the differences in these factors among these three types of partnership methods are listed.

Table 1. Differences among the three types of partnership methods

Factors	Cooperation	Collaboration	Integration
Trust	May or may not have	May have	Have
Org structure	Horizontal	Horizontal	Hierarchical
Leadership/C2	Not designated	May be designated	Designated
Responsibility	Not assigned	May be assigned	Assigned
Liability	Not known	May be known	Known
Relationship	Very loose	Loose	Tight
Communication	Horizontal	Horizontal	Hierarchical
Checks-and-balances	May have	Have	Not have
Budget & Resources	Not allocated	May be allocated	Allocated
Approach Taken	Bottom-up	Bottom-up	Top-down
Common process	May or may not have	May have	Have
Dedicated team	May or may not have	Have	Have
Common goal	May or may not have	May have	Have
Shared strategy	May or may not have	May have	Have
Dedicated Tools	May or may not have	May have	Have

As shown in Table 1, cooperation, in general, provides a loose and informal working environment. Specifically, the cooperators work in an informal and horizontal management environment, in which they can choose their own ways of performing a task. They do not care too much about leadership and responsibility for a task. Their informal communication is smooth. While cooperating, the bottom-up approach is utilized. They may not have a special and dedicated budget. There is no common process to follow. As they are all task-oriented, they may not have a common long-term goal and shared strategy, and they may not use commonly dedicated tools.

The table above also clearly shows the parameters of collaboration. In general, collaborators still have flexibility in an informal but motivated work environment. Specifically, the collaborators can still work in an informal and horizontal management environment, in which they are motivated to take the lead and take responsibility. As they are in an informal relationship, they may easily communicate with each other. Within this environment, checks and balances are employed; the bottom-up approach is utilized; a special and dedicated budget is approved; and a dedicated team with people from both sides is formed. In addition, the collaborators may have the same common goal and the shared strategy; they may use the same dedicated tools.

Besides, the table reveals the characteristics of integration, which, in general, creates a formal working environment that is better managed with less flexibility offered. Specifically, people work in a formal and hierarchical management environment. They are in a formal relationship. The communication reflects a hierarchical structure. Within this environment, employing an outside organization to conduct checks and balances is usually not an option for various reasons; the top-down approach is utilized; a special and dedicated budget is approved and used; and a dedicated team with dedicated management is formed. Besides, people in a team have the same common goal and the same strategy. They use the same dedicated tools.

It is evident that this analysis, with the help of these relevant factors, can successfully reveal the differences among these three types of partnership methods. After a careful analysis, one may find out that these factors fall into three major categories, i.e., leadership, strategy & implementation, and resources. The relationship among these three categories is shown below:

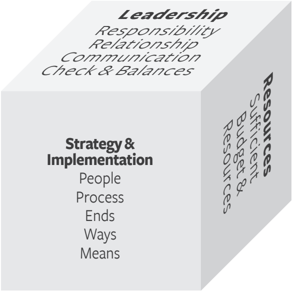

Figure 5. Three categories of factors that determine different types of partnership methods

The parameters of these three categories determine the differences of the partnership methods, which obviously have different levels of requirements for partnership effort. Based on the mission, requirements, needs, and severity level of the environment, an organization can now pick and choose an appropriate partnership method with the help of these three categories of factors. The guidance provided by the proposed framework definitely speeds up the selection process.

The level of severity in an environment also has a say in the selection of an appropriate partnership method. For instance, if the severity level is low, the cooperation method is preferred in most cases. If the severity level is medium, the collaboration method is usually selected. If the severity level is high, the integration method is typically chosen.

For instance, in a national security crisis, an integrated task force needs to be formed and put into action. Within this formal working environment, the hierarchical management is practiced. So is the top-down approach. There is little to no flexibility. With the same goal and strategy and with a dedicated budget, the chance of success for the mission is greatly increased.

This proposed framework can not only distinguish different types of partnership methods with the help of the list of factors but also provide guidance for selecting an appropriate partnership method based on specific conditions, needs, and requirements. In the next section, the advantages of this framework are discussed, and future research is also recommended.

4. DISCUSSION

The proposed framework is able to offer several advantages. First, it clearly differentiates three types of partnership methods. Being aware of the parameters of each method, one can quickly make a decision of which partnership method should be chosen based on one's mission, requirements, needs, and the severity level of the environment. This can serve as a useful decision-making instrument for leaders.

Second, it fully utilizes the effective leadership skills. Building trust, delegating leadership roles and responsibility, encouraging communication, providing a flexible, informal but motivated working environment, adopting the bottom-up approach, and offering financial support are just a few good examples. All these give people in the private sector incentive to actively engage in helping the common public good and national security. They become motivated rather than being forced to share their talents and commit resources. As a result, a strong bond is created between the government and the private sector in handling the challenges in national security. Also, given this framework, the "power over personnel and resources," in Alford and Greve[18]'s term, can be shared; the state of partnership as power sharing, as Linder[19] calls it, can be achieved; control and governance, in Bochoven[20]'s term, can be increasingly shared and collaboration boundaries can thus be broken; and the role of the private sector, as Carrapico and Farrand[21] argue, can be changed "from objects of regulation to regulation shapers."

Third, it promotes the best practice in strategic thinking. On one hand, it lets partners from both sides figure out a common goal and a shared strategy. It can bring partners with different backgrounds together in tackling the same challenges with their unique talents and perspectives. This joint effort can yield unexpected results in figuring out effective solutions. Naturally, this can successfully address the issue of lacking clear objectives and the issue of "wide gaps between public and private sector expectations," as discussed by Zhang[22]. On the other hand, tools like checks and balances can be employed to prevent, detect, and correct errors, issues, and problems while promoting professional environments.

Fourth, it helps to develop leaders who will be efficient and effective in leading partnership efforts in any environment. Specifically, the framework enables leaders to improve three skills essential for leadership, i.e. technical skills, human skills, and conceptual skills. The three-skill approach is the essential component of Katz[23]'s model in leadership research. It also helps leaders learn how to work with common, diverse, or conflicting goals while "being both participative and authoritative" in a partnership effort, as suggested by Connelly et al.[24] as well as O'Leary and Vij[25]. Ultimately, it provides them with an environment in which they can practice "compromises, humbleness, broad-mindedness, ability to work in settings where power is dispersed, and also high conceptual skills (e.g. working with visions and abstractions)," as recommended by Uhr[26].

There are some areas that need to be addressed. As the framework proposed in this article is at a high level, the inner-workings and details at the low level need to be worked out, especially for collaboration. Besides, this framework has not been tested in real-world environments yet. In addition, metrics have not been developed to measure the effectiveness of this framework.

Hence, future research should be focused on figuring out the inner-workings and details at the low level as well as metrics that can be used to evaluate and measure the effectiveness of the framework. Once done, the framework needs to be tested in various real-world environments to find out its real practical value. Meanwhile, the framework needs to be assessed and its effectiveness needs to be measured and evaluated.

5. CONCLUSIONS

Cyber defense against cyber threats requires the whole-of-society approach, which calls for partnership among the whole society, especially the partnership between the government and the private sector. Partnership can yield a great number of good outcomes for both the common public good and national security. However, it requires leadership, team-building, budget, resources, and strategy. There are different partnership methods for different goals. Without a better understanding of varied requirements for different partnership methods, one may fail to choose the most appropriate partnership method for a specific environment.

To address the issues in the current approach, such as lack of leadership, lack of responsibility, and lack of explicit parameters for partnership effort, a novel framework that incorporates a spectrum of partnership methods is proposed. In the current version, it consists of cooperation, collaboration, and integration. Three major categories of factors—namely leadership, strategy & implementation, and resources—are used to explicitly differentiate the different types of partnership methods. This framework can provide guidance for selecting an appropriate partnership method based on specific conditions, needs, and requirements. Other than these capabilities, this framework is able to fully utilize effective leadership skills, promote the best practice in strategic thinking, and help develop leaders who will be efficient and effective in leading partnership effort in any environment.

Author Bio

Professor Jim Q. Chen, Ph.D.

Dr. Jim Q. Chen, Ph.D. is Professor of Cyber Studies in the College of Information and Cyberspace (CIC) at the U.S. National Defense University (NDU). His expertise is in cyber warfare, cyber deterrence, cyber strategy, cybersecurity technology, artificial intelligence, and machine learning. Based on his research, he has authored and published numerous peer-reviewed papers, articles, and book chapters on these topics. Dr. Chen has also been teaching graduate courses on these topics. He is a recognized expert in cyber studies and artificial intelligence.

ACKNOWLEDGEMENT

The author of this article is grateful to Mr. Antonio Rosa and Dr. Corvin J. Connolly at the Cyber Defense Review (CDR), the Army Cyber Institute (ACI) at the U.S. Military Academy (USMA), Dr. Jeffrey D. Smotherman at the U.S. National Defense University (NDU) Press, Mr. Michael Miklaucic at the U.S. National Defense University PRISM Journal, and the blind reviewers for their helpful comments and suggestions for the previous version of this article. Any error in the article is still the responsibility of the author.

NOTES

1. Editor in Chief of Joint Force Quarterly, (2019), An Interview with Paul M. Nakasone. *Joint Force Quarterly* 92 (1), 4-9.
2. B. Obama, (2016), U.S. Presidential Policy Directive 41 (PPD-41): United States Cyber Incident Coordination. Washington DC: The White House.
3. W. Clinton, (1998), A National Security Strategy for a New Century. Washington DC: The White House.
4. G. Bush, (2003), The National Strategy to Secure Cyberspace. Washington DC: The White House.
5. B. Obama, (2011), International Strategy for Cyberspace. Washington DC: The White House.
6. D. Trump, (2018), National Cyber Strategy of the United States of America. Washington DC: The White House.
7. F. Maude, (2011), The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World. London: Cabinet Office.
8. M. Carr, (2016), Public-private partnership in national cyber-security strategies, *International Affairs* 92, 43-62.
9. B. Obama, (2013), U.S. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, Washington DC: The White House.
10. N. Blacker, (2017), Winning the cyberspace long game - applying collaboration and education to deepen the U.S. bench, *The Cyber Defense Review* 2 (2), 21-30.
11. M. Carr, (2016), Public-private partnership in national cyber-security strategies, *International Affairs* 92, 43-62.
12. R. Wettenhall, (2003), The rhetoric and reality of public-private partnerships, *Public Organization Review* 3 (1), 77-107.
13. M. Carr, (2016), Public-private partnership in national cyber-security strategies, *International Affairs* 92, 43-62.
14. J. Healy, (2017), Who's in Control: Balance in Cyber's Public-Private Sector Partnerships, *Georgetown Journal of International Affairs* 18 (3), 120-130.
15. S. Osborne, (2002), P*ublic-Private Partnerships: Theory and Practice in International Perspective*, London: Routledge.
16. M. Manley, (2015) Cyberspace's dynamic duo: forging a cybersecurity public-private partnership, *Journal of Strategic Security* 8 (5), 85-98.
17. K. Eichensehr, (2017), Public-private cybersecurity, *Texas Law Review* 95, 467-538.
18. J. Alford and C. Greve, (2017), Strategy in the public and private sectors: similarities, differences and changes, *Administrative Science* 7 (35), 1-17.
19. S. Linder, (1999), Coming to terms with the public-private partnership: a grammar of multiple meanings, *American Behavioral Scientist* 43 (1), 35-51.
20. L. Bochoven, (2016), Industry and policy: partnerships in disruptive times, *Connections: The Quarterly Journal* 15 (2), 19-29.
21. H. Carrapico and B. Farrand, (2017), Dialogue, partnership and empowerment for network and information security: the changing role of the private sector from objects of regulation to regulation shapers, *Crime, Law and Social Change* 67 (3), 245-263.
22. X. Zhang, (2005), Critical success factors for public-private partnerships in infrastructure development, *Journal of Construction Engineering & Management* 131 (1), pp 3-14.
23. R. Katz, (1955), Skills of an efficient administrator, *Harvard Business Review* 33 (1), 33-42.
24. D. Connelly, J. Zhang, and S. Faerman, (2008), The paradoxical nature of collaboration, *Big Ideas in Collaborative Public Management*, edited by L. Bingham and R. O'Leary, Armonk, New York: M.E. Sharpe, 17-35.
25. R. O'Leary and N. Vij, (2012), Collaborative public management: where have we been and where are we going? *The American Review of Public Administration* 42 (5), 507-522.
26. C. Uhr, (2017), Leadership ideals as barriers for efficient collaboration during emergencies and disasters, *Journal of Contingencies and Crisis Management* 25 (4), 301-312.