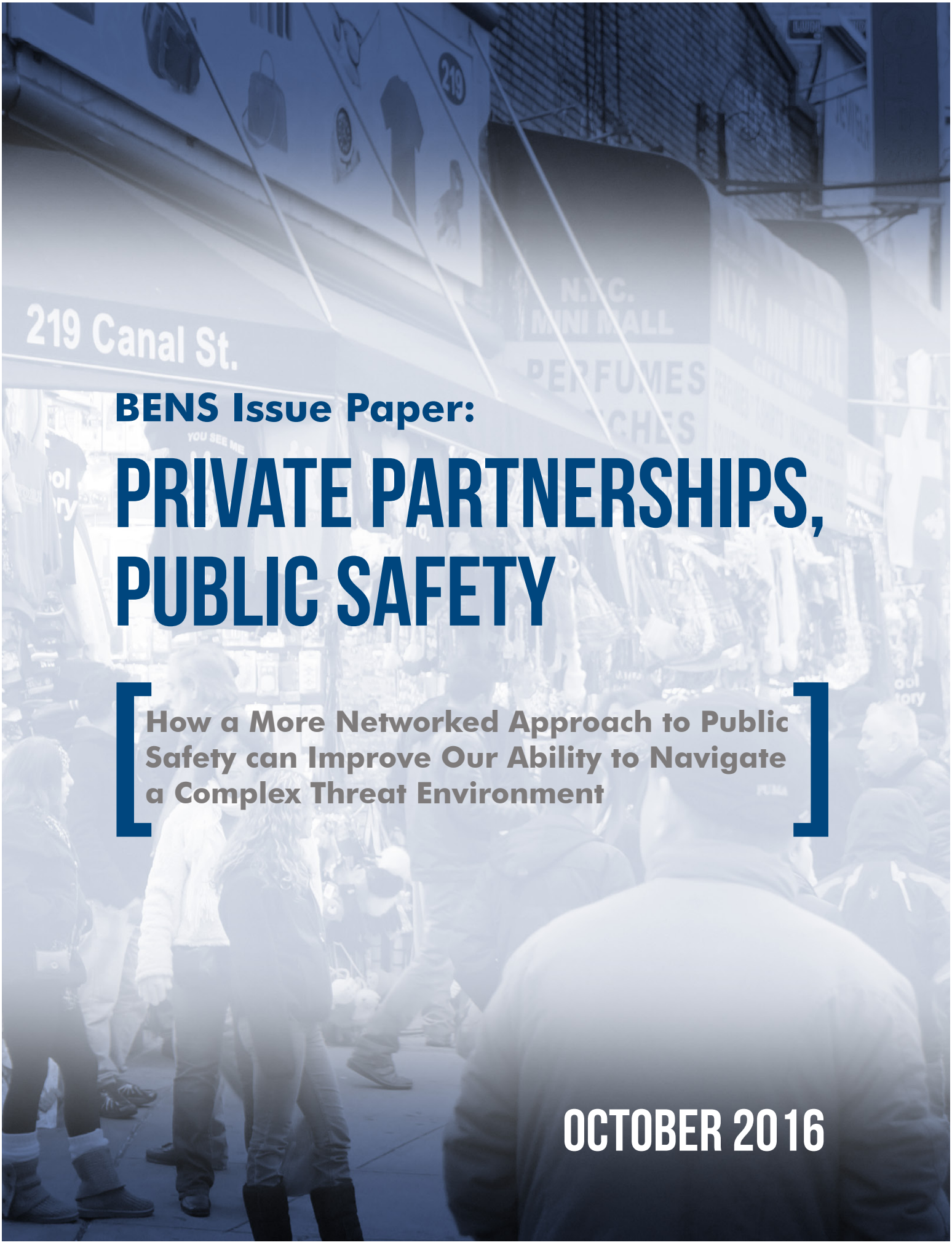


BENS Issue Paper:

PRIVATE PARTNERSHIPS, PUBLIC SAFETY

How a More Networked Approach to Public Safety can Improve Our Ability to Navigate a Complex Threat Environment

OCTOBER 2016

Business Executives for National Security

WHO WE ARE

Business Executives for National Security is a unique nonpartisan, nonprofit organization of senior executives who volunteer time, expertise, and resources to assist defense and homeland security leaders on a variety of national security challenges.

OUR MISSION

Apply best business practice solutions to our nation's most challenging problems in national security, particularly in defense and homeland security.

ACKNOWLEDGMENTS

BENS gratefully acknowledges the expert contributions of our membership, their colleagues, and their staff. We would also like to acknowledge the tremendous assistance received from the senior leadership and the staff of the Department of Homeland Security, Federal Bureau of Investigation, the Office of the Director of National Intelligence, the National Governors Association, and the National Fusion Center Association.

BENS ISSUE PAPER: Private Partnership, Public Safety

BENS Members

Dan Botsch
President
TrapWire Inc.

Norman C. Chambers
Chairman & CEO
NCI Building Systems, Inc.

John Hurley
Managing Partner
Cavalry Asset Management

Dr. Kathleen Kiernan
Founder & CEO
Kiernan Group Holdings

Dawn Scalici
Government Global Business Director
Thomson Reuters

BENS Staff

Thomas Tennant
Director for Emerging Threats

Mitchell Freddura
Senior Policy Associate

Published October 2016

EXECUTIVE SUMMARY

America today is confronted by a complex array of physical threats to public safety. Technological advancements have empowered individual actors at the local level, and successful attacks, such as those in Charleston, San Bernardino, and Orlando, demonstrate an intent to produce a high level of casualties by deliberately targeting privately owned and soft targets. These kind of locally-directed, less-sophisticated attacks cannot be adequately addressed through a solely top-down or one-size-fits-all approach to public safety. Rather, public and private sector leaders must expand and deepen their horizontal partnerships through a more networked approach to public safety. Private sector practices for horizontally integrated and networked business processes may be instructive for how to effectively pursue such an approach while navigating a complex threat environment.

In response to a similarly dynamic global marketplace, many elements of the private sector have embraced a decentralized, flexible, and technologically enabled approach to service and product delivery. These horizontally integrated and networked business processes use information technology to facilitate partnerships among a diverse array of stakeholders who collaborate to create value for discrete customer groups at the local level. Through this approach, functional teams are empowered to effectuate clear organizational missions while being held accountable by attentive leaders who emphasize integration across teams. This paper will examine the private sector trend toward horizontally integrated and networked business processes, and explore their application to US public safety efforts.

A more networked approach to public safety could improve the ability of stakeholders to capitalize on each other's authorities, provide greater visibility into each partner's information supply chain, and enable stakeholders to pursue rapid, flexible responses to perceived threats at the community level. The US public safety architecture is sprawling, composed of entities at the federal, state, and local levels of government, including nearly 800,000 law enforcement officers at over 18,000 departments across the nation. Therefore, organizing an effective and responsive public safety network among these stakeholders requires identifying key nodes and ensuring that they are adequately resourced and connected. This paper focuses on three key nodes in the US public safety network: the private sector, state and major urban area fusion centers, and state Homeland Security Advisors (HSAs), or the comparable executive state-level position.

The following discussion raises key management issues that public and private sector executives may consider in order to sufficiently empower and connect the three key nodes identified above. These issues include: how to identify and overcome barriers to developing effective public-private partnerships, how to adequately value and resource state and major urban area fusion centers, and how to improve coordination among state HSAs.

In keeping with the mission of Business Executives for National Security (BENS), the following discussion is not intended to be overly prescriptive. Rather, it is based on the private sector insight of our national Membership and is meant to complement and support existing public sector efforts. BENS has established itself as an honest broker on these issues through past work on improving the private sector's role in disaster preparation and response and improving domestic security structures and processes. As the United States continues to navigate a complex threat environment, our Members offer a complementary method to their past work, that of a more networked approach to public safety.


F.D.N.Y.

CONTENTS

I. INTRODUCTION

"A Future We Cannot Yet Envision"

America today is confronted by a complex domestic threat environment that is characterized by increasingly decentralized physical and virtual threats to US public safety. To be sure, some of these threats are not new. For example, America has a long history of politically-motivated violence. Modern communication and information technologies, however, have significantly increased the speed and scale of threat propagation. It is now easier for disruptive foreign ideologies to spread and take root in America's communities, or for international events to translate into local acts of violence. Recent physical attacks demonstrate an intent to produce a high level of casualties by deliberately targeting privately owned and soft targets. These attacks also suggest that the existing approach to public safety may not be optimized to effectively detect, prevent, and respond to current challenges.

> "It is at the community level where active physical threats...are likely to have the most immediate impact."

Although it is unrealistic to expect public safety personnel to identify or stop all potential threats, there is room for continuous coordinated improvement. In fact, the same dynamics that are animating today's threats—technological innovation, individual empowerment, and locally directed action—may also prescribe new ways to defend against them going forward. Indeed, to effectively navigate a complex threat environment, law enforcement, homeland security, and private sector stakeholders must adopt an equally decentralized and coordinated approach to public safety. This can be accomplished by expanding and deepening the horizontal partnerships between stakeholders at all levels of government, particularly at the community level, through a more networked approach to public safety.

The US public safety architecture is sprawling, composed of entities at the federal, state, and local levels of government, including nearly 800,000 law enforcement officers at over 18,000 departments across the nation. At the federal level, law enforcement, homeland security, and intelligence agencies operate according to different authorities and pursuant to different mission sets. Moreover, variations in state and municipal statutes, sunshine laws, and political structures prohibit both a federally-directed or one-size-fits-all public safety approach. Therefore, law enforcement and homeland security leaders, in partnership with the private sector, must place greater emphasis on creating a more cohesive and horizontally integrated public safety network that coordinates these varying authorities and organizational structures. Such a network must leverage the United States' federated governing structure as an asymmetric advantage over our adversaries, not as a complicating factor to coordinated action.

A more networked approach to public safety could improve the ability of stakeholders to capitalize on each other's authorities, provide greater visibility into each partner's information supply chain, and enable stakeholders to pursue rapid, flexible responses to perceived threats at the community level. It is at the community level where active physical threats (herein defined as terrorist attacks, active shooter scenarios, and other events that can cause immediate physical harm) are likely to have the most immediate impact. A more networked approach must incorporate the unique capabilities and insight of state, local, tribal, territorial (SLTT), and private sector stakeholders in each community. Improving coordination and de-confliction among all stakeholders will also ensure that US public safety efforts are conducted within transparent legal boundaries and with respect to appropriate civil liberty protections.

Within an ever shifting domestic threat environment, improvement must be pursued as an ongoing and sustained process, rather than a goal that can be reached as if it were a fixed end point. This is undoubtedly difficult. As one law enforcement leader

observed, continuous improvement within a complex environment is "challenging because we're trying to describe a future we cannot yet envision…" However, private sector best practices for implementing horizontally integrated and networked business processes may offer a roadmap for effectively navigating today's threat environment. In response to a similarly dynamic global marketplace, many elements of the private sector have embraced a decentralized, flexible, and technologically enabled approach to service and product delivery.

These horizontally integrated and networked business processes use information technology to facilitate purposeful partnerships among a diverse array of stakeholders who collaborate to create value for discrete customer groups at the local level. Through this approach, functional teams are empowered to effectuate clear organizational missions while being held accountable by attentive leaders who emphasize integration across teams. Such horizontal networks do not completely replace vertical constructs within an organization; rather, they complement them by providing for more efficient value creation and servicing the requirements of senior-level decision-makers in a timelier manner. In trying to describe an undetermined future, this paper offers one potential vision: that of a more networked approach to public safety which embraces private sector best practices for horizontal integration.

Organizing an effective and responsive network among public safety stakeholders requires identifying key nodes in the network and ensuring that they are adequately resourced and connected. There is already considerable movement among federal, state, and local entities toward a more horizontal approach.[a] This paper builds upon the existing momentum and offers ways to further empower three key nodes in the US public safety network: the private sector, state and major urban area fusion centers, and state Homeland Security Advisors (HSAs), or the comparable executive state-level position (e.g. the Director of Public Safety, Director for Emergency Management, or the Adjutant General).

If properly empowered, these nodes can act as force multipliers for the entire network by identifying key patterns among the flood of available data and sharing contextualized knowledge back into and up through the overall network. This obviates the need for every component to receive all available data, as long as every network component has responsive partnerships with the HSAs, state and major urban area fusion centers, and geographically relevant private sector stakeholders. The following discussion elevates key issues which public and private sector leaders must consider in order to adequately empower the key nodes at the center of this discussion. These issues include how to sufficiently value and resource state and major urban area fusion centers beyond simple cost-benefit calculations, and how to improve coordination among state-level leaders.

In order to be effective, the US public safety network must be linked through partnerships with a variety of stakeholders, including the private sector. Today, active physical threats are impacting civilian and privately owned soft targets with greater frequency. Consequently, the private sector is often not only the first casualty of a successful attack, but in some instances is also the best potential early warning system or initial responder before public safety officials arrive. At the same time, as more is expected from the private sector in terms of resilience and defense, there is a growing acknowledgement that the public sector cannot or should not be the primary service provider for such efforts as countering violent extremism (CVE). This blurs traditional distinctions between government and industry.

The private sector is not a monolith. Much like the US public safety architecture, it's a diverse ecosystem composed of different entities that operate according to different policies and legal frameworks; from small locally-owned businesses to large publically traded multinational corporations. Approximately 85% of US critical infrastructure is owned and operated by the private sector; however, this discussion is not limited to those players. Each private citizen has a role to play, and academic institutions, hospitals and medical service centers, nongovernmental organizations, and commercial businesses can all be critical partners for US public safety efforts.

For the purposes of this discussion, 'private sector' refers to those individuals and commercial or noncommercial entities with the closest proximity to the community within a government actor's

[a] For more, see BENS' report Domestic Security Revisited

jurisdiction. As previously stated, it's at the community level where individuals detect suspicious behavior, where physical threats are identified and prevented, and, in the event of a successful physical attack, where recovery will begin. In today's threat environment the private sector can no longer remain a subordinate partner, but must be a full participant in helping to ensure our public safety and enable recovery from natural and man-made disasters.

The creation of more effective and mutually beneficial public-private partnerships (PPPs) is central to this paper's proposed networked approach to public safety. To have the most immediate impact on US public safety, effective PPPs should serve the communities in which the participants operate. PPPs are defined here according to the Defense Business Board's definition of "public-private collaboration": "a voluntary interaction between public and private sector entities through which both parties leverage the expertise, resources, and incentives of the other in order to address an issue or opportunity with greater speed, effectiveness, efficiency, or residual impact."[1]

PPPs are an increasingly important construct to ensure US homeland and national security, particularly as government resources continue to flatten or decline. Productive PPPs, however, can be stymied by the lack of a compelling business case for private sector participation, an overemphasis on process rather than outcomes, ill-defined responsibilities, or partnerships that are more transactional interactions than collaborative endeavors. PPPs can also be encumbered by real and perceived variations among state or municipal laws governing how information can be shared, the federal authorities to which government agencies must adhere, and a lack of trust among all parties—which is difficult to cultivate and easy to squander.

This paper is based on the expertise and experience of Business Executives for National Security's (BENS) Member working group, which authored this paper, and on direct engagement with law enforcement, intelligence, and homeland security practitioners at all levels of government. BENS conducted these engagements under strict Chatham House Rules and will not attribute any quotes to individuals. Where appropriate, footnotes cite additional BENS work on the issues raised in this discussion (conversely, endnotes provide formal citations for referenced works). The discussion is divided into three sections: an examination of today's threat environment; an overview of private sector horizontally integrated and networked business practices; and a discussion of how these practices may be applied in the US public safety network, focusing on the private sector stakeholders, fusion centers, and state HSAs.

The following discussion is not intended to be overly prescriptive in its description of the challenges associated with navigating today's threat environment. Rather, in keeping with BENS' nearly four decade tradition, this paper elevates issues worthy of further consideration and offers pragmatic, business-based steps to support existing public sector efforts. In 2017 BENS will initiate a series of activities and engagements to develop viable recommendations to overcome barriers to public-private partnerships, improve coordination among state HSAs, and clarify roles and responsibilities for state, local and federal public safety stakeholders. As the United States continues to navigate an ever shifting domestic threat environment, the unique perspective and capabilities of private sector stakeholders may help define the contours of a future we cannot yet envision.

II. THE THREAT ENVIRONMENT

"How, Not Why"

Today's threat environment is complex, presenting both physical and virtual threats to US public safety. As former New York Police Commissioner Bill Bratton recently stated, "there is no 'new normal', the normal is going to keep changing…."[2] Within such an environment, threat categories are increasingly blurred (e.g. criminal vs. terrorist) and the attribution or motivation for an event may be difficult to precisely discern, even in retrospect (e.g. cyber hacktivism vs. economic espionage). This discussion will focus primarily on active physical threats, defined here as terrorist events, attacks by homegrown violent extremists, active shooters, and physical insider threats. Such threats are increasingly locally focused and decentralized, facilitated by technological innovation and characterized by an emphasis on mass-casualty attacks on soft targets. Recent successful attacks demonstrate the limitations of the current approach to public safety, and the need for a more flexible and collaborative response.

Technological innovation has enabled secure communication and rapid distribution of propaganda to diverse audiences, increasing the speed to execution and scale of active physical threats. "It's very much an evolution," said Michael Steinbach, Executive Assistant Director of the FBI's National Security Branch, "and that evolution is driven by technology."[3] Social media and secure messaging applications have democratized information, made it easier to connect with like-minded individuals, and redefined traditional notions of community. Consequently, events are increasingly interdependent, threats are no longer confined by geographic boundaries, and international trends can now inform local dynamics. Yet, even with advances in communication and messaging, recent incidents suggest that the preparation and execution for an attack are largely low-tech, less sophisticated exercises (e.g. using a truck, knife, or simple improvised explosive device to harm people). Thus, it is important to distinguish between technological improvements for communication and radicalization, and actual attack preparation and execution, for which many of the tactics, techniques, and procedures are largely unchanged (e.g. purchase of a weapon or surveillance of a target).

Active physical threats also seem to be increasingly locally generated and focused, often carried out by individuals with tenuous or nonexistent operational links to foreign organizations. Attacks in San Bernardino, CA, Orlando, FL, and Nice, France seem to have been characterized by a combination of ideological inspiration and virtual facilitation rather than traditional operational direction. Organizations like the self-styled Islamic State (IS) encourage this type of terrorist entrepreneurship which has, in effect, reduced the barrier to entry and unit cost of terrorism such that one individual can have a disproportionate impact on public safety. Actors no longer need to travel or communicate with other individuals who reside overseas, which heightens the importance of the role of the local community in identifying and reporting indicators of potential threats.

This terrorist entrepreneurship also has consequences for the private sector. As Robert Griffin, General Manager of Safer Planet for IBM Analytics, has stated: "As we moved from nation-state terrorism to market-based terrorism the battlespace changed. I think it's drawing more and more of my [private sector] clients into that

Unidentified Flying Threats. Criminals and bad actors are often among the earliest adopters of technological innovations. For example, based on BENS' discussions with homeland security practitioners, drones are an increasing issue of concern, particularly with regard to their potential to damage or otherwise disrupt US critical infrastructure. One practitioner indicated that commercially available drones are capable of carrying steel cable and dropping it on electricity substations, causing them to catch fire and short out. Practitioners also worry that drones could be used to hack into critical infrastructure control centers—even those that are not connected to external networks— and provide unauthorized access to control systems and/or sensitive networks. However, even as technological innovations introduce new threat vectors, it also affords new ways to improve US public safety. Indeed, drones have been successfully deployed during emergency response and recovery scenarios or to inspect and monitor critical infrastructure facilities.

battle space."[4] Indeed, recent attacks demonstrate an emphasis on producing as many casualties—both civilian and non-civilian—as possible through the deliberate targeting of privately owned and soft targets. However, although this trend suggests an inclination toward less sophisticated attacks, the threat of larger-scale coordinated attacks remains. IS and other organizations continue to demonstrate an interest in acquiring chemical or biological weapons. For example, one federal law enforcement official indicated to this paper's authors that foreign-based terrorists may be using encrypted channels to distribute instructions for creating biological agents that could be used in an attack.

While the traditional pathway to violence (i.e. grievance, ideation, research/planning, preparation, breach, attack) is still valid, attacks in San Bernardino, Orlando, and Charleston suggest that the progression may be non-linear, highly individual, significantly compressed in time, and increasingly hard to detect using traditional intelligence and law enforcement means. These recent attacks also suggest that individuals may be dedicated adherents of a particular ideology, alienated from their surrounding community, mentally ill, or in search of a cosmic justification for an existing pathology or propensity to violence. In some cases, it may be a combination of all four.[5]

Michael German, Fellow at the Brennan Center for Justice and former FBI Special Agent, has observed that the so-called radicalization process happens "between the ears of the individual….Unfortunately what we know from scientific studies is that individuals come to the decision to engage in terrorism for any number of reasons. There is not a predictive path that people follow."[6] Various studies have demonstrated that personal or group identity, social dynamics, or family relations can play a role in an individual's radicalization to violence.[7] A recent report by The George Washington University concluded that, "The profiles of individuals involved in ISIS-related activities in the U.S. differ widely in race, age, social class, education, and family background. Their motivations are equally diverse and defy easy analysis."[8]

Accordingly, although understanding why individuals carry out acts of violence is important over the longterm, focusing on how they carry out their acts, not why, may have a more immediate impact on public safety, given the diversity of person-dependent motivations at play.[9] Indeed, focusing on how individuals plan and commit acts of violence can offer a more effective means for understanding how to detect, interdict, and prevent those actions. This approach requires a more bottom-up, collaborative approach to public safety which leverages the knowledge and insight of SLTT officials in whose jurisdiction these attacks may be prepared and carried out. It may also require greater inclusion of non-traditional public safety stakeholders such as mental health practitioners, human resource personnel, or other civic leaders.

"Like Water Spreading on a Table"

Although there have been improvements, the differing authorities and jurisdictions of federal, state, and local law enforcement and homeland security agencies can complicate the detection, prevention, and response to active physical threats. After 9/11, legislative and executive reforms (to include the 2002 Homeland Security Act and 2004 Intelligence Reform and Terrorism Prevention Act) created an intelligence and counterterrorism apparatus that was largely designed to defend against large-scale coordinated attacks from foreign terrorist organizations. Intelligence and homeland security stakeholders have recognized the need to adapt the post-9/11 architecture to today's changing threat environment, but improvement has been slow and uneven. As one federal law enforcement leader stated, many homeland security and public safety agencies are organized vertically, but today's threat vectors are horizontal. "It's like water spreading on a table," he said "and we're able to stick our finger in it but we can't get our arms around it."

Based on BENS' discussions with public safety officials, the US Intelligence Community

(IC) does not fully incorporate, exploit, or take into account SLTT perspectives when assessing national security threats to the United States.[b] There are, however, some promising initiatives that could be emulated more widely. The National Counterterrorism Center's Joint Counterterrorism Assessment Team (JCAT) provides opportunities for state and local first responders and public safety officials to work alongside their federal counterparts to identify information that is relevant to SLTT stakeholders, and distribute it at the lowest possible classification level.[10] Similarly, in 2015 the Drug Enforcement Administration (DEA) coordinated a National Heroin Threat Assessment, in partnership with other federal and SLTT partners, which incorporated state and local perspectives through a survey that was distributed to over 1,000 stakeholders. In fact, it was the Superintendent of the New Jersey State Police who originally recommended conducting the assessment.

The Program Manager for the Information Sharing Environment (PM-ISE) in the Office of the Director of National Intelligence has also noted that Congress laid the foundation for a network-centric approach to counterterrorism in the 2004 Intelligence Reform and Terrorism Prevention Act. The law stipulated that the ISE be "a decentralized, distributed, yet coordinated environment" that is not bound by normal jurisdictional limitations (federal, SLTT, and the private sector).[11] Rather, the ISE is intended to facilitate interaction across these jurisdictions in a manner that that would take most advantage of this paper's proposed networked approach.

Federal officials have indicated their support for the Criminal Intelligence Coordinating Council (CICC), a coordinating and advisory body that brings together law enforcement officials from all levels of government.[12] According to one report, during the January 2016 CICC meeting Deputy Attorney General Sally Quillian Yates "affirmed that CICC meetings provide an opportunity for federal partners to listen to and participate in a dialogue with state, local, tribal, and territorial (SLTT) partners to learn about and better understand issues affecting them and their agencies and organizations."[13] The CICC has made considerable progress in building an interoperable national information sharing framework and aligning the capabilities of federal, state, and local entities.[14]

Yet, while these developments are encouraging, practitioners with whom BENS has engaged indicated that programs like JCAT and the 2015 heroin assessment—while valuable—are too small scale or not institutionalized throughout the federal IC. The CICC, PM-ISE, and federal partners are building clear momentum toward further aligning and integrating criminal intelligence into national security and public safety efforts, in strict accordance with appropriate legal and civil liberty protections. Yet, SLTT and private sector stakeholders continue to observe that criminal intelligence and local perspectives remain a valuable but underutilized resource in the public safety space.

BENS has learned that there may be resistance to elevating the role that the CICC could play beyond its mandated interagency advisory role. SLTT and private sector stakeholders also continue to indicate that information sharing remains oneway (up to the federal level) and lacks an interactive feedback loop. Consequently, they often do not know if the information that they shared was valuable, or if a threat is still active. Reporting can then become less of a priority and more of a burden on already over-burdened organizations. The lack of feedback also erodes trust and confidence in partnership efforts.

Recent attempted and successful physical attacks demonstrate that virtually anything and anyone is a potential target and everything is a potential weapon. This requires a much more proactive and bottom-up approach to public safety. Thus, the challenge is not how to improve information sharing, per say, but rather how to cultivate purposeful partnerships that provide insight into stakeholder requirements and provide value pursuant to those needs. This goal is to facilitate knowledge creation and rapidly bring it to scale. This can be difficult, however, if law enforcement officials at all levels of government operate from a "case-making" and prosecutorial mindset. Looking for evidence of an attack rather than pre-attack indicators can cause investigators to discard potentially relevant information if it is not sufficient to begin or build upon a case.

For example, officials with whom BENS spoke suggested that the investigations into the San Bernardino and Orlando attacks suggest that the FBI, in particular, may overemphasize operational links to foreign terrorist groups, and thus may be slow to adapt to the

[b] For more, see BENS' report Domestic Security Revisited

changing nature of the terrorist threat in which operational links are no longer a prerequisite for action. To be sure, there are certainly external pressures bearing down on the FBI to identify potential external links to foreign terrorist groups. The FBI has also made great strides since 9/11 in transforming into a threat-based and intelligence-led organization. Yet, according to Lorenzo Vidino, Director of the Program on Extremism at the George Washington University Center for Cyber & Homeland Security, "There's an overemphasis on operational links…it's easier to put into a box—a paradigm that the FBI is more used to."

Continued focus on foreign operational links is also evident at the state and local level. For example, during the preliminary stages of the investigation into the September 2016 bombing of a Chelsea neighborhood in New York City, Governor Andrew Cuomo was quick to observe, "There have been no international groups that have put out any statements connecting them with this action. Now it depends on your definition of terrorism…but it's not linked to international terrorism."

Public safety officials' collection and exploitation of pre-event indicators can be stymied by advances in encryption technologies, a lack of coordinated suspicious activity reporting (SAR), or a lack of awareness among public or private sector stakeholders about what type of information might be relevant. This is true even as on-the-ground attack preparations continue to be relatively low-tech. In fact, pre-incident indicators can often be hidden in plain sight, invisible to the untrained eye, and as a result may be treated as innocuous activities that do not reach a threshold of official interest. This can occur for a lot of reasons ranging from a lack of knowledge of value to the fact that the anomalous activity may not initially be criminal.

Terrorist entrepreneurs can adapt and improvise on demand, in part, because they are not encumbered by the legal constraints, bureaucratic imperatives, or long decision-making processes with which our public safety officials must contend. Consequently, an equally flexible and multidisciplinary approach to public safety may need to reconsider what type of information is relevant. This is one of the reasons that a horizontal and collaborative approach to information collection is so important. Better understanding and exploitation of the information that is collected routinely by law enforcement officers through community policing, neighborhood watch, and SARs can be extraordinarily valuable. Open source information, such as subscription services and publically available information, may provide additional insight if leveraged to a more meaningful degree; however, the use of this information must strictly adhere to appropriate legal constraints and privacy and civil liberty protections.

In today's threat environment, relevant pre-attack indicators may include extreme rhetoric on social media, signs of mental instability, domestic abuse, a criminal history, illicit financial transactions, and/or physical surveillance of particular locations. The Orlando nightclub shooter, for example, allegedly was a psychological and domestic abuser, according to his ex-wife.[15] Similarly, the killer of nine parishioners at the Emanuel African Methodist Episcopal Church in South Carolina had a reported history of drug use and multiple encounters with police.[16] The individual who killed over 80 civilians in Nice, France was found to have conducted surveillance on his target at least three times prior to the attack, as well as once on the day of the attack, and rehearsed the route.[17] As individual data points, these and similar pieces of information certainly do not suggest an imminent threat, but within the proper context and assembled together they may reveal a clearer indication of intent.

> "The FBI has also made great strides since 9/11 in transforming into a threat-based and intelligence-led organization."

Many forms of criminal behavior can lead to terrorist activity. The challenge in a strictly top-down structure is that data about criminal activity or the individuals involved can become highly siloed, difficult to share, and may lack the context needed for proper interpretation. It is important, then, to move beyond only information sharing and toward greater "knowledge" creation; that

is to say, the combination of data with the benefit of first hand personal interaction and history of particular individuals. As Robert Griffin has observed, "the reality is that [information sharing] is table stakes…If content is king, and information is king…access and distribution is King Kong. The ability to get that information to the right people, at the right place, at the right time, as close to the edge as possible is the stuff that's going to make a major difference."[18] This can be accomplished through more responsive and two-way partnerships between local law enforcement and the federal counterterrorism apparatus.

Again, this is not to say that every domestic abuser or drug user is a potential terrorist, nor is it an attempt to criticize law enforcement officials in hindsight. Detecting, preventing, and responding to active physical threats is an exceedingly difficult task. That some recent attacks were conducted by individuals who were already on law enforcement's radar suggests that the structures and processes established to identify and assess potential threats are working to some degree. Yet, broadening the scope of what data may be relevant, and leveraging non-traditional resources to collect it, may better position public safety officials to identify and address potential threats.

This must be conducted in a transparent way and pursuant to appropriate legal and privacy and civil liberty protections. In some instances, as was the case in Nice and Orlando, evidence of traditional surveillance may have been missed or discounted. In others, criminal activity or evidence of a criminal history were overlooked as potentially important information. As Dr. John Nicoletti, a Colorado-based police psychologist, has demonstrated from his research, patterns of behavior are broadcasted such that the behavior highlights their planning leading to the violence.

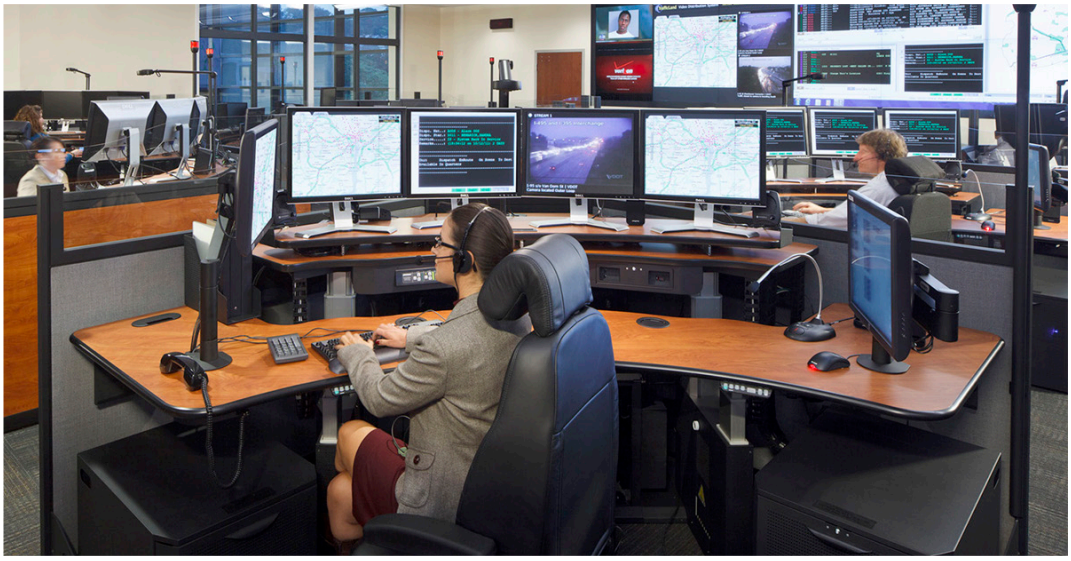
In addition to reconsidering what information may be germane to public safety efforts, stakeholders might consider pursuing tailored, non-governmental, and non-law enforcement responses to perceived or potential threats. While such approaches might entail law enforcement outcomes (e.g. arrests and criminal prosecutions), a prosecution-only approach leaves little recourse for law enforcement officials to respond to a potential threat if there is no case to be made. In individual instances, alternative responses can include interventions by mental health practitioners or human resources personnel, and engagements with community, education, and faith leaders.

John Cohen, former Counterterrorism Coordinator at the Department of Homeland Security, reinforced the importance of a multidisciplinary approach by observing "Family and friends are going to be much more likely to call law enforcement to report troubling behavior if they know that it's not going to result in an arrest, but an intervention instead."[19] An Illinois man was recently arrested and charged with material support for terrorism when his grandmother called police trying to gain help in getting her grandson treatment for his schizophrenia. As she said, "Had I [known] by me trying to get help for him would cost him to be in jail, I would never call the police."[20] Ultimately, public safety is every citizen's responsibility. A truly networked approach must engage the entire community and empower citizens to understand their role as well as that of federal, state, and local public safety entities.

This approach must include meaningful and deliberate engagement with the private sector as a partner in ensuring US public safety, not merely as a beneficiary of public safety. Approximately 85% of critical infrastructure is owned and/or operated by the private sector, and many of the recent targets or would-be targets of terrorist attacks are privately owned soft targets. And yet, based on BENS' research and outreach to public safety leaders, private sector engagement is ad hoc and uneven among public entities, particularly state and major urban area fusion centers and various offices within the Department of Homeland Security (DHS). To be sure, public sector organizations are bound by the federal or state authorities that govern their actions. These authorities can, at times, constrain how and when public sector partners engage their private sector counterparts.

Further, BENS has found that among public sector participants there is no consensus on what "engagement" means. Many public safety and law enforcement officials also lack a meaningful appreciation for the unique capabilities and information private sector partners can bring to bear, including business facility surveillance, competitive intelligence, and enterprise risk management. Absent a compelling business case for investing

in resilience or a clear return on their investment, private sector partners often do not view such expenditures as long term investments. Such a business case could frame resilience in terms of insurance, business continuity, and brand protection or reputational considerations,and should account for liability considerations.



Improvement to the US public safety architecture can be pursued with the goal of elevating the role of state and local law enforcement entities, engaging community leaders, and strengthening partnerships with private sector stakeholders. Wherever possible, these changes can occur within and among existing structures and processes, better coordinating and improving current authorities and processes for building PPPs, rather than creating new ones. As these changes are undertaken, new ways for measuring effectiveness, value, and progress toward established objectives will be required.

Public and private sector leaders must pursue this improvement in a collaborative manner, working together to clearly define the priorities and informational requirements of each partner, and providing information that adds value to those requirements. Private sector best practices for horizontal integration provide insight as to how to achieve a more networked approach to public safety which may better position US public safety practitioners to begin to get their arms around the water spreading on the table.

THE THREAT ENVIRONMENT | KEY TAKEAWAYS

- **Technological innovation has had a significant impact on active physical threats**, increasing their speed and scale by enabling individuals' ability to communicate securely and quickly distribute propaganda to diverse audiences.
- Recent attacks suggest that active physical threats are also **increasingly local**, often carried out by individuals with tenuous or nonexistent operational links to foreign organizations.
- Focusing on ***how rather than why*** individuals realize their violent intent can have more immediate impact on public safety.
- **Facilitating and rapidly scaling the creation of knowledge** is critical. This will require building purposeful partnerships with SLTT and private sector stakeholders at the community level, which can provide greater insight into their information requirements.
- It may be necessary to **reconsider what type of information is relevant** (e.g. past criminal behavior, extreme rhetoric, illicit financial transactions). Individual data points certainly do not suggest an imminent threat, but within the proper context and assembled together they may reveal a clearer indication of intent.
- **Multidisciplinary and non-governmental responses should be pursued**, where appropriate, in close partnership with the private sector. These may include law enforcement investigation, interventions by mental health practitioners or human resources personnel, or engagement with community, education, and faith leaders.
- All such activities must be **conducted in a transparent way and pursuant to appropriate legal and civil liberty protections**.

III. HORIZONTAL INTEGRATION AND NETWORKED BUSINESS PROCESSES

"What was the profit I wanted? Crime reduction."

Traditionally, organizations have tended to integrate vertically; however, over the past three decades there has been a trend in the private sector toward horizontally integrated business practices. This trend has been in response to a rapidly evolving global market place and digital disruption, both of which have created a demand for customer-centric, responsive, and tailored product and service delivery at the local level.[21] Mobile applications and distributed communication technologies enable horizontal and networked integration by freeing individuals to work effectively outside a traditional hierarchy.

Businesses embrace horizontal integration, at least in part, to continually improve their financial results by attacking inefficiencies and increasing the speed and clarity of data across the horizontally integrated operating platform. The work of W. Edwards Deming and other leaders of the "quality movement" has institutionalized the practice of continuous improvement by challenging taken-for-granted norms and practices. For successful continuous improvement to occur, organizations must develop cultures that support change and risk taking. Managers and employees at all levels must find ways of embracing the uncertainty in a manner that allows new patterns of action to emerge. In traditional, vertically integrated business models, management typically exerts control with strong guidance and defined targets for performance. Armed with a corporate vision, values, and norms to guide behavior, horizontally integrated businesses are essentially intelligent systems that evolve and innovate appropriately to the situation at hand.[22]

W.L. Gore & Associates—manufacturer of the synthetic weatherproof fabric Gore-Tex—has gradually developed a horizontal business model since its founding over half a century ago. Only three levels of hierarchy separate Gore's 10,000 person workforce; a chief executive officer (CEO) and a series of functional directors are all that sit atop Gore's employees.[23] This flatter hierarchy is part of Gore's "lattice" management structure in which small, self-managing teams of 8-12 employees are responsible for most decisions, from hiring and firing to prioritizing on which projects to work.[24] "It's far better to rely upon a broad base of individuals and leaders who share a common set of values and feel personal ownership for the overall success of the organization," says CEO Terri Kelly. "These responsible and empowered individuals will serve as much better watchdogs than any single, dominant leader or bureaucratic structure."[25]

This structure allows Gore to remain innovative and competitive because good ideas can come from anyone in the organization and don't need to traverse several layers of management to receive attention from decision-makers.[26] "It absolutely is less efficient upfront," Ms. Kelly admitted to the Wall Street Journal in 2012, "[But] once you have the organization behind it…the buy-in and the execution happen quickly."[27] Indeed, Gore's lattice structure has allowed it to remain among Fortune's 100 best companies to work for over almost two decades.[28]

Innovative public sector leaders have applied similar private sector principles to great effect. In Iraq, General Stanley McChrystal succeeded in navigating a complex battlespace by reengineering the Joint Special Operations Task Force from a traditional military hierarchy into a more nimble "team of teams" by emphasizing interpersonal relationships and organizational transparency. Similarly, as New York Police Commissioner in the early 1990s, Bill Bratton decentralized his department by empowering lower-level leaders and encouraging locally-driven solutions. Both of these examples are instructive as to how private sector best practices can be applied in the public sector to better address today's threat environment.

Like W.L. Gore & Associates, horizontally integrated or networked business processes are generally characterized by fewer levels of management, improved manager-employee communication, and

an increased capacity for quick and flexible responses to events.[29] Such an approach allows for greater adaptability, increased innovation and collaboration among employees, and higher organizational resiliency.[30] According to a recent Deloitte study which surveyed over 7,000 business leaders, "Companies are decentralizing authority, moving toward product- and customer-centric organizations, and forming dynamic networks of highly empowered teams that communicate and coordinate activities in unique and powerful ways."[31]

During his time as Commander of the Joint Special Operations Task Force in Iraq, General Stanley McChrystal developed an effective fighting force by creating similarly dynamic networks of empowered teams. When he took command in 2003, General McChrystal found himself confronted by a complex battlespace evolving in a nonlinear fashion. As he observed, "Being effective in today's world is less a question of optimizing for a known…set of variables than responsiveness to a constantly shifting environment."[32] In such an environment every piece of information can be relevant to anyone at any time, which defies the capacity of a single director to manage from the top.[33] "Our Task Force's rigid top-to-bottom structure," he wrote, "was a product of military history and military culture, and finding ways to reverse the information flow—to ensure that when the bottom spoke the top listened—was one of the challenges we would eventually have to overcome."[34]

As General McChrystal realized, teams are far more effective at navigating a complex environment. "A group can improvise a coordinated response to dynamic, real-time developments," General McChrystal remarked, because "teamwork is a process of

HORIZONTAL INTEGRATION | KEY TAKEAWAYS

- Companies are moving toward horizontally integrated processes in response to a rapidly evolving global market place and digital disruption, both of which have created a **demand for customer-centric, responsive, and tailored product and service delivery at the local level**.
- Horizontal integration is characterized by fewer levels of management, improved manager-employee communication, and **an increased capacity for quick and flexible responses to events**.
- For General McChrystal, **teams were far more effective** at navigating a complex environment, but needed to be linked through interpersonal relationships to provide a complete awareness of how a team's actions advance the strategic direction.
- As NYPD Commissioner, Bill Bratton **empowered lower-level leaders**, held them accountable through direct management, and **encouraged locally-driven solutions**.

reevaluation, negotiation, and adjustment."[35] Teams, however, are only as effective as their scale and horizontal integration allows. If, for example, a team is embedded within a traditional hierarchy, its adaptability and innovativeness can be stifled. This was one of the Task Force's early obstacles. The teams on the Task Force were composed of individuals from various intelligence and military services and "…the only external ties that mattered… ran vertically, connecting to the command superstructure… meaningful relationships between teams were nonexistent."[36]

Achieving scale within a shifting environment requires developing strong, responsive, and trust-based horizontal connections among the individuals who make up each team. These relationships provide transparency into each members' operations and are facilitated by a complete awareness of how a team's actions advance the strategic direction.[37] As McChrystal explains, "Team members tackling complex environments must all grasp the team's situation and overarching purpose. Only if each of them understands the goal of a mission and the strategic context in which it fits can the team members evaluate risks on the fly and know how to behave in relation to their teammates."[38] Regardless of the organization's mission, scaling trust with key partners is a fundamental element of continuous improvement. Team member performance and a commitment among team members to improving processes are more likely to cultivate trust than the behavior or credentials of any one individual.

General McChrystal's application of networked processes follows an established trend in the private sector. Indeed, according to Deloitte, the two primary factors animating this trend are a need to deliver products and services quickly, and the belief that empowered teams "can deliver results faster, engage people better, and stay closer to their mission."[39] Engaging subordinates and key stakeholders and staying closer to mission were two central tenants for Bill Bratton during his first tenure as New York Police Commissioner. Between 1994 and 1996, Commissioner Bratton succeeded in reducing felony crime rates by nearly 40%, murders by 50%, and theft by 35% by empowering lower-level leaders, holding them accountable, and encouraging locally-driven solutions.[40] He accomplished this while public confidence in the NYPD grew to 73%.[41]

As Bratton described it, when he arrived in 1994 the New York Police Department (NYPD) "…was divided into little fiefdoms… Each bureau was like a silo: Information entered at the bottom and had to be delivered up the chain of command from one level to another until it reached the chief's office."[42] At the time, the NYPD was divided into eight boroughs, each of which contained several divisions which, in turn, presided over several more precincts.[43] When he became commissioner, Bratton eliminated the division-command level and devolved authority to each precinct commander, thereby creating "76 miniature police departments."[44] Commissioner Bratton and his management team held commanders accountable though weekly meetings at headquarters, during which someone would be chosen to lead a briefing on his jurisdiction.[45] These briefings provided opportunities for commanders to share information, de-conflict operations, and identify common challenges.

Bratton also encouraged each precinct commander to come up with creative ways for dealing with local problems. He insisted that his officers meet with the communities they served to get a better understanding of their priorities. As an officer with the Boston Police Department, Bratton met with residents of a local neighborhood who were dissatisfied with police performance, even though official crime statistics for their district were positive.[46] According to authors W. Chan Kim and Renee Mauborgne, the meeting revealed "a huge perception gap…While the police officers took pride in solving serious offenses…few citizens felt in any danger from these crimes. They were more troubled by constant minor irritants."[47] Bratton used this feedback to refocus his officers' efforts on issues that were core to their customers. Commissioner Bratton brought his customer-centric focus with him to the NYPD. As he explained, "We began to run the NYPD as a private profit-oriented business. What was the profit I wanted? Crime reduction. I wanted to beat my competitors…I wanted to serve my customers, the public, better; and the profit I wanted to deliver to them was reduced crime."[48]

IV. TOWARD A NETWORKED APPROACH TO PUBLIC SAFETY

Similar to the complex battlespace in which General McChrystal operated, today's threat environment is characterized by increasingly localized and ad hoc acts of violence by individuals who are enabled by advancements in information and communications technology. This threat defies a traditional top-down response and requires a more decentralized and networked approach to public safety, one which leverages SLTT and community-based private sector partners to a greater degree. As Bill Bratton's time as commissioner demonstrated, such an approach requires identifying and empowering key nodes of the network (in his case, the precinct commanders) that are capable of delivering locally-driven solutions to unique customer segments in a responsive manner.

The private sector, state and major urban area fusion centers, and state HSAs are three key nodes in the US public safety network. They can act as force multipliers for the entire network by ascertaining key themes among the crush of available data, and sharing contextualized knowledge back into and up through the network in order to support decision-makers at the federal, state, and community levels. Public and private sector leaders must integrate these nodes by building partnerships that provide increased transparency along the information supply chain and an awareness about how each team contributes to the national public safety mission. The following discussion will examine how to properly resource and empower these nodes by overcoming barriers to purposeful public-private partnerships, adequately valuing state and major urban area fusion centers beyond simple cost-benefit calculations, and improving coordination among state HSAs.

Making Public-Private Partnerships Purposeful

Traditionally, the private sector has been fundamental in enabling US national security and public safety; as a robust economic engine, it has propelled the US to secure its interests both at home and abroad. As discussed previously, however, terrorist entrepreneurs are targeting the private sector with increasing frequency, making them both the first casualty and first responder in many instances. Accordingly, the private sector can no longer remain an enabling partner, but must be a full participant in helping to ensure our public safety and facilitate our recovery from natural and man-made disasters. Public sector

stakeholders need to understand the unique capabilities that industry can bring to bear and work with their private sector counterparts to consider how best to engage and utilize those capabilities. Likewise, private sector executives must understand the organizational or statutory limits placed on their public sector partners, and overcome any lingering misperceptions about working with the government.

There have been successful PPPs in the public safety space. One example is Project Touchstone, an FBI led PPP that includes stakeholders from the retail, commercial property, education, and tourism industries. Through Touchstone, private sector participants in several cities nationwide have built personal relationships with the public safety and law enforcement officials in their region, and receive intelligence products and warning information that are specifically tailored to their needs. These partnerships also provide avenues for private sector stakeholders to send SARs to their law enforcement counterparts, support law enforcement priorities by remaining alert to criminal activity, and create pragmatic crisis response plans through regular meetings and table-top exercises. In 2013, Touchstone was recognized as a best in class practice.[49]

> "...BENS has found that the lack of a compelling business case for private sector participation stymies productive PPPs."

Yet, BENS has found that the lack of a compelling business case for private sector participation stymies productive PPPs. Collaboration is also obstructed by an overemphasis on process rather than outcomes, ill-defined responsibilities, and/or perceived or artificial barriers which have no legal, policy, or organizational basis but nonetheless become institutionalized over time. In other instances, PPPs are sometimes pursued in general terms and toward ill-defined ends. This can manifest itself in a "check-the-box" mentality, wherein simply meeting with a private sector representative is considered an achievement, or in partnerships that lack the structure, tempo, or trust to achieve a defined objective. As a result, PPPs have achieved successes in certain areas but the overall results are uneven.

Cultivating effective PPPs requires an appreciation for the unique capabilities that the private sector can bring to bear and a willingness on the part of the private sector to utilize them. Companies have developed corporate intelligence units, big data analysis methodologies, and enterprise risk management strategies to compete in a dynamic and uncertain global marketplace. Many large companies, to include Bank of America and United Airlines, have developed sophisticated travel safety programs for their employees, which consider political and public health risks associated with foreign countries, and provide real-time notifications for individuals traveling abroad. Financial market data can also provide meaningful insight into capital flows, consumer behavior, and potential indicators and warning information of threats to public safety.[c]

Equipped with a better understanding of private sector capabilities and resources, law enforcement and public safety officials will be better positioned to determine when it is appropriate to encourage private sector stakeholders to take more of a leadership role for specific issues. For example, Jigsaw, the idea incubator within Alphabet (Google's parent company), has developed the technical means to redirect individuals who are actively searching for extremist content online.[50] It has also partnered with nonprofit organizations to develop counter messaging and engagement campaigns designed to divert individuals who may be on the path to radicalization.[51]

More focus should be given to identifying other challenges that may be addressed by privately led and locally-driven solutions. This is increasingly important as active physical threats continue to diversify. Further, for specific industries or geographic regions, it may be appropriate for public safety entities to identify where their priorities overlap with those of the private sector stakeholders and consider how they may be brought into closer alignment. Understanding what the private sector perceives as an emerging market or potentially disruptive technology, and how they've

[c] For more information, please refer to BENS' upcoming issue paper "From Counter Threat Finance to Countering Financial Threats"

resourced themselves accordingly, can allow public safety agencies to manage evolving threats in a more proactive manner.

To provide the most value to all parties, PPPs must be purposeful—created to address a specific threat or vulnerability, leverage a specific capability, engage a specific industry, or all of the above. In any case, partnership should not be sought as an end in itself, but must have a clear business case underpinning it. This business case should be framed around resiliency, business continuity, corporate citizenship, and/or brand protection or reputational considerations, and should account for liability considerations. PPPs can also be organized around mutually beneficial objectives and goals. For example, the Standards Coordinating Council created by the PM-ISE brings together industry and standards setting bodies and government officials to develop information sharing standards and architectures of value, and to empower the IT industry to develop and implement advanced information sharing applications. This PPP is developing an enhanced framework for information sharing and safeguarding that covers all levels of government and disciplines.[52]

A more resilient company is capable of withstanding and recovering quickly after an event, whether man-made or natural. Some businesses have developed methodologies for measuring their captured sales post-event as compared to those of their competitor. BENS has been working with law enforcement officials in Chicago to develop a short, replicable, and compelling business case for investing in a PPP with local law enforcement there.[d] The work has focused on understanding the concerns and requirements of local stakeholders and developing a value proposition that focuses on post-event possibilities (e.g. looting, medical response, facility damages, and litigation risk) that participation in the PPP can mitigate.

Maintaining effective PPPs is an enduring challenge. The likelihood that a previously disengaged private sector business or business owner will share information about a specific threat would be enhanced by the predictability of liability protection. Variations in state and municipal sunshine laws prohibit a one-size-fits-all public safety approach. Based on BENS' past research, liability protection is an important consideration for private sector entities and citizens that share "Good Samaritan" threat information at the request of government stakeholders.[e] To address this issue, legislators, both in Congress and at the state level, may consider reviewing all applicable safe harbor provisions to ensure that all appropriate Good Samaritan activities are identified and covered. Public sector stakeholders must also be mindful of private sector concerns that sharing information may lead to regulatory action that can adversely affect profitability.

Purposeful PPPs must also be flexible enough to allow for collaborative and improvised interactions, yet structured enough to maintain appropriate tempo and clearly defined roles and responsibilities. Absent a coherent structure, PPPs can atrophy over time and produce little value. This may cause all parties to become disinterested and skeptical of embarking on future partnerships. This is a common occurrence among the private sector stakeholders with which BENS has met.

This does not mean PPPs have to be sustained efforts over time. In fact, many valuable partnerships can be temporary endeavors

I&A | Q&A. In an effort to provide more useful products to its key stakeholders, the Department of Homeland Security's Office of Intelligence and Analysis (I&A) and National Programs and Protection Directorate (NPPD) have begun to invite private sector representatives (acting on behalf of their sectors) to review intelligence products before they are published. These representatives are invited to I&A's Washington DC headquarters on a biweekly basis (and a quarterly basis regionally) to offer recommendations on the type of information that is included and how that information is packaged and disseminated, and to lend their perspectives on key issues. To the extent that it is appropriate, fusion centers and state emergency management or public safety offices may consider instituting a similar practice to ensure that their intelligence products are providing value to their customers. Other Federal agencies may consider participating in the forums as DHS expands them to a whole-of-government approach.

[d] For more information, please refer for BENS' upcoming issue paper "A Business Case for Resilience"
[e] For more, see BENS' report Domestic Security Revisited

PURPOSEFUL PUBLIC-PRIVATE PARTNERSHIPS | KEY TAKEAWAYS

- Cultivating effective PPPs requires an appreciation for the **unique capabilities** that the private sector can bring to bear.
- **PPPs must be purposeful**—created to address a specific threat, leverage a specific capability, engage a specific industry, or all of the above.
- **A business case for entering into a PPP** could be framed around resiliency, business continuity, corporate citizenship, and/or brand protection or reputational considerations, and should account for liability considerations.
- Public sector entities need to understand their private sector stakeholders' information requirements and develop mechanisms to serve them. This will require a **more meaningful appreciation of what it means to "engage"** with the private sector.
- Private sector partners must **overcome the misperceptions** that the government is intentionally or needlessly holding back information. This can be accomplished through a better understanding of public safety entities' structure or authorities.
- Optics or **public relations concerns must be appropriately accounted** for, but should not dictate the nature of the PPP.

formed to address a specific objective and disbanded once that objective is achieved. Thus, it may be appropriate to differentiate between building relationships (long-standing and responsive interpersonal connections) and building partnerships (purposeful engagements toward a specific end). It's also important to recognize the limitations of PPPs and to not default to partnership as a presumed silver-bullet solution to every issue. Some issues are complex and challenging and cannot be solved simply by building PPPs, which could ultimately be counter-productive to solving the identified challenge.

Based on BENS' work in this area, both public and private sector leaders must overcome obstacles in order to build purposeful PPPs. Public sector leaders must place greater emphasis on engaging private sector customers in order to understand their capabilities and requirements. This will first require a more meaningful definition of what "engagement" actually means. In many instances, a company cannot be considered to be "engaged" simply because it is on a distribution list or its employees attend a meeting. This is confusing an output (e.g. a company receiving intelligence products) with outcomes (e.g. a company using information tailored to their needs to support a decision or action).

In reality, engagement is a spectrum and may be determined based on the company's size, resources, receptivity, or industry (this is also true for fusion centers, based on mission, authorities, size, resources, and even geographic region). This can range from a fulsome and interactive relationship with corporate leadership and key employees, to routinized exchanges of information. Where a company falls on the spectrum should be determined in collaboration with that company's leadership. For sake of the public safety network's viability, engagement is required at the local level. It is a failure to assume that engagement with corporate headquarters is analogous with engagement at the local level with franchise owners, managers, and security officers. The men and women who work and live in the communities where businesses operate will most quickly recognize disruptions in patterns of life and will be the direct beneficiaries of strong connections with local public safety agencies.

Similar to Bill Bratton's experiences at the NYPD, improved stakeholder engagement can help public safety agencies provide more value to those stakeholders and cultivate greater goodwill and trust among all parties. Public safety entities must work with each company to identify the appropriate point(s) of contact (e.g. the chief risk officer, chief security officer, human resource personnel, interested employees, etc.) and understand how that company will use the information provided to them to make decisions. These discussions should also focus on what type of information to share and how to share it.

Trust-based interpersonal relationships are crucial for effective information sharing, and cannot be taken for granted. Good practices include periodically convening small working groups, either in-person or virtually, to determine how to tailor information products and reassess information requirements. In some cases

an electronic survey or questionnaire may suffice, but a responsive feedback loop is necessary to constantly improve and reorient the partnership. Classification issues can be a barrier to quick or meaningful information sharing, but government stakeholders may be able to address classification issues by reconsidering what stakeholders actually want. For example, several private sector leaders indicated to BENS that their operators don't care about sources and methods (which are often the reason information products are classified at higher levels), they primarily care about getting the information needed to remediate an issue.

Fusion center directors, DHS personnel, and other public safety leaders should also reconsider how information is shared with the private sector, whether over government systems, through third-party applications, or via personal interactions. This may be dictated by the classification level of the information, the authorities of the public sector stakeholder, or the preferences of the private sector partner. In all instances, however, the law of the instrument should not dictate how information is shared. For example, throughout BENS' work, public safety personnel often cited the Homeland Security Information Network (HSIN), a sensitive but unclassified network, as the preferred and familiar tool to share information with SLTT and private sector stakeholders. Yet, private sector counterparts with whom BENS has discussed information sharing challenges did not share the same enthusiasm for HSIN.

Purposeful public-private partnerships are two-way streets, and there are challenges that the private sector must overcome as well. Principally, private sector partners must move beyond the perception—or in some instances misperception—that the government is intentionally or needlessly holding back essential information. While classification issues certainly dictate what is and is not shared, BENS has frequently encountered a belief that the government is sitting on an information goldmine that it refuses to share. In reality, this is not often the case. A better understanding of the limitations imposed on public safety entities by their structure or authorities may help to dispel this perception. Similarly, over the past few years concerns have arisen over the public relations considerations of partnering with the government. While these must be appropriately considered and accounted for, optics alone should neither hinder nor define effective PPPs.

"The Dog that Didn't Bark"
Valuing State and Urban Area Fusion Centers

State and major urban area fusion centers are another key node in the national public safety network but they must be properly valued beyond a traditional cost-benefit analysis. Owing to their preventive nature, this can be challenging. Unless a fusion center can make a direct correlation between their functions and a criminal and/or terrorist event not occurring, it can be difficult to articulate a value proposition that quantifies progress against established objectives and demonstrates a tangible contribution to public safety. No one gets rewarded for solving a problem that didn't manifest. As one high-level intelligence leader observed, "How do you measure that? It's the dog that didn't bark."

THE DOG THAT DIDN'T BARK | KEY TAKEAWAYS

- Many fusion centers pursue an all-crimes, all-hazards mission, but unless a fusion center can establish a connection between their functions and a terrorist or criminal event not occurring, **it can be difficult to articulate a value proposition** that quantifies progress against established objectives and demonstrates a tangible contribution to public safety.
- **Internal and external messaging are a necessary**, but often overlooked, component of demonstrating value.
- Without a **clear, concise, and consistent mission statement**, employees may not understand how their actions contribute to the overall context or enterprise.
- For private sector stakeholders, a confusing or vague mission statement can make it **challenging to understand how the center can support their operations**.
- **Commercial line insurance methodologies** may offer an additional means for demonstrating and measuring the value of a fusion center.

BENS has worked with two fusion centers to articulate their public safety contributions and develop new ways to value them. Through these partnerships, two criteria have proven effective. First, a clear, concise, and consistent mission statement communicated to internal and external audiences. Second, the application of commercial risk mitigation methodologies to measure fusion centers as a form of terrorism insurance.

Clear and effective messaging is a necessary, but often overlooked, component of demonstrating value. BENS worked with one major metropolitan fusion center to develop an internal and external messaging strategy, which included reworking the mission and vision statements.[f] Without a clear, concise, and consistent mission statement, employees may not understand how their actions contribute to the overall context or enterprise. As discussed above, General McChrystal routinely emphasized the importance of teams understanding their contribution to the strategic purpose. "Functioning safely in an interdependent environment," he observed, "requires that every team possess a holistic understanding of the interaction between all the moving parts. Everyone has to see the system in its entirety for the plan to work."[53] Employees may also become dissatisfied if they feel as though their job functions don't align with the center's stated purpose (e.g. if analysts are performing tactical case support for a center that purports to have a strategic focus). This can result in the perception that the center's mission has shifted and make it challenging to recruit and retain talented individuals.

External stakeholders will also struggle to see the value provided by the fusion center, absent a clear communications strategy. For private sector stakeholders, a confusing or vague mission statement can make it challenging to understand how the center can support their operations. This may cause them to drift away or not participate in active partnerships with the center, which, in turn, can skew the center's understanding of what individuals and entities constitute its key customers. It can also be challenging for fusion centers to justify their budget or request additional resources from municipal and state legislatures if those legislators lack a clear understanding of how the center supports the community.

A clear, concise, and consistent messaging strategy is critical to communicating a fusion centers' value, but demonstrating that value requires an approach beyond the traditional cost-benefit analysis. BENS has partnered with the Tennessee Fusion Center (TFC) to apply commercial line insurance methodologies as a means for demonstrating value.[g] In the insurance market, Terrorist Risk Insurance is available to cover commercial structures with market driven premiums and high deductibles. BENS compared the TFC budget to an equivalent Terrorist Risk Insurance Act (TRIA) premium, covering the exposure of critical infrastructure, valued at $79 billion. The commercial premium for this amount of coverage would be approximately $5.4 million, $2 million greater than the TFC budget. In other words, this is comparable to an annual premium of $12.50 for a $250,000 home owner policy with a deductible of $87. Even the most parsimonious legislature would struggle to find a better bargain.

Information Federation. Recently, the PM-ISE convened an executive summit of state leaders who have been actively implementing state-based information sharing environments under their local authorities and appropriations but with national guidance, frameworks, and standards. The 15 leading states have demonstrated progress in maximizing their collaboration by using the infrastructure originally put in place to share counterterrorism information as a foundation to build network-based approaches to other challenges in today's complicated threat matrix. The summit produced a set of requests from the participating states, including more aggressive federal support in federating and integrating state and regional ISEs into the broader national information sharing environment.

[f] For more information, please see BENS' paper "Internal and External Messaging for Fusion Centers"
[g] For more information, please see BENS' paper "Alternative Valuations for State and Major urban area fusion centers"

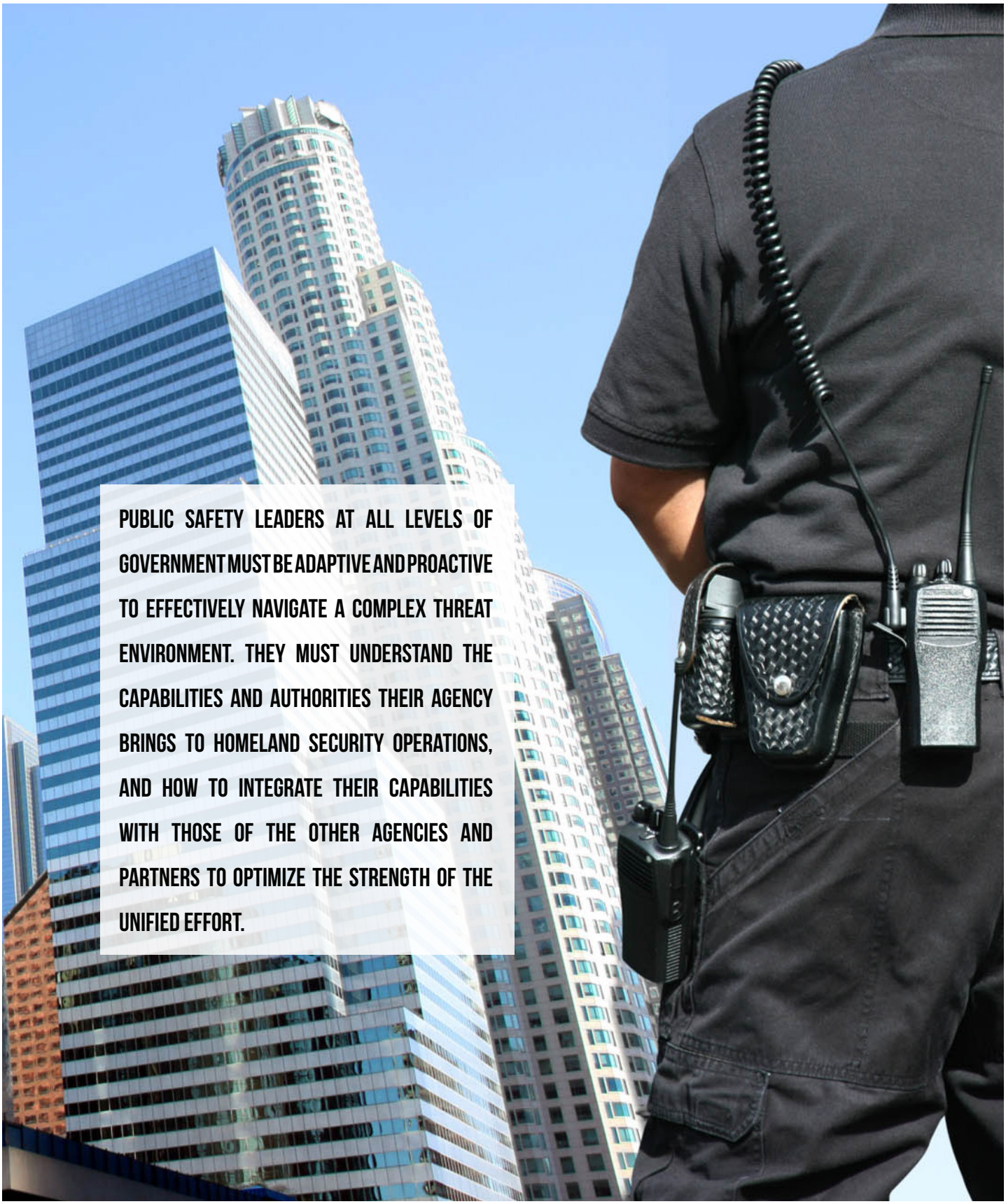
Improving Coordination at the State Level

State Homeland Security Advisors are responsible for coordinating and implementing the Governor's homeland security mission, and are the primary interlocutor through which DHS shares and receives information with each state. As such, HSAs serve a critical role in the US public safety network at the state level. Yet, active physical threats are not confined to state borders, and state leaders must address many of the same challenges (e.g. resource constraints). At a national level, HSA's impact on US public safety could be further enhanced through improved coordination with their peers at the state level, whether on a regional or state-by-state basis. This could be facilitated by improving the existing frameworks that allow HSAs to collaborate with one another, as well as with other state-level leaders. HSAs, Governors, DHS, and other appropriate parties must also give more consideration to creating a concept of operations that clearly defines the HSAs' roles and responsibilities as they relate to national public safety.

State Homeland Security Advisors are the Governor's primary representative to the DHS and responsible for executing the state's homeland security strategy, as defined by the Governor.[54] They are also empowered to act on behalf of the Governor during crises and in response to evolving events.[55] Because each state is unique, there is no uniform model for how HSAs are supposed to operate or organize themselves within the state. Overall there are 56 HSAs in the states, territories, commonwealths, and District of Columbia. According to the National Governors Association (NGA), more than half of all HSAs are a cabinet-level position (in some states, the HSA or public safety executive may have a direct line to the Governor but not be a cabinet-level position), and 75% serve multiple roles, including homeland security advisor, adjutant general, or chief public safety executive.[56] In fact, of the 56 total HSAs, only 14 are solely responsible for homeland security. This means that some HSAs operate according to different authorities or within different bureaucratic constraints.

IMPROVING COORDINATION AT THE STATE LEVEL | KEY TAKEAWAYS

- **HSAs serve a crucial role** for ensuring their state's public safety and coordinating among the various public safety and law enforcement agencies within their borders.
- HSAs, or other appropriate public safety, emergency management, or law enforcement leaders, must put **more focus on improving coordination with their peers at the state level nationwide**.
- More consideration should be given **to enhancing the existing national frameworks** to provide additional opportunities for HSAs to interact on an ad hoc basis.
- HSAs, state Governors, DHS officials, and other appropriate public and private sector stakeholders should **begin to map a national unified concept of operations** that articulates the roles and responsibilities of all stakeholders at all levels of government.



PUBLIC SAFETY LEADERS AT ALL LEVELS OF GOVERNMENT MUST BE ADAPTIVE AND PROACTIVE TO EFFECTIVELY NAVIGATE A COMPLEX THREAT ENVIRONMENT. THEY MUST UNDERSTAND THE CAPABILITIES AND AUTHORITIES THEIR AGENCY BRINGS TO HOMELAND SECURITY OPERATIONS, AND HOW TO INTEGRATE THEIR CAPABILITIES WITH THOSE OF THE OTHER AGENCIES AND PARTNERS TO OPTIMIZE THE STRENGTH OF THE UNIFIED EFFORT.

State Homeland Security Advisors can serve a crucial role for ensuring their state's public safety and coordinating among the various public safety and law enforcement agencies within their borders. Based on BENS' discussion with public safety officials, however, HSAs could place a greater emphasis on their role in ensuring US public safety beyond their state. To be sure, it is understandable that an officials' top priority would be serving the needs of his or her Governor. Further, although individual HSAs only have jurisdiction within their state, their mission, in partnership with DHS, can contribute to US public safety overall. Yet, a horizontal or networked approach to public safety is only as effective as its weakest link, whether that link is a fusion center, private sector stakeholder, or HSA. Moreover, networked integration can lead to interdependence among the various components, which can introduce new types of risk or the potential for cascading effects from one point in the network to another. Accordingly, in order to avoid any potential seams in the national public safety network, more consideration should be given to HSAs' role beyond their states—either on a regional or national basis.

Currently, the NGA provides a forum for HSAs to collect and disseminate best practices, and also convenes two meetings annually. Moreover, the NGA's Governors Homeland Security Advisors Council provides additional opportunities for HSAs to collaborate. Still, the complex nature of state and federal structures can make it difficult for federal, state, and private partners to collaborate with one another. This variation can make it challenging for federal and private sector partners to engage HSAs (or, for that matter, state and major urban area fusion centers) as a collective group, rather than on an ad hoc or bilateral basis. While those peer-to-peer relationships are important, a more robust and interconnected national framework could provide common points of entry where all partners can collaborate.

More consideration given to enhancing the existing NGA structure (or, in the case of fusion centers, enhancing the National Fusion Center Association) and providing additional opportunities for HSAs to interact on an ad hoc basis would strengthen their effectiveness. A strengthened national framework could allow HSAs more flexibly to share best practices, observe trends, and increase their situational awareness during emerging events on a regional or national basis, thereby further enhancing their value to their Governor and constituents. Collaboration among HSAs could be further improved by adding additional resources to the existing virtual HSA community of interest on HSIN.

Inter-state coordination may also be hampered by the absence of a national overarching concept of operations. This overarching construct could provide a common perspective from which to plan and coordinate operations in cooperation with state, local, and federal partners and would empower decentralized decision making in the absence of specific guidance for unforeseen threats. This document could also define the relationships among HSAs and other public safety stakeholders at all levels of government to ensure unity of effort and de-confliction along different and complementary lines of effort. HSAs, if fully empowered, can be a powerful integrator and interlocutor for the public safety entities within their jurisdiction and between the federal and SLTT levels. Existing interstate coordination models such as the Emergency Management Assistance Compact[57] or the All Hazards Consortium could provide a roadmap for bolstering other areas of public safety and homeland security.

Public safety leaders at all levels of government must be adaptive and proactive to effectively navigate a complex threat environment. They must understand the capabilities and authorities their agency brings to homeland security operations, and how to integrate their capabilities with those of the other agencies and partners to optimize the strength of the unified effort. HSAs, state Governors, DHS officials, and other appropriate public and private sector stakeholders should begin to map a national unified concept of operations that articulates the roles and responsibilities of all stakeholders at all levels of government.

V. CONCLUSION

"The Soft Changes"

Today's threat environment is complex. Terrorist entrepreneurs are enabled by technological innovations (including advances in communication and secure messaging technologies) to target privately owned establishments with increasingly deadly results. This requires a more collaborative and integrated approach to public safety, one in which the private sector, state and major urban area fusion centers, and state HSAs are adequately empowered and linked at the community level. Such horizontal linkages are critical to accessing and incorporating non-traditional sources of information and creating new partnerships with public health, education, religious, and civic leaders to utilize their unique perspective and strengths.

Implementing the networked practices this paper has examined will require consistent and attentive leadership to overcome bureaucratic inertia and cultural resistance to change that is resident in many public sector organizations. For example, as stated previously, operating from a "case-making" mindset can limit the type of information that a law enforcement official considers relevant. Federal intelligence and law enforcement also experiences constant leadership turnover which, combined with the human tendency to change the way your predecessor did business, can make it challenging to maintain cultural and bureaucratic consistency over time.

If the US public safety network is to become more horizontally integrated, attentive leadership will be necessary. Public safety leaders should view their role less as administrative task managers and more as orchestrators who encourage collaboration among and across functional teams.[59] In the private sector, effective managers are project-focused and mission-oriented; they evaluate employees against their contribution to the organization's mission, and focus on matching qualified people with the right project. As General McChrystal observed of his time in Iraq, "We didn't need every member of the Task Force to know everyone else; we just needed everyone to know someone on every team…"[60]

Training is critical to overcome behavior that is counterproductive to a networked approach and encourage consistent collaboration. The difficulty, however, is that behavior that may have contributed to an individual rising to the level of a manager may not be the same behavior that's needed to ensure they are a successful manager within a network. Indeed, effective leaders must practice extreme ownership of a situation and be willing to take responsibility for areas that are out of their direct control. Failure to do so may create seams in the national network at which emerging threats will tear.

More so than technical or procedural challenges, leadership and cultural challenges—the soft challenges—may be the most difficult to overcome. However, it's the soft challenges that must be addressed in order to strengthen our national public safety network and improve our ability to navigate a complex threat environment. Ultimately, it's the soft changes that will enable the hard ones.

IMPLEMENTING THE NETWORKED PRACTICES THIS PAPER HAS EXAMINED WILL REQUIRE CONSISTENT AND ATTENTIVE LEADERSHIP TO OVERCOME BUREAUCRATIC INERTIA AND CULTURAL RESISTANCE TO CHANGE THAT IS RESIDENT IN MANY PUBLIC SECTOR ORGANIZATIONS.

VI. REFERENCES

[1] Barbara Barrett, Matthew Duffy, Mel Immergut, Kelsey Keating, Philip Odeen, Atul Vashistha, and Jack Zoeller, "Report to the Secretary of Defense: Public-Private Collaboration in the Department of Defense," Defense Business Board, July 2012, Retrieved from: http://dbb.defense.gov/Portals/35/Documents/Reports/2012/FY12-4_Public_Private_Collaboration_in_the_Department_of_Defense_2012-7.pdf

[2] William Bratton, "The New Normal?" Aspen Security Forum, July 27, 2016, Retrieved from: http://aspensecurityforum.org/media/live-video/

[3] Michael Steinbach, "The New Normal?" Aspen Security Forum, July 27, 2016, Retrieved from: http://aspensecurityforum.org/media/live-video/

[4] Robert Griffin, "The New Normal?" Aspen Security Forum, July 27, 2016, Retrieved from: http://aspensecurityforum.org/media/live-video/

[5] Michael Hirsh, "Why Didn't the FBI Stop Omar Mateen?", Politico, June 17, 2016, Retrieved from: http://www.politico.com/magazine/story/2016/06/orlando-terrorism-fbi-omar-mateen-213971?utm_source=Sailthru&utm_medium=email&utm_campaign=Defense%20EBB%2006-20-16&utm_term=Editorial%20-%20Early%20Bird%20Brief

[6] Ibid.

[7] See for example: Lydia Alfaro-Gonzalez, RJ Barthelmes, Christina Bartol, Michael Boyden, Thomas Calderwood, Jeffrey Connor, Daniel Doyle, Carol Rollie Flynn, Jacob Green, Erin Herro, Taylor Johnson, Katelyn Lawrenze, Katharine McMaster, Margaret Nencheck, Neil Noronha, Lee Smith, Kathleen Walsh, Letitia Wu, and Kaila Yee, "Report: Lone Wolf Terrorism," Security Studies Program National Security Critical Issue Task Force, June 27, 2015, Retrieved from: http://georgetownsecuritystudiesreview.org/wp-content/uploads/2015/08/NCITF-Final-Paper.pdf

[8] Seamus Hughes and Lorenzo Vidino, "ISIS in America: From Retweets to Raqqa," George Washington University Program on Extremism, December 2015, Retrieved from: https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf

[9] Trapwire, "The Importance of Understanding the 'How' Rather than Just the 'Why' of Terrorism," Trapwire, June 20, 2016, Retrieved from: https://www.trapwire.com/blog/importance-understanding-rather-just-terrorism/

[10] The Joint Counterterrorism Team (JCAT), National Counterterrorism Center (NCTC), Office of the Director of National Intelligence, Retrieved from: https://www.nctc.gov/jcat.html

[11] Intelligence Reform and Terrorism Prevention Act of 2004, "Section 1016 Information Sharing," 2004, Retrieved from: https://www.ise.gov/sites/default/files/IRTPA_amended.pdf

[12] "Addressing the Challenges of Maintaining Robust State and Regional Information Sharing Environments," Information Sharing Environment (ISE), ISE Bloggers, June 6, 2016, Retrieved from: https://www.ise.gov/blog/ise-bloggers/addressing-challenges-maintaining-robust-state-and-regional-information-sharing

[13] Ibid.

[14] Program Manager, Information Sharing Environment, "ISE Annual Report to the Congress," Information Sharing Environment (ISE), August 2016, Retrieved from: http://www.ise.gov/annual-report/sites/annual-report/files/2016_ISE_Annual_Report.pdf

[15] Merrit Kennedy, "Investigators Say Orlando Shooter Showed Few Warning Signs of Radicalization," The Two-Way-NPR, June 18, 2016, Retrieved from: http://www.npr.org/sections/thetwo-way/2016/06/18/482621690/investigators-say-orlando-shooter-showed-few-warning-signs-of-radicalization RJune 15; Also: Kelly Mcevers, "Ex-Wife Reveals Orlando Gunman's History of Domestic Violence," All Things Considered-NPR, June 15, 2016 Retrieved from: http://www.npr.org/2016/06/15/482206228/ex-wife-reveals-orlando-gunmans-history-of-domestic-violence; Also: Max Bearak, Adam Goldman, and Joby Warrick, "'He was not a stable person': Orlando shooter showed signs of emotional trouble," Washington Post, June 12, 2016, Retrieved from: https://www.washingtonpost.com/world/national-security/ex-wife-of-suspected-orlando-shooter-he-beat-me/2016/06/12/8a1963b4-30b8-11e6-8ff7-7b6c1998b7a0_story.html

[16] Frances Robles and Nikita Stewart, "Dylann Roof's Past Reveals Trouble as Home and School," New York Times, July 16, 2015, Retrieved from: http://www.nytimes.com/2015/07/17/us/charleston-shooting-dylann-roof-troubled-past.html?_r=0

[17] William Horobin and Stacy Meichtry, "Attacker in Nice Showed Online Fascination with Islamic State," Wall Street Journal, July 18, 2016, Retrieved from: http://www.wsj.com/articles/french-police-step-up-investigation-into-bastille-day-truck-attack-1468847127

[18] Robert Griffin, "The New Normal?" Aspen Security Forum, July 27, 2016, Retrieved from: http://aspensecurityforum.org/media/live-video/

[19] Michael Hirsh, "Why Didn't the FBI Stop Omar Mateen?", Politico, June 17, 2016, Retrieved from: http://www.politico.com/magazine/story/2016/06/orlando-terrorism-fbi-omar-mateen-213971?utm_source=Sailthru&utm_medium=email&utm_campaign=Defense%20EBB%2006-20-16&utm_term=Editorial%20-%20Early%20Bird%20Brief

[20] Kelsey Landis, "Grandmother sought out help for teen charged with terrorism," Alton Telegraph, September 1, 2016, Retrieved from: http://thetelegraph.com/news/88698/grandmother-man-facing-terrorism-charges-suffered-from-mental-illness

[21] Dimple Agarwal, Tiffany McDowell, Don Miller, Tsutomu Okamoto, and Trevor Page, "Organizational structure: The rise of teams," in "Global Human Capital Trends 2016," Deloitte University Press, 2016, Retrieved from: http://www2.deloitte.com/us/en/pages/human-capital/articles/introduction-human-capital-trends.html

[22] Morgan Gareth, "Images of Organization," Sage Publications, 2006, Pages 91-92.

[23] Tim Kastelle, "Hierarchy is Overrated," Harvard Business Review, November 20, 2013, Retrieved from: https://hbr.org/2013/11/hierarchy-is-overrated

[24] Ibid.

[24] Ibid.

[26] Rachel Emma Silverman, "Who's the Boss? There Isn't One," Wall Street Journal, June 19, 2012, Retrieved from: http://www.wsj.com/articles/SB10001424052702303379204577474953586383604

[27] Ibid.

[28] "100 Best Companies to Work For: Section W.L. Gore & Associates," Fortune, 2016, Retrieved from: http://fortune.com/best-companies/w-l-gore-associates-12/

[29] Frank Rappa, "The Difference Between Vertical & Horizontal Business Organizations," Houston Chronicle, Retrieved from: http://smallbusiness.chron.com/difference-between-vertical-horizontal-business-organizations-24915.html

[30] PWC, "Hierarchy vs. network – A new business model for success," PWC, 2014, Retrieved from: http://www.digitalinnovation.pwc.com.au/hierarchy-vs-network-business-models/

[31] Dimple Agarwal, Tiffany McDowell, Don Miller, Tsutomu Okamoto, and Trevor Page, "Organizational structure: The rise of teams," in "Global Human Capital Trends 2016," Deloitte University Press, 2016, Retrieved from: http://www2.deloitte.com/us/en/pages/human-capital/articles/introduction-human-capital-trends.html

[32] General Stanley McChrystal, USA (Ret.), "Team of Teams: New Rules of Engagement for a Complex World," Portfolio/Penguin, 2015.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] Ibid.

[39] Dimple Agarwal, Tiffany McDowell, Don Miller, Tsutomu Okamoto, and Trevor Page, "Organizational structure: The rise of teams," in "Global Human Capital Trends 2016," Deloitte University Press, 2016, Retrieved from: http://www2.deloitte.com/us/en/pages/human-capital/articles/introduction-human-capital-trends.html

[40] W. Chan Kim and Renee Mauborgne, "Tipping Point Leadership," Harvard Business Review, April 2003, Retrieved from: https://hbr.org/2003/04/tipping-point-leadership

[41] Ibid.

[42] Andrea R. Nagy and Joel Podolny, "William Bratton and the NYPD: Crime Control through Middle Management Reform," Yale School of Management, 2007, Retrieved from: http://som.yale.edu/sites/default/files/files/Case_Bratton_2nd_ed_Final_and_Complete.pdf

[43] Ibid.

[44] Ibid.

[45] W. Chan Kim and Renee Mauborgne, "Tipping Point Leadership," Harvard Business Review, April 2003, Retrieved from: https://hbr.org/2003/04/tipping-point-leadership

[46] Ibid.

[47] Ibid.

[48] Andrea R. Nagy and Joel Podolny, "William Bratton and the NYPD: Crime Control through Middle Management Reform," Yale School of Management, 2007, Retrieved from: http://som.yale.edu/sites/default/files/files/Case_Bratton_2nd_ed_Final_and_Complete.pdf

[49] FBI Washington Field Office, "2013 Director's Community Leadership Awards", FBI, 2013, Retrieved from: https://archives.fbi.gov/archives/about-us/partnerships_and_outreach/community_outreach/dcla/2013/washington-field

[50] "Redirect Method," Jigsaw, Retrieved from: https://jigsaw.google.com/projects/#redirect-method

[51] "Against Violent Extremism Network," Jigsaw, Retrieved from: https://jigsaw.google.com/projects/#against-violent-extremism-network

[52] Standards Coordinating Council, 2015, Retrieved from: https://www.standardscoordination.org

[53] General Stanley McChrystal, USA (Ret.), "Team of Teams: New Rules of Engagement for a Complex World," Portfolio/Penguin, 2015.

[54] Carmen Ferro, David Henry, Thomas McLellan, National Governors Association (NGA), "A Governor's Guide to Homeland Security," NGA Center for Best Practices Homeland Security & Public Safety Division, November 2010, Retrieved from: http://www.nga.org/files/live/sites/NGA/files/pdf/1011GOVGUIDEHS.PDF

[55] Ibid.

[56] Ibid.

[57] Emergency Management Assistance Compact (EMAC), National Emergency Management Association (NEMA), 2015, Retrieved from: http://www.emacweb.org/

[58] All Hazards Consortium (AHC), 2015, Retrieved from: http://www.ahcusa.org/

[59] Sohrab Vossoughi, "Today's Best Companies are Horizontally Integrated," Harvard Business Review, December 14, 2012, Retrieved from: https://hbr.org/2012/12/todays-best-companies-are-hori

[60] General Stanley McChrystal, USA (Ret.), "Team of Teams: New Rules of Engagement for a Complex World," Portfolio/Penguin, 2015.


F.D.N.Y.

Business Executives for National Security

1030 15th Street, N.W.
Suite 200 East
Washington, D.C. 20005

www.bens.org