



Calhoun: The NPS Institutional Archive
DSpace Repository

Center for Homeland Defense and Security (CHDS)

Homeland Security Affairs (Journal)

2018

Homeland Security Affairs Journal, Volume 14 / 2018

Monterey, California. Naval Postgraduate School, Center for Homeland Defense and Security

Homeland Security Affairs Journal, Volume 14
<http://hdl.handle.net/10945/62007>

The copyright of all articles published in Homeland Security Affairs rests with the author[s] of the articles. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. Anyone can copy, distribute, or reuse these articles as long as the author and original source are properly cited.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



HOMELAND SECURITY AFFAIRS

VOLUME 14 / 2018

The image is a composite. The top half shows a soldier in a desert environment, viewed from behind, carrying a rifle. In the background, a military vehicle is parked on a dirt road, with another soldier standing nearby. The bottom half of the image shows a close-up of a soldier's legs in camouflage pants and a tan jacket, walking on a dirt path. The overall scene is set in a dry, outdoor environment under a clear sky.

Defected from ISIS or Simply Returned, and for How Long?-- Challenges for the West in Dealing with Returning Foreign Fighters

By Anne Speckhard, PhD., Ardian Shajkovci, PhD., & Ahmet S. Yayla, PhD.

Abstract

Many of the 38,000 foreign fighters ISIS has managed to attract to Syria and Iraq will return home. As increasing numbers of ISIS cadres flee the battlefield, some as defectors and others as returnees still aligned with ISIS' goals and ideology, the challenges for the West will be how to identify and sort out true defectors from returnees, and determine if they are at risk to support again or rejoin a terrorist group. In this context, the authors of the article stress that it will be incumbent on Western states to find adequate ways of determining who among returnees is a security risk at present, who may become one in the future, specifically by returning their allegiance to this violent group, and who can be safely reintegrated into society for the long term. The authors also highlight important policy alternatives for dealing with returning foreign fighters who will continue to pose both an immediate security threat and a long-term challenge.

Suggested Citation

Speckhard, Anne, PhD., Ardian Shajkovci, PhD., & Ahmet S. Yayla, PhD. "Defected from ISIS or Simply Returned, and for How Long?-- Challenges for the West in Dealing with Returning Foreign Fighters." *Homeland Security Affairs* 14, Article 1 (January 2018). <https://www.hsaj.org/articles/14263>

Introduction

The U.S. Pentagon has reported a considerable drop in the number of foreign fighters flowing to Iraq and Syria, from 2000 to 500 a month according to some estimates.¹ While such numbers are encouraging and offer evidence of foreign fighter attrition from Iraq and Syria, one must not underestimate the rate at which the group continues to replenish itself, which according to some sources, is far greater and faster than that of al-Qaeda at its peak.² The "Islamic State" also continues to suffer significant territorial losses in Iraq and Syria.³ Such setbacks are likely to continue to weaken the group's recruitment campaign and efforts, especially important given that the group also relies on recruits from the territories it controls.⁴

Despite the significant setbacks in the battlefield, ISIS continues to attract followers. During our *ISIS Defector Interview Project*, we interviewed dozens of defectors and foreign fighters from Syria, Europe, Central Asia, and the Balkans who had served in "Islamic State" controlled territories. We found that a vast majority of these were truly defectors, and no longer support or ever intend to go back to the ranks of ISIS in Syria and Iraq, or to serve them at home. However, we also found that some were more accurately viewed as "Islamic State" returnees, but not defectors, having only temporarily disengaged from the battleground—sometimes even being allowed to temporarily return home by the group, or more chillingly, sent home to recruit or otherwise serve the group's goals in the West. These returnees remain aligned with the so-called "Caliphate" and contemplate returning to Syria and Iraq and, in some cases, we learned that they have already returned to the battlefield and rejoined the terrorist group. Some of those who truly defected from ISIS, even risking their lives to do so, also returned to supporting or actually returned to the group. In the

case of some of these defectors, despite having disavowed ISIS for a considerable period of time, the challenges of living back home caused them to flip and return to the group. Some were actually contacted by ISIS, or unable to reintegrate well at home, and again took up the cause. This article relies on a sample of sixty-three ISIS defectors/returnees imprisoned by authorities, collected between May 2014 and August 2017.

The sample of nine out of sixty-three total was collected between May 2014 and February 2017 from returnees of Western European and Balkans countries as well as Syrians fleeing ISIS by escaping into Turkey. One of the returnees was interviewed in a prison setting. He was imprisoned by the authorities following his defection from ISIS and return from Syria. Interviews were conducted in a semi-structured manner, allowing the participants to tell their stories of being recruited into the group, serving, and then defecting, followed by detailed questioning involving a series of twenty-five questions and going in depth on topics they had personal experience with inside the group. The defectors were judged to be genuine on the basis of four things: referral from prison authorities and prosecution records, referral from defectors who knew them from inside the group, insightful knowledge about experiences inside the group, and intense post-traumatic responses during the interview evidencing they had been present and taken part in events they were describing. The subjects were contacted via smugglers, other defectors, personal introductions, and via prison authorities, thus the sample is entirely nonrandom. The defectors did not give their real names except for those in prison or already prosecuted.

Before and during the course of the research, the participants were informed about the authors' credentials in the field of counter-radicalization and counter-terrorism so as to secure interviews. The participants were informed that this research is part of a larger research project and is not sponsored or reporting to law enforcement. Informed consent was gained from each participant, with special care taken for those in prison to ensure they were speaking freely and knew that they may be under surveillance that neither they nor we could control. In the case of those interviewed in prison, the authors filed proper applications to gain access to the correctional facilities, and abided fully by the policies and procedures of those facilities. The authors did not pose any questions that could lead to the disclosure and admission of potential crimes or participation in illegal activities. This was important in the sense that it represents an ethical issue and any potential disclosure of incriminating evidence may be utilized against our participants in a court of law. That said, the interviewees were fully aware that in the event they voluntarily disclosed incriminating information, such as information about an impending attack, the principle of confidentiality would no longer apply. Our results cannot be generalized from this non-representative and small sample to apply to all returnees/defectors, yet the issues these interviews raise are deeply important for policy considerations in dealing with ISIS returnees because they describe the pathways into terrorism and back out for some, and how some at least deal with having returned from the conflicts in Syria and Iraq.

Some security experts predict that as ISIS continues to lose territory and its brutal grip on local populations in Syria and Iraq, it will migrate to other territories, with Southeast Asia (Philippines, Malaysia, and Indonesia), Libya, and even the Balkans being cited as possibilities.⁵ When we interviewed Syrian defectors from June 2015 to February 2017 in the *ISIS Defectors Interviews Project*, many told us that in the event of losing their territory in Syria and Iraq, ISIS cadres plan to shave their beards and blend into normal society in Syria and elsewhere to mount guerilla warfare attacks.⁶ Certainly, of the 38,000 foreign fighters ISIS has managed to attract to Syria and Iraq, many will return home—some disaffected

and defecting from the group, some disillusioned in the short-term but still longing to build an Islamic “Caliphate,” and still others sent back to recruit and attack at home. Already Western consulates in Turkey report an increase in their citizens showing up to report “lost passports” and wishing to return home.⁷

As ISIS continues to lose most or all of its territory, it is important for Western governments, particularly from the Balkans and Western Europe, to prepare for the reality that in this flood of returnees only some will be defectors, while others will simply be returnees who will continue to support the Islamic State. Many of these returnees will be dangerous and may return to Syria and Iraq at some point, or go elsewhere, or act at home on behalf of ISIS or its potential successor organizations. Whether all returnees from ISIS constitute a danger to their homelands is unknown, although those who left ISIS but are not necessarily defectors nor disillusioned with Islamic State’s claim to be able to construct a utopian Islamic Caliphate are likely more easily manipulated to attack at home and return to service. In our interviews, we found the dream of the “Caliphate” was a very potent one, and while many understood that ISIS would never be able to deliver it, that nevertheless remained as a hoped-for ideal.

As increasing numbers of ISIS cadres flee the battlefield, some as defectors and others as returnees still aligned with ISIS’ goals and ideology, the challenges for the West will be how to identify and sort out true defectors from returnees and determine if they are at risk to flip back again to supporting or rejoining the group. It will be incumbent on Western states to find ways of determining who among returnees is a security risk at present, who may become one in the future (e.g. by returning their allegiance to the group), and who can be safely reintegrated into society for the long-term. The questions for those handling the likely flood of ISIS returnees include identifying the variables that can be manipulated potentially to lessen the possibilities of return to the group. This article offers a small insight into those returnees who have not entirely renounced ISIS, or who have re-connected with the group over time, identifying what appeared to be the causes.

Sample

This analysis is based on nine cases chosen from a total of sixty-three ISIS defectors/returnees imprisoned by authorities (See Chart 1). The sample of sixty-three was identified by the smuggler who had brought them to Turkey, via a defector network, by virtue of their cases being public and having gone through prosecution, or because of the fact that they were imprisoned as ISIS (or in the case of the two Central Asians as ISIS affiliate) members.

Table 1 ISIS Cadres Interviewed

Total # of ISIS Cadres Interviewed	63
Countries Interviewed	Syrians in Turkey (33) Western Europe (3) Central Asians (2) Balkans (7)(1 Prison) Iraq (18) (18 Prison) Total: 63
# ISIS defectors reversing their decision or continuing their loyalty to ISIS (also subjects of this paper).	9

Nine Cases Discussed

The age of the participants at the time of the interview ranged from fifteen to forty-nine, with the majority being under thirty. Their professions before joining ISIS included farming, trade, and professional jobs, with the majority being blue collar, farm workers, or unemployed. All but one of the nine cases were men. Of the nine cases culled for this analysis, one was female, one was a minor, and the rest were adult males. These nine cases (the returnee or the defector representing all geographic areas of the sample) were specifically selected from the rest of the total sample because, unlike others, they: 1) expressed conflicting feelings about having left ISIS; 2) expressed the potential desire to return to the group; 3) expressed outright, continued affiliation and support for ISIS, and/or; 4) we learned that the person actually returned to fighting with ISIS.

Methods

All of the nine defectors were interviewed in-depth using a semi-structured interview instrument (with open-ended questions included) between May 2014 and February 2017. One of the interviews took place in a prison setting. The person had defected, but was arrested by the authorities upon his return. Most interviewees did not give their names and real names are used only for those whose cases are public and already in the press. The interviews served to develop an understanding of their motivations for joining ISIS, what attracted them, what they found positive, how they were trained and ideologically indoctrinated into the group, what they witnessed inside ISIS, and what disturbed them enough to defect or to leave for those who did so.

For the forty-five out of sixty-three interviewees who were true defectors, their main reasons for leaving included the brutality and corruption of ISIS (including its hypocritical and un-Islamic nature), being coerced into actions they found morally or otherwise repellant, and sheer terror for their own or family members' lives.⁸ Note that Speckhard and Shajkovci interviewed sixteen ISIS cadres imprisoned in Iraq, and with the exception of one prisoner, they could not determine their current level of support or loyalty for ISIS.

With the exception of the nine who continued or clearly returned their allegiance or who physically returned to ISIS, we could not determine if the remaining sample of interviewed ISIS defectors/returnees who denounced ISIS at the time of their interview ever returned to ISIS or expressed allegiance once again to the group. The nine who continued or clearly returned to their allegiance, or who actually physically returned to ISIS, are the subject of this analysis with the focus being on their motivations for doing so and the potential factors regarding their decisions to continue or return to supporting ISIS.

Results

Out of the sixty-three interviewed ISIS cadres, we found nine of them to have either reversed their defection by returning to the battlefield or to have continued their ideological commitment to ISIS. Among the nine subjects who, despite having left the group, were conflicted about ISIS and continued or returned to supporting the group (physically or

ideologically), one was Belgian, three were Albanians from Kosovo, two were Bosniaks, and three were Syrians in Turkey. We know that four of these physically returned to the group, and one who was jailed in Kosovo had come and gone previously and flipped again back to ISIS in prison.

Reasons cited for leaving ISIS included homesickness, battle fatigue, fear of ISIS leadership, disillusionment with ISIS living up to its utopian ideals, problems that needed attending to at home, anger over ISIS hypocrisy and/or mendacity, and the prospect for females of being forced to remarry. Yet despite this, upon return to their home countries, or in the case of Syrian defectors fleeing to Turkey, they expressed allegiance to the group, with nearly half returning to it. While our research ethic was never to ask our respondents to directly incriminate themselves, including asking them directly if they still wanted to return to ISIS, it became clear to us from what they voluntarily offered that of these nine subjects, all of them either continued or returned their allegiance to ISIS at some point after leaving the group and that half of them actually returned to the ISIS battlefield.

Discussion

After interviewing more than five hundred terrorists (or their family members and close associates when they are already dead) between us, it is clear that the individual vulnerabilities and motivations for joining terrorist groups are always contextual and vary even by neighborhood, even within the same city.⁹ The same is true for this sample.

Among the thirty-three Syrians interviewed in our sample of sixty-three, the desire to join the uprising against Assad, alongside heavy coercion from ISIS, was a huge factor for joining the group. Some of the fighters from other militias joined the “Islamic State” only when they were captured and offered a choiceless choice: die or join the group. Other Syrian militia members joined ISIS voluntarily, citing it as more Islamic, more successful in battles, and better financed in terms of weapons and providing better salaries than their group—reasons they gave for switching allegiances. Likewise, the Syrian respondents told us that Syrian youth easily believed the lies of ISIS preachers who promised youth unheard-of salaries, marriages, and even cars if they joined. This happened despite the fact that many of the *Cubs of the Caliphate* were actually groomed for vehicular suicide missions and received only some of these rewards. Local Syrian civilians who joined ISIS also referenced the fact that when ISIS overtook their areas, “Islamic State” took over all the means of employment and sustenance in the territories they controlled, and that to fail to join meant suffering, possible targeting for punishments, and potential starvation. Female Syrians told us, and male Syrians confirmed, that local Syrian women also often married into ISIS as a means of feeding themselves and their families.

European foreign fighters, by contrast, were repeatedly referenced by the Syrians as already indoctrinated into Salafi militant jihadi ideas before coming to Syria, and were seen as the “true believers” who had come for “jihad.”¹⁰ Western foreign fighters, male and female, enjoyed exalted status above the Syrians in the “Islamic State” and were given many perks including free housing, arranged marriages, sometimes cars—and for the men, sex slaves.¹¹ Our interviews in Europe and the Balkans point to a completely different set of motivations for joining ISIS than many of the Syrians had. High unemployment in the Balkans and in Muslim enclaves in Europe, alongside the marginalization and discrimination of first and second-generation Muslim minorities in many Western European countries, played an important

role in these recruits finding ISIS attractive. Offers of a real salary, arranged marriages, sex slaves for men, traditional living for women, free housing and other amenities, along with the honors bestowed by ISIS on foreign fighters who come to Syria and Iraq, attracted many who also felt their lives to be lacking dignity, purpose, significance, and honor.

More importantly, however, our total sample of interviews revealed that the significance of the ISIS captured territory and what appeared to be the real possibility of establishing a utopian Islamic “Caliphate”—given the oil wealth and battlefield successes of ISIS—were strong motivating factors for joining. The dream of the “Caliphate” was important to them.

Those from the Balkans who went early on to join the uprising against Assad and later found themselves in the ranks of ISIS also referenced their own personal experience of war as children and youth, and the duty they felt for Muslims to defend one another from tyrannical and violent leaders and unjust attack.¹² In fact, all of those interviewed in Kosovo by Speckhard (n=6), referenced the fact that others, including Americans, had come to save them from killings and rapes decades ago, and that now it was their Islamic duty to help Syrians defend themselves from Assad’s atrocities—events they had viewed on video and found extremely disturbing. However, once in Syria, they discovered the unexpected complexities of multiple actors with differing goals and the various militias warring with each other. Those we interviewed left while others who stayed in Syria became enamored of what became the Islamic State.

Likewise, many foreign fighters from Central Asia, Europe, and the Balkans were recruited into “Islamic State” by friends and family members, or with offers of marriage—creating and deepening already existing friendship and familial bonds—making it harder to exit the group. Some of the reasons we identified that seem to draw foreign fighters back to the group include: the friendships and camaraderie that also arose between foreign fighters, along with their deepened Islamic identities, sense of purpose, significance, heroism and dignity forged in ISIS; the material as well as spiritual rewards of participation; the potential of dying for a greater purpose with the religious promises of “martyrdom,” versus living a life of ennui; and the manner in which the group promoted its brand as representing an ultimate quest for Muslim dignity, self-rule, and justice. Whereas Syrians were more aware of the brutalities of ISIS toward other Sunnis (e. g. the decimation of the Sunni al-Sheitaat tribe) and their hypocritical lies, the Syrians in our sample also expressed vulnerabilities to returning to ISIS, such as longing for “true” Islamic living and Syrian freedom with the overthrow of Assad, as well as having become invested in the possibility of a real Islamic Caliphate.

Alongside the motivations for joining, the problems facing foreign fighters back home—factors that played in their decisions to join such as high unemployment, underemployment, discrimination, marginalization, difficulty living a conservative Salafi lifestyle in the West, messy and unsatisfying family relationships that they had fled—all still existed as problems once they returned home. And these problems continued on without new or satisfying solutions. In addition, having lived in a conflict zone and having witnessed and taken part in extreme brutality also took a heavy psychological toll upon returned ISIS cadres, who now in safety told us of enduring symptoms of post-traumatic stress disorder (PTSD). Their high arousal states in particular—feeling jumpy, fidgety, and on high alert—do not match the calm, bored ennui of being back home, or of hiding in Syria without a clear purpose. Equally important, they are lacking good psychological treatment along with the ability to safely admit the disturbing things in which they took part. Many returnees long again for the

clarity of purpose and experiences of the battleground with the potential rewards of death by “martyrdom.” Only one returnee in our sample received psychological assistance—an Albanian from Kosovo who was offered psychological help in France for the traumas of having served in “Islamic State.” He stated that before taking the offered therapy he suffered nightmares and what sounded like symptoms of PTSD, but that the treatment greatly helped him to reintegrate. Some of the aforementioned factors also serve to explain why some foreign fighters seem to overlook the group’s limitations and territorial setbacks, dismissing reality while hoping for the best upon return.

Case Examples

ISIS, like al-Qaeda before it, has been adept at convincing adherents that to die killing enemies of the group is to die a “martyr’s” death with all the Islamic rewards of “martyrdom” conveyed to the suicide terrorist. Of course, most Muslims would not recognize this terrorist ideology as their Islam. Yet, during the course of our interviews we have learned how the group has managed to hijack Islamic scripture by promising fighters that suicide terrorism is an act of “martyrdom” that wipes away sins, gains the adherent immediate entry to Paradise, and grants family members Paradise upon their deaths as well. Our defectors told us of many Arabs and some Westerners who joined ISIS for the express purpose of gaining a “martyr’s” death—even volunteering for suicide missions. When one is faced with a seemingly insignificant and purposeless life, and problems of rampant unemployment, or if one is carrying guilt over “sins,” a significant death with an immediately improved afterlife can become an important allure to returning to ISIS, as one of our Balkan defectors told us:

I am thinking about it [returning to Syria]. There is a possibility. There is a bigger purpose in dying than staying here. Here is worse than you think. The cause I was fighting for, the brotherhood, and the life I had in Syria was powerful. I had a reason both to live and to die. I had a reason to live because I had income and food on the table every day. I also did not mind dying because I believe in God and justice. What I mean is that I don't have to worry about starving, like here [in Kosovo]. I have stability, and I don't mind dying because it is for a greater purpose: to free innocent Muslim brothers and sisters who are being killed every day. (D.K, age thirty-five, interviewed in June 2015, Kosovo)¹³

A thirty-four year old Albanian Kosovar explained how he had found purpose and meaning in ISIS and only returned for a short time to Kosovo—for a break from the battlefield, “I am temporarily disengaged. I will return. I have established my life in the Islamic State. This [Syria] is my new home.” He denied defecting saying,

Defecting means switching allegiance and commitment. I have not abandoned my brothers and sisters in Syria. I will be there for as long as I need to. I will help my brothers and sisters in Syria. It is my new career and my new life. Even though I love my family in Kosovo, I have found a new purpose in life (R.B., age thirty-four, interviewed in March 2016, Kosovo).

Two middle-aged men who went to join ISIS from Bosnia but had returned to be with their families stated, “Our families are in Bosnia. The war is not over yet. We hope to bring our families to live with us in the Islamic State.” (M.S., age forty-seven and B.I, age forty-nine, interviewed between May and September 2014, Bosnia and Herzegovina)

Another thirty-five-year-old Albanian Kosovar explained that it is hard to reintegrate into a society that labels those who went to assist in the uprising in Syria as terrorists and that he intends to return to ISIS, “[There is] no reason to live here, stigmatized by Kosovars. Difficult to return when people call you a terrorist.” (A.K., age thirty-five, interviewed in June 2015, Kosovo)

Syrian defectors in Turkey also told us about languishing in refugee camps and looking impatiently back to ISIS, idealizing what they had defected from and hoping still that ISIS could liberate their country from Assad. One defector stated :

I complain to my friends here in Turkey [about ISIS atrocities]. I always complain to them. I tried to convince them, at a time when they tried to convince me to go back. “Let’s go back. We will have money and pay.” I told them, “Money is not everything. You need to be patient here. Inshallah, you will feel relieved soon. It won’t be long. It won’t be long. They [ISIS] are not righteous.” They didn’t believe me. A lot of my friends went back and they are still there. The others were convinced because I told them about the reality of things. (Abu Yousef, age twenty-nine, interviewed in November 2015, Turkey)

Syrian Tahir, age fifteen when we interviewed him, returned to ISIS despite having become disaffected with ISIS cadres tricking small children into suicide missions and also pushing him to take one during his time inside Islamic State. He returned after ISIS fighters came and told him that they could take his town back from the Kurds but needed his help as a guide. Homesick and desperate to return home, he was easily manipulated by them. Tahir, we later learned through those who knew him, was killed on a landmine as he tried to guide the fighters in their unsuccessful bid to overtake his village. (Tahir, age fifteen, interviewed in November 2015, Turkey).

Umm Rasheed, a twenty-one-year-old Syrian woman who had been indoctrinated by ISIS after being orphaned as a teen and married into the group, was forced by circumstances into three serial marriages (after each husband died in battle). The single mother of a small child had been living in a Turkish refugee camp for nine months but still expressed deep confusion about ISIS when we spoke to her in Turkey. Her case made it clear to us that those who escape from terrorist groups need supportive therapy and remain deeply vulnerable to the ideologies they have been forced to live under, especially if they fell under ISIS rule as youth, as she did.

Despite having run from them when she believed they would force her into yet a fourth ISIS marriage, Umm Rasheed appeared completely disoriented in her life in Turkey, telling us, “I would do the same thing again if given the opportunity. I escaped because I have a small child, but I want to go back after the baby is grown. I want to go back. When my son is three or four years old, if ISIS still exists, I will go back and fight with them.”

Having known poverty in her family home and then repeated tragedy in her late teens as her parents and three husbands were all killed and then knowing poverty again as a refugee, she idealized the prosperity and powerful position she had briefly held in ISIS, married to a Saudi foreign fighter and being herself a member of the ISIS *hisbah*. She claimed, “ISIS is a really good group, I have to help them. If they allow me to keep my son, I would marry [again] but I don’t know yet. They are not as bad as people tell. ISIS is good. Woman are covered over there.”

Like many who had fallen under the total indoctrination of ISIS, she still believed that “Islamic State” represented the true Islam and all others were enemies. She also had personal experience to back up some of her beliefs. She had been relatively rich in ISIS until each of her husbands were killed in battle. Likewise, she had seen the civilian killings caused by Coalition bombings that made her conclude that the West was an enemy to Syrian civilians, “Those coalition forces are not killing us, our soldiers, but they are attacking civilians, and everyone sees that.” She claimed to have seen dead women and children killed by Coalition airstrikes as well.

While she had risked her life to escape ISIS and was clearly relieved to be away from the battlefield and not forced to remarry yet a fourth time, she still idealized the “Islamic State” and was unclear about what to believe, “They lie about us and create negative propaganda,” she said of the West. Also having so many of her close family killed in battle and having been taught by ISIS that they were “martyrs,” it may have been hard for her to let go of this idea. When asked about others joining the group, she said,

Advise them to come and join ISIS. Go! Die in the road of Allah. When you die for the religion you save yourself. I want my child to be an ISIS fighter and martyr. That son must go through the way of his father, follow his path, I wish I was a ‘martyr’ as well. I can die when he’s ten. Martyrdom is the most important rank you can reach.

When asked if she would take other Syrian refugees back to ISIS with her, she answered,

Of course if someone wants to go I will take them. I invited a lot of women in Raqqa to become ISIS members. Inshallah, ISIS will become the real state of the region and I will become the martyr for them. What you hear here is all lies. You think they won’t last but if you go to Raqqa you see everyone is living peacefully there.

Having lost her girlhood dream of becoming a doctor, her parents having been killed by regime bombings, and having to marry young and repeatedly with little chance to grieve and then having been trained by ISIS as a young woman to be sadistic in torturing other women who infringed upon their strict rules, it is likely this widowed single mother was so traumatized by all she had seen that she could not clearly work through ISIS claims of being righteous (Umm Rasheed, age twenty-one, interviewed in May 2016, Turkey).

In Belgium, 27-year-old Younes Delefortrie (his real name) told of being raised by an alcoholic and violent mother and feeling that the Catholic Church he regularly worshipped in as a child had failed to protect him. When introduced to Islam by second-generation North African Belgians who have strong extended family ties, he was captivated by a religion that bans alcohol and immediately converted. He gave up drugs and alcohol and over time moved beyond those Muslim friends to an extremist version of Islam and eventually went to Syria in 2013. Delefortrie spent only five weeks in Syria in a group composed of al-Nusra and ISIS cadres and returned to Europe when the groups started fighting each other, giving as his reasons that he wanted to make a better living, reunite with his wife, and escape the battleground.

Yet, when he returned to Europe, he was returning to a troubled marriage, a conviction on terrorism charges, release on a travel ban, and overall failure. After having tried to restart his life, he had his business shut down by Gert Wilders, who complained that his bakery loaves “have blood on them.” Disillusioned with life in Belgium, Delefortrie expressed in

his interview his wish to return to ISIS. Idealizing their “Caliphate”, he justified the 2015 Bataclan Paris attacks as retaliation for Coalition bombings and said he hoped for the ISIS “Caliphate” to extend to Brussels. Journalists who have interviewed him at home report an ISIS flag hanging in his bedroom and Delefortrie dressed in a hoodie adorned with the ISIS flag. The judge who decided Delefortrie’s case saw him as not enough of a danger to society to lock him up; however, there are clear signs of his vulnerability to rejoin old comrades and his continued adherence to an ideology that addresses his childhood traumas and that supports terrorist attacks on European soil. His case would seem to support an argument for providing remedial therapy for ISIS returnees (Younes Delefortrie, age twenty-seven, interviewed February 2016, Belgium).

Fitim Lladrovci (his real name), a twenty-five-year-old Albanian Kosovar interviewed in prison in Kosovo, raises many of the war-related issues associated with others from the Balkans who went to Syria. As a young boy, Lladrovci had witnessed his own family attacked by Serbs and vividly recalled that an American woman had saved their village. He, like many of the other Albanians who initially went to fight against the Assad regime, recalled how traumatized and helpless they felt during their war. As a result, he felt that it was his Islamic duty to help. He, like the others interviewed, felt that the Kosovo government had supported Albanians going to help with the uprising in Syria, but later hypocritically condemned him as a terrorist. Lladrovci travelled first to Syria in 2013 and joined the Free Syrian Army for four months. Like many Albanians in the conflict zone, he became disenchanted when the militias started turning on each other and returned home. Recalling that time, he stated, “I joined the FSA. [When they] started fighting al-Nusra, I decided to return to Kosovo.” Despite trying to return to his normal life, he kept abreast of developments in Syria, particularly the rise of ISIS, as he became enamored of their claim for an Islamic “Caliphate.”

Lladrovci had, during his brief time in Syria, met many of the Albanian foreign fighters who later became leaders in ISIS, so he knew he could play an important role if he joined. Recalling how he tried to settle back into normal life in Kosovo, Lladrovci stated, “I got back and tried to move away from those kind of things, go back to my own life, but it was impossible. When I saw ISIS created, my desire [to return] was so great. The second trip in ISIS was totally exciting. The first time was boring, just guard duty.”

Like many of the Albanian foreign fighters from Kosovo, Lladrovci expressed extreme disappointment with the Kosovo government for criminalizing his initial acts of fighting with the Free Syrian Army to assist in the Syrian uprising and equating it to joining a terrorist group, more specifically,

Once I came back in 2014, arrests started to happen in Kosovo and police took me in to question me. ... They came and arrested me, took my computers and phones. They found evidence. It wasn't like I didn't admit it. I told them I went to [Syria to] help the people. It shouldn't be a surprise. Even the Kosovo Islamic community made a call for going [to Syria] and helping, so it wasn't like I ever denied it.

Yet, despite there being no law on the books in Kosovo for joining the uprising in Syria at the time he served the Free Syrian Army, his act of helping the Syrians was criminalized as terrorism. “[I was] put on the potential terrorist list. Arrested for nine hours. At the time, we didn't have a law,” Lladrovci recalled, obviously angry about what he saw as hypocrisy on the part of the state. Lladrovci, however, also had a criminal streak—with a history of stealing and petty criminality in his early life (according to those who knew him)—and he easily lied

to the government, “In front of prosecutor I said that I regret and have no intentions of going back. He believed me. I went home and the first thing I did was contact the people in Syria.”

As ISIS declared its “Caliphate”, Lladrovci became excited by the idea of joining and getting in on the ground floor. The first time in Syria he had left his wife behind, but this time he recalled, “It was at that period, people were taking their wives, wives were joining their husbands. Why not? I can do that too. So, I got in touch with Lavdrim Muhaxheri and Ridvan Haqifi, [They were] big shots at the time. I made some very good connections since my first time.” Material considerations played a part as well. Lladrovci told his ISIS friends that he wanted to bring his wife and asked them, “Can I get a house?” The answer back, “Yes conditions here are excellent for you. We are just waiting.”

Lladrovci continued to misrepresent himself to the authorities, recalling,

I started searching for ways how to get there. I decided to go from Montenegro. I took a bus with my wife, flew from Podgorica. I was on the [potential terrorist] list so once I got to the border of Kosovo, I didn't need a passport to cross to Montenegro, I showed my ID—they saw the name and questioned me. “Yes, I've been to Syria but now we are going to Ulcinj and taking my wife. We are going to work. My wife shouldn't be punished, for a stupid decision, why should she suffer?”

Lladrovci lied charmingly to the authorities and passed into Montenegro unstopped.

Once inside ISIS, Lladrovci recalled fighting for ISIS on an almost daily basis and had no regrets whatsoever about ISIS killing civilians, taking sex slaves, beheading so-called spies and enemies of the “Islamic State,” and killing other Sunnis—most notably decimating the al-Sheitaat tribe in a genocidal battle where thousands of men, women, and children were killed by ISIS. He had so completely drunk the ISIS poisonous ideology of believing the “Islamic State” was righteous that he rarely questioned their brutalities or corruption.

However, when he began to witness discrepancies that reflected his own life and values as they were played out upon insiders, he became upset with the leaders of ISIS. Lladrovci, whose father died when he was young, was raised by his mother and perhaps easily felt sympathy for widows. Likewise, he had vivid recollection of himself, his mother and an older brother being attacked by Serbs when he was only eight—an age that he would also relate to during his time in ISIS.

Lladrovci recalled, “When wives got sick they [ISIS] wouldn't take them to the hospital. They can't travel alone. [According to ISIS] wives are only there to cook and take care. For me that was a huge sign something is wrong.” Lladrovci's wife fell ill and was not cared for by ISIS. He continued, “There was not only my case, there was another person's wife. She was sick with cancer, had four kids. They didn't take care of her or allow her to go back [home for medical treatment].” He also became upset seeing that ISIS was only paying a widow's pension for the first month then refusing to pay further payments and not helping the women to get out to buy necessities, effectively forcing these women to remarry in order to survive.

As is the case with many who join ISIS, part of the attraction to the group is its promise to deliver justice and dignity to all Muslims. Lladrovci was no different in this regard. He became enraged when he saw hypocrisies and injustice as it applied to ISIS members. His refusal to simply follow the group motto of “hear and obey,” and his tendency to speak out about these injustices did not endear him to the ISIS leadership. He recalled, “I told you

I cannot tolerate injustice, so I always confronted them [the ISIS leaders] and argued. At some point, we even went to the *shariah* court. Because of that they started distancing themselves from me.”

The final straw for Lladrovci was an eight-year-old child who probably represented for him, his own fatherless, boyhood, unprotected-self during war. “So, there was this eight-years-old kid,” Lladrovci recalled, whose father had brought him to Syria against the wishes of his mother.

His mother was in Kosovo. They didn't allow him to use the Internet. Imagine this kid not being able to speak with his mother! His father went to Iraq to fight, so he left his kid with some Arabs. He told the Arabs, "Please send my kid to the Albanian group." He got wounded. From the hospital he wouldn't call his son or anything. At some point the hospital was bombarded. We thought he was dead. This boy had no food to eat and no one was taking care of him. Within the [ISIS] law he was supposed to get money, but other Albanian kids were mocking him. So, he came to me one day, "Abu Musab brother, sorry to bother you, I don't have anything." He had ten cents in his pocket while the other kids had 10 Euros.

Lladrovci got upset and complained to the Albanian leaders,

I got very distant with Muhaxheri, but with Lavdrim, I spoke to him, "He is being mistreated, you have to help him." The answer, "You have to mind your own business." But for me it was very important. I loved that boy and you have to help him somehow. There was one night during bombings around the house of Lavdrim Muhaxheri. He [Muhaxheri] was scared and took his wife and left this kid all alone, knowing they were bombing and aiming at the house. I couldn't tolerate it. The Coalition, I think, was bombing and aiming at his house specifically. Later he recalls that the boy was also beaten, "Ramadani and Astrajevi, beat him very badly." (Lladrovci denied that the child was raped.)

Unable to help the boy, Lladrovci started risking his life by taking the boy daily on the back of his motorcycle to an Internet café to talk with his mother. Ultimately, Lladrovci decided to defect with his wife and take the boy back to his mother, probably because he truly cared for and identified with the boy's plight, and quite possibly because he also saw it as an insurance policy to avoid a prison sentence upon his return to Kosovo.

Again, Lladrovci spoke cavalierly about the details of his escape, saying he paid smugglers \$3000 to get the three of them out of Syria—the money he freely admitted to stealing from homes ISIS cadres pillaged. Nowhere in his interview did Lladrovci express concern for the homes that were taken from Shia to house ISIS cadres, nor for looting homes, the genocidal killings and enslavement of Sunnis, Shia, and Yazidis, rapes of Yazidi women, or ISIS beheadings. Nevertheless, he did feel bad for ISIS widows who were not paid their widow's pensions and were forced to remarry in order to survive, and for this boy whom ISIS mistreated. Thus, he decided to risk everything and defect from the group.

To an experienced psychotherapist speaking with Lladrovci (Speckhard), his personality in regard to his time in ISIS appears naïve, undeveloped, and somewhat psychopathic. Expressing no regret for serious war crimes, combined with total surprise that he was imprisoned upon his return from ISIS to Kosovo, Lladrovci stated, “The court gave me the letter that when I came here [to Kosovo], I'll be free.” Yet the Kosovo courts did not honor

the arrangement that Lladrovci claims to have negotiated. He was initially sentenced to five years for “participating with terrorist organization and for illegal possession of weapons,” but his sentence was later reduced to three and a half years. Lladrovci was serving his time in prison at the time we interviewed him.

“I’m threatened inside the prison,” Lladrovci complained. “There are people who are praying all the night to kill people in Kosovo. They are on first barrier [in the prison]. They are going to kill me for sure.” As a defector, Lladrovci knew that other ISIS inmates would like to kill him, but he did not blame ISIS at all for that—he blamed Kosovo.

Suffering alone in prison, he also got very angry at the state for not keeping the bargain he claimed they had made for rescuing the boy, and Lladrovci began returning in his mind to freedom all the while idealizing his time in ISIS and their so-called “Caliphate” where he again believed justice would be served, “The things that the IS has done, I’m willing to forgive them for everything. Compared to what they have done in Kosovo [to me]. It is way worse, I will never forgive them,” Lladrovci complained from prison.

Lladrovci acknowledged that he had indeed defected from ISIS and would have been killed had he been caught, but now in prison he was again enamored with ISIS, “[y]es it was a time when I decided ad- Dawlah [the Islamic State] was not for me. But when I came here to this *kufir* [unbelieving] state and institutions, they made me think I am for ad-Dawlah.” Discussing how hard prison can be, Lladrovci rationalized,

I was trying to help my country. Being alone in the jail for sixteen hours by myself [he is in solitary for his own protection] everyday, of course I’m going to think to kill. I never used to hate persons like you—civilians. Now I’m hating institutions, courts, because these are the people who put me in this position. They are the reason. They put me in the problems with ISIS. They are the reason why I was arrested and I’m leaving my family. The way I’m standing in the jail. The “Caliphate” is quite better than where I am treated by Albanians.

Lladrovci never admitted that in this victim stance he takes no responsibility for his own actions and simply blames others.

Lladrovci’s case also argues for in-prison rehabilitation treatment for those in Europe who will not be serving long sentences, as he becomes more violently committed to ISIS each passing day in prison, “[w]hen I stay in my cell, I don’t want to watch Turkish TV. I read Koran and reflect. There is no doubt that life in the Caliphate was better.”

When confronted with the fact that he is comparing apples and oranges—freedom to imprisonment, and is being contradictory, given that when a male ISIS defector is caught he is beheaded—Lladrovci stated, “Be honest, death is easier. When you die, you go to hell or heaven. To be alive and mistreated it really hurts. I’m losing the hope; I can’t stand myself like this.”

Over years of interviewing terrorists, we have often heard them say that prison is psychologically untenable and that they would rather take a suicide mission than return to a prison cell. Indeed, Chechen suicide bombers were overrepresented by those who had fugitive status within Russia. They would rather take a “martyrdom” mission than risk arrest, torture, and prison. Some Palestinians also said they would rather die fighting than return to prison.¹⁴ Belgians involved in the 2016 airport attacks also said they wanted to avoid arrest and prison and preferred “martyrdom.” This is a chilling thought: if the person

emerging from prison is not fully disengaged from the terror group, he or she may be more than willing to be sent on a suicide mission rather than get re-arrested. This is something Western nations will have to think over when they begin to imprison ISIS returnees. Holding the returnees in cages and not offering useful rehabilitation, including not helping them to admit what they are indeed responsible for, may keep society safe while they are locked up, but may make even more of a monster out of those already strongly indoctrinated by ISIS—and increase societal danger upon their release.

After being totally disillusioned by his imprisonment, Lladrovci explained that he flipped from being an ISIS defector to a full supporter and encouraged others to go to ISIS, “[a]fter I came back from Syria and Iraq, two persons came and I said, ‘Don’t go there,’ and I made them promise not to. But since I’m arrested, I’m going to say go there.”

He also idealized depending on God for everything, despite ISIS currently losing in Syria and Iraq, “Yes things have gotten worse. They’ve lost territory, weapons, and money. They don’t have good military tactics. They are not doing very well, but the point is, we only depend on Allah’s will and that is what is important.”

Having learned to view the world through the lens of Islamic State and the claim that they alone are representing Islam correctly, Lladrovci also fails to distinguish terrorist acts against innocent civilians from collateral damage during acts of war. When asked about the airport, restaurant, and nightclub terror attacks carried out by ISIS cadres in Brussels and Paris he answered,

Alhamdulillah [praise be to God], they [the Coalition] are bombing in Syria and Iraq! Restaurants! They bomb children all the time in Syria and they complain after... That’s why they [ISIS] bombed in the [Brussels] airport. It’s almost the same. They have tortured in Syria, now they have the same in their cities.” He added, “I am not like the Islamic Community of Kosovo to put a candle and say I’m crying for them.”

Having been taught well by ISIS, he also now judges people’s worth by asking, “But do they follow *shariah*?” Lladrovci, consumed with issues of social justice, also asked important questions about controversial interrogation practices, like, “Do you know what Americans did to the Muslims in the jails, especially jails in the Middle East?”

When calmed a bit, Lladrovci stated, “If you love justice you should work both sides, not leave only one,” and admits, “I know it’s not good to do terror in Europe or Kosovo.” However, the difficulty of being in solitary confinement in prison continues to eat at his soul. He admitted, “But then you have the pressure like this, put in jail, and you are dirty in everywhere—then of course you will be a terrorist.”

His case profoundly illustrates the challenges faced by Western governments that are unwilling to lock individuals like him up for a lifetime—shifting views and the idealizing of ISIS that may occur when faced with the challenges of prison as well as simply the return to “normal” life. (Fitim Lladrovci, age twenty-five, interviewed in June 28, 2016, Kosovo).

Policy Implications

This original, field-based research reflects our sixty-three interviewed ISIS cadres worldwide. Out of sixty-three interviewed, we found nine of them to have either reversed their defection and returned to the battlefield or continued their ideological commitment to ISIS. In this paper, we examined all nine cases using a psycho-social, case study methodology. While we cannot know the entire sample of ISIS returnees, nor what percentage is likely to reverse or continue their loyalty to ISIS, we believe that our sample gives the reader important insights into the factors that lead to discontinuing their loyalties toward the terrorist group, and then later in some cases reversing that position. This field-based research helps to develop an understanding of factors that may play into terrorists' recidivism, particularly in the case of returning ISIS foreign fighters.

These nine examples raise issues of enduring ideological indoctrination to groups like ISIS, strong ties with ISIS that persist even upon return from the battlefield, and the glum depression of having returned from the excitement of ISIS to a life of frustrated boredom, seeming insignificance, and economic challenges. Given that those who lived under ISIS are often initially attracted to join it as a result of childhood traumas, current challenges and deprivations, possible psychopathic traits as well as failures in relationships and life—all problems they initially believed the terrorist group could ameliorate or at the minimum distract them from—we can expect that they also return to the same issues that have not disappeared during their stint with the terrorist group. As a result, returnees, even those who claim to have deradicalized or disengaged from the terrorist group, may continue to be vulnerable to further involvement in terrorism. For that reason, all returnees and those suspected of having traveled to terrorist groups should be carefully assessed by qualified mental health workers and possibly religious leaders (e.g. qualified imams in the case of ISIS, al-Qaeda, and al-Shabaab, for instance). Moreover, those who have these psycho-social vulnerabilities should receive supportive therapy to ensure they do not involve themselves in terrorism again.

We must also keep in mind that many who traveled to join ISIS will return even further handicapped by additional traumas experienced in ISIS that may manifest as symptoms of post-traumatic stress disorder (PTSD). This requires careful assessment and treatment. One Albanian interviewed in Kosovo who had spent time fighting in Syria stated that he greatly benefited from a French treatment program that helped him come to terms with the atrocities in which he had taken part. Feelings of guilt, fear, shame, nightmares, flashbacks, bodily arousal, and avoidance are all symptoms of post-traumatic stress that may occur from having been involved in ISIS. Those who were involved during their development also need supportive therapy to help them recover from shattered world assumptions (e.g. the world is predictable, safe, human beings are caring, etc.) and from loss of childhood dreams and innocence. Umm Rasheed, for instance, who wanted to be a doctor as a teen girl and put considerable effort into her dream was turned into a sadistic torturer by ISIS: a group that provided her security when she had lost everything as a young woman. She will need supportive therapy to overcome her identification with a brutal group and to overcome her feelings of shame once she begins to admit that what she participated in was morally wrong.

Prison, or the threat of it, also appears to be a major stressor driving some back into the arms of ISIS. There is a tension in all societies between repressive measures against those involved in terrorism and rehabilitative measures that may put society at increased risk.

Policy makers need to assess the risk of radicalized individuals being imprisoned without treatment—that is, whether they will seed their terrorist ideas throughout the prison. Likewise, short prison sentences risk returning would-be terrorists back into society, but long ones may make choosing to die as a terrorist seem like a good choice.

The direct effects of imprisonment on cognitive changes or cognitive aspects of radicalization are poorly understood,¹⁵ yet it is well known that prisons often represent potentially fertile recruiting grounds for those representing groups like ISIS.¹⁶ The stressors of being in prison are many, and it is often necessary to join a group to gain protection and camaraderie, and feelings of resentment for the government can easily be exploited in prison. However, the prison environment also may provide a venue and opportunity for those disengaged from groups like ISIS to receive treatment and interact with others who could have a positive effect if they are placed in a controlled environment where they may have access to more progressive or liberal religious literature¹⁷ and contacts and treatments that could challenge their existing radical worldviews.¹⁸ Such programs need to be individualized, highly specialized, and carried out by highly skilled professionals. They must also include prisoner dispersion¹⁹ to isolate those who are vulnerable from terrorist recruiters and leaders to minimize group control over prisoners in isolated conditions and the immediate undoing of any prison treatment program that could potentially encourage prisoners to rethink their support for terrorism and, most importantly, ensure their reintegration into society once out of prison. Whether imprisoned upon their return, or free, it appears ISIS returnees and defectors harbor many vulnerabilities for return to the group, to recruit for it, and to offer it support, and they would benefit from well-thought-out treatment plans that effectively address both their original reasons for joining and the challenges they face upon return.

Given that most of the defectors we spoke to were truly repulsed by ISIS and harbored no positive feelings for the group at the time of our interviews (n=43), we must also stress that most of those who we spoke to did not remain aligned to ISIS, nor appear easily vulnerable to return. This does not mean, however, that they never will flip. Likewise, while Syrian ISIS cadres with whom we spoke cited Westerners as the “true believers,” not all were. A European woman who returned pregnant via an extremely perilous escape after her ISIS husband was killed, for instance, never really endorsed the group, and only followed her husband to Syria to remain married. She had no illusions about ISIS after having been pressured to leave her baby behind in order to leave with their blessings. Many of the Albanians who went to Syria early in the conflicts also said they went for humanitarian reasons to help in the uprising against Assad, but quickly returned upon seeing the factions turning upon each other. They also held no interest in the ISIS “Caliphate,” either while in Syria or upon their return.

All of these cases demonstrate that it will be important for governments, when dealing with ISIS returnees, to look carefully into the motivations and vulnerabilities of each individual for having traveled to Syria and Iraq and for having fallen into the ranks of ISIS. Those who appear as truly defected must be given a chance to prove themselves through the justice systems of their countries while being monitored by their governments to ensure that they do not continue to have ties with ISIS, intentions of going back, or intentions to carry out attacks in the name of ISIS in their countries. Such policies will be important as governments consider the impact on those who have been deceived into joining terrorist organizations in Iraq and Syria and now have second thoughts. This is especially crucial considering that not all who have joined ISIS were religious or ideological fanatics. As evidenced in our research, some joined for what they believed to be humanitarian reasons and quickly backed away from ISIS when they saw its extreme brutality.

During the course of our interviews with government officials and religious and civil society figures, some stressed the importance of introducing amnesty in the case of those who wish to return but have not committed crimes. The issue of granting amnesty remains contentious and open to debate and it is very difficult to distinguish between those who committed crimes and who have not. Already one ISIS defector imprisoned in Germany who claims not to have killed anyone while there was denounced by ISIS themselves as a killer.²⁰ However, providing adequate legal tools and venues for the returnees to prove their innocence is necessary to fight the narratives of alienation and victimization that groups like ISIS seek to exploit. That said, new policy initiatives must strike a delicate balance between ensuring security, including imprisoning those who might threaten society, while encouraging full rehabilitation of those who really have defected.

On the government side, it is difficult to prove which groups a returnee was in and produce evidence strong enough for courts to indict them on terrorism charges. Yet, it is important to remember what ISIS cadres told us about their one to three-week long *shariah* indoctrination classes (occurring after the ISIS Caliphate was declared and functioning as a “State” of sorts)—that these classes ended with sworn *bayats* and demonstrations of loyalty being carried out by each cadre beheading an ISIS prisoner. If true for returnees who joined ISIS once it was a “State,” they have committed war crimes and truly have blood on their hands, and psychologically have crossed a barrier from which it may be hard to return.

Conclusion

Arguably, the group’s battlefield losses due to aerial bombardments and ground combat, alongside the recent introduction of laws that criminalize material support and travel to combat zones with the purpose of joining terrorist organizations in Iraq and Syria, will continue to slow, if not completely halt, the flow of foreign fighters to Syria and Iraq. Equally important, the group’s aura and appeal are likely to continue to dwindle in light of accounts and narratives that depict the extreme violence and brutality of life under the “Islamic State” and ISIS-controlled territories, as is also evidenced in our recent research in Syria, Europe, and the Balkans. Some, however, will continue to fall prey to the group’s slick recruitment strategy, the promise of a “righteous” Islamic life, and the allure of successes that resulted in the creation of the “Islamic State.” However, as foreign fighters begin to stream home, a whole new set of challenges will begin. Now is the time to start planning how best to respond.

About the Authors

Anne Speckhard, PhD. is Adjunct Associate Professor of Psychiatry at Georgetown University's School of Medicine and Director of the International Center for the Study of Violent Extremism (ICSVE). She is also the author of *Talking to Terrorists*, *Bride of ISIS*, and co-author of the newly released *ISIS Defectors: Inside Stories of the Terrorist Caliphate, Undercover Jihadi, and Warrior Princess*. Dr. Speckhard has interviewed nearly 500 terrorists, their family members, and supporters in various parts of the world including Gaza, West Bank, Russia, Iraq, Jordan, Lebanon, Turkey and many countries in Europe. In 2007, she was responsible for designing the psychological and Islamic challenge aspects of the Detainee Rehabilitation Program in Iraq to be applied to 20,000 + detainees and 800 juveniles. She may be reached at annespeckhard@icsve.org.

Ahmet S. Yayla, PhD. is Senior Research Fellow at the International Center for the Study of Violent Extremism (ICSVE). He is also Adjunct Professor at the Department of Criminology, Law and Society at George Mason University and formerly served as Professor and the Chair of the Sociology Department at Harran University in Turkey. Dr. Yayla earned both his Master's and PhD. degrees in Criminal Justice and Information Science from the University of North Texas in the United States. Dr. Yayla served as the Chief of Counterterrorism and Operations Division for the Turkish National Police. He may be reached at ayayla@gmu.edu.

Ardian Shajkovci, PhD. is Research Director/Senior Research Fellow at the International Center for the Study of Violent Extremism (ICSVE). He has been collecting interviews with ISIS defectors and studying their trajectories into and out of terrorism as well as training key stakeholders in law enforcement, intelligence, educators, and other countering violent extremism professionals on the use of counter-narrative messaging materials produced by ICSVE both locally and internationally. He has also been studying the use of children as violent actors by groups such as ISIS and how to rehabilitate them. He has conducted fieldwork in Western Europe, the Balkans, Central Asia, and the Middle East, mostly recently in Jordan and Iraq. He is an adjunct professor teaching counter-terrorism courses at Nichols College. He holds a doctorate in Public Policy and Administration, with a focus on Homeland Security Policy, from Walden University. He may be reached at shajkovciardian@gmail.com.

Acknowledgement

The authors wish to thank "Murat" for his help in Turkey and Haris Fazilu for interpreting in Kosovo.

Notes

- 1 PBS NewsHour, "Are Airstrikes Successfully Weakening ISIS?" May 1, 2016, [URL:http://www.pbs.org/newshour/bb/are-airstrikes-successfully-weakening-isis/](http://www.pbs.org/newshour/bb/are-airstrikes-successfully-weakening-isis/) .
- 2 Carrol Lauren, "Retired General Says al-Qaeda has Grown 'Fourfold' in Last 5 years," [Politifact.com](http://www.politifact.com/punditfact/statements/2015/feb/01/jack-keane/retired-general-says-al-qaida-has-grown-fourfold-l/), February 1, 2015, <http://www.politifact.com/punditfact/statements/2015/feb/01/jack-keane/retired-general-says-al-qaida-has-grown-fourfold-l/> .
- 3 Krystal Chia and Lin Xeuling, "ISIS is Targeting Southeast Asia amid Declining Mideast Support: Terror Expert," *The Soufan Group*, August 4, 2016, <http://soufangroup.com/tsg-report-cited-on-channel-newsasia-isis-is-targeting-southeast-asia-amid-declining-mideast-support-terror-expert/>; ISIS recently lost cities of Mosul and Tal Afar in Iraq, including Raqqa in Syria, complicating their prospect for administering territories in Iraq, including their survival.
- 4 Sean D. Naylor, "Airstrikes Killing Thousands of Islamic State Fighters, but It Just Recruits More," *Foreign Policy*, June 9, 2015, <http://foreignpolicy.com/2015/06/09/airstrikes-killing-thousands-of-islamic-state-fighters-but-it-just-recruits-more/>.
- 5 See Jessica L. McFate et al., "ISIS Forecast: Ramadan 2016," *Institute for the Study of War*, May 2016, <http://www.understandingwar.org/sites/default/files/ISW%20ISIS%20RAMADAN%20FORECAST%202016%20FINAL.pdf>; Krystal Chia and Lin Xeuling, "ISIS is Targeting Southeast Asia amid Declining Mideast Support: Terror Expert," *The Soufan Group*, August 4, 2016, <http://soufangroup.com/tsg-report-cited-on-channel-newsasia-isis-is-targeting-southeast-asia-amid-declining-mideast-support-terror-expert/>; Walter Mayr, "Bosnia's Islamic State Problem," *Spiegel Online*, April 5, 2016, <http://www.spiegel.de/international/europe/islamic-state-presence-in-bosnia-cause-for-concern-a-1085326.html>.
- 6 Anne Speckhard and Ahmet S. Yayla, *ISIS Defectors: Inside Stories of the Terrorist Caliphate* (McLean, VA: Advances Press LLC, 2016), 332.
- 7 See also Maria Abi-Habib, "Islamic State Members from the West Seek Help Getting Home," *The Wall Street Journal*, June 6, 2016, [URL:http://www.wsj.com/articles/islamic-state-members-from-the-west-seek-help-getting-home-1465244878](http://www.wsj.com/articles/islamic-state-members-from-the-west-seek-help-getting-home-1465244878).
- 8 Note that 45 out of 63 we interviewed defected from ISIS. The remaining 18 (captured by the Iraqi government forces) are not included in the category of "defected." Although three individuals in Kosovo at the time of the interview were serving prison sentences for having joined ISIS, they are considered defectors in this paper as they all had fled ISIS and were only arrested upon their return.
- 9 Anne Speckhard, *Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant Jihadi Terrorists, Mass Hostage Takers, Suicide Bombers & Martyrs* (McLean, VA: Advances Press, 2012).
- 10 Anne Speckhard and Ahmet S. Yayla, "Eyewitness Accounts from Recent Defectors from Islamic State: Why They Joined, What They Saw, Why They Quit," *Perspectives on Terrorism* 9, no. 6 (December, 2015): 95-118, <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/475/934>.
- 11 Anne Speckhard and Ahmet S. Yayla, *ISIS Defectors: Inside Stories of the Terrorist Caliphate* (McLean, VA: Advances Press LLC, 2016), 332.
- 12 Anne Speckhard and Ardian Shajkovci, "Balkan Jihad: Recruitment into Violent Extremism and Issues of Returning Foreign Fighters in Kosovo and Southern Serbia," Manuscript submitted for publication.
- 13 We have used pseudonyms for most interviewees except those whose cases are public—they have spoken openly to the press or their cases have been discussed extensively in the press.
- 14 Anne Speckhard, *Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant Jihadi Terrorists, Mass Hostage Takers, Suicide Bombers & Martyrs* (McLean, VA: Advances Press, 2012).
- 15 Disley et al., *Individual Disengagement from Al- Qa'ida-influenced Terrorist Groups: A Rapid Evidence Assessment to Inform Policy and Practice in Preventing Terrorism* (Santa Monica, CA: Rand Corporation, 2010).

16 Anne Speckhard, "Challenging Militant Jihadi Terrorist Ideology," *Rusi Monitor*, December 18, 2009, <https://rusi.org/publication/challenging-militant-jihadi-terrorist-ideologies>.

17 Michael Jacobson, *Terrorist Dropouts: Learning from Those Who Have Left*, (Washington, DC: Washington Institute for Near East Policy, 2010).

18 Anne Speckhard, "Prison and Community-Based Disengagement and Deradicalization Programs for Extremists Involved in Militant Jihadi Terrorism Ideologies and Activities," RTO-TR-HFM-140-Psychological, Organizational and Cultural Aspects of Terrorism, Research and Technology Organization, North Atlantic Treaty Organization (NATO), 2011.

19 Rogelio Alonso, "Why do Terrorists Stop? Analyzing Why ETA Members Abandon or Continue with Terrorism," *Studies in Conflict and Terrorism* 34, no 9 (August, 2011): 696-716.

20 Rukmini Callimachi, "How a Secretive Branch of ISIS Built a Global Network of Killers," *The New York Times*, August 3, 2016, <http://www.nytimes.com/2016/08/04/world/middleeast/isis-german-recruit-interview.html> .

Copyright © 2018 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).



Improving Maritime Transportation Security in Response to Industry Consolidation

By Nick Monacelli

Abstract

Containerized cargo is the single largest security vulnerability in maritime shipping. Recent consolidation in the maritime shipping industry, along with freefalling shipping rates and increased vessel sizes, combine to cause concern for the future of containerized shipping security. Maintaining security in the maritime shipping industry is critical. Programs including the Container Security Initiative and Customs-Trade Partnership Against Terrorism apply risk-based approaches. However, with fewer market players after industry consolidation, it is time for regulators to review the success of current programs and search for new initiatives. New partnerships and outreach may use current efforts as a framework to respond in a dynamic environment to improve the industry's overall security. This essay investigates the way ahead, while proposing solutions. Changes to C-TPAT and CSI may be necessary to maintain a secure Maritime Transportation Security (MTS).

Suggested Citation

Monacelli, Nick. "Improving Maritime Transportation Security in Response to Industry Consolidation." *Homeland Security Affairs* 14, Article 2 (January 2018). <https://www.hsaj.org/articles/14257>

Introduction

Containerized cargo is an ongoing security challenge for the Maritime Transportation System. With gargantuan container vessels plying international routes, it becomes nearly impossible to ensure the safety of these trade lifelines. Recent consolidation in the maritime shipping industry, combined with free-falling shipping rates, combine to cause concern for the future of containerized shipping security. Compounding the present difficulties, container ships are growing in size and capability. Where once it was possible to inspect every container on a given ship, it is now unthinkable with vessels carrying over 20,000 containers.

Maintaining security in the maritime shipping industry is critical to preparing and responding to the parallel growing security threat. Programs including the Container Security Initiative and Customs-Trade Partnership Against Terrorism apply risk-based approaches. However, with fewer market players after industry consolidation, it is time for regulators to review the success of current programs and search for new initiatives. New partnerships and outreach may use current efforts as a framework to respond in a dynamic environment to improve the industry's overall security.

This essay presents a path forward for U.S. security professionals by providing specific recommendations for the Department of Homeland Security. By leveraging existing programs, policy-makers can make some minor changes which may pay large dividends. Regulators should take the industry's mergers as an opportunity to engage in an effort to shape security measures in a changing environment. An understanding of the current situation requires a review of the evolution of containerized shipping and the industry's development. A discussion of current regulatory approaches follows, with examples and the effects of recent industry re-alignment. Finally, the essay provides tools that U.S. regulators may adopt to make the industry safer and more secure.

The Evolution of Containerized Shipping

The New Era of Containers for Intermodal Shipping

Fewer technological advances contributed more to globalization than the advent of containerized shipping. In the span of 60 years, shipping containers evolved from novelty to ubiquity. Originally designed to assist intermodal transportation by Malcom McLean in 1955,¹ containerized shipping became a lightning rod for commerce. The first container ship, *Ideal X*, sailed in 1956 with 58 containers from New Jersey to Houston. Because of the decreased shipping costs, mainly due to efficiencies with loading/unloading and locking mechanisms (to prevent pilfering), the idea quickly took hold.²

The conflict in Vietnam created a large demand for McLean's containers.³ With the U.S. military needing a way to quickly and efficiently move massive amounts of war materiel to the jungles of Southeast Asia, containers saw heavy use. By 1968, McLean's containers had the industry's attention, with the International Organization for Standardization (ISO) issuing its first standard.⁴ Shortly thereafter, the ISO issued additional standards in identification and size, giving rise to the 20 and 40 foot common containers in use today. This set the groundwork for a new form of low cost intermodal transportation.

While ports initially resisted the shift to containers,⁵ the cost savings of up to 50% was hard to ignore. When international maritime trade boomed, ports quickly came onboard. By the late 1960s, ships slid down the ways with the ability to carry 1,000 TEUs (twenty-foot equivalent units). While this pales in comparison to the 20,000+ TEU vessels available today, 1000 TEU was enormous for its time. The number of countries with ports capable of servicing container vessels jumped from 1% in 1966 to 90% in 1983. Costs to ship cargo dropped dramatically from nearly \$6/ton to less than \$0.25/ton.⁶

With rapid expansion, many companies initially tried to cash in on the intermodal container craze. However, competition grew fierce and industry consolidation began. Paralleling the railroad consolidation in the U.S. in 1980, containerized shipping evolved into a business run by giant operators. When the dust settled, the entire market, responsible for transporting trillions of dollars in global trade, consisted of ~10 companies.

Current Market State

Since 2000, the shipping market has consolidated. While the top three shippers combined for 23.7% of overall market share, by 2016, the same top three companies comprised an astonishing 39.9% of the market.⁷ The top shipper, Maersk Sealand, expects to continue growth through 2017 in the wake of Hanjin Shipping's bankruptcy in 2016, pushing the top three shippers to an estimated 42.8% market share.⁸ The main reason for consolidation is the pace of mergers and acquisitions in maritime shipping, with five major shipping companies closing up shop from 1999-2016.⁹ Maersk Sealand alone is responsible for more than 3 million TEU in capacity, capturing nearly 15% of the global market.¹⁰

While the numbers alone are not particularly insightful, the trends provide an opportunity for analysis. The Hanjin bankruptcy is a symptom of the shipping industry's financial troubles.

While Maersk increased shipping volume by 9% in 2016, its total revenues dipped by 13%, mostly due to the sharp 21% decline in maritime shipping rates.¹¹ The effect on maritime security may not be obvious at first glance. Still, as one looks deeper into the industry's financial woes, new vulnerabilities emerge.

Current Regulatory Framework

Before investigating the impact of market consolidation, dipping freight rates, and the evolution of containerized shipping, it is important to look at the current state of security programs. The three primary security initiatives directed at maritime container shipping include the Container Security Initiative (CSI), Customs-Trade Partnership Against Terrorism (C-TPAT), and the International Ship and Port Security (ISPS) code.¹² Each, in turn, provides its own benefits to maritime security that may require re-evaluation in the face of industry changes.

Container Security Initiative

The United States developed CSI as a response to the September 11, 2001 terrorist attacks.¹³ U.S. officials were quick to identify maritime shipping as a possible threat vector for terrorism. The program's "core elements" are to 1) identify high-risk containers, 2) employ screening before shipping, and 3) leverage technology to prevent impeding commerce. It is the only program of the three identified with the sole focus of improving *container* security. The program has seen uncertain success, but in 2017, the program boasts that it prescreens over "80 percent of all maritime containerized cargo imported into the United States."¹⁴

By employing teams of customs officers at ports around the world, CSI casts a global net.¹⁵ With 58 ports participating under treaties with the United States, the host countries receive a purported benefit of shared intelligence and a better working relationship with U.S. officials.¹⁶ The customs officials use technology to screen containers as they are loaded, or prior to loading, on ships destined for the United States.¹⁷ X-rays, radiological detectors, and bomb-sniffing canines are standard methods to ensure security of the US-bound containers.¹⁸

Still, the program has limitations. To start, the inspectors are primarily concerned with containers with the United States as a final destination.¹⁹ With the growth of mega-ships, and a mix of containers destined for a variety of international destinations, the inspectors are unable to screen non-U.S. bound containers with the same level of detail. Further, while technology is getting better, the impact of larger ships capable of carrying 20,000 containers or more means that the potential delay for finding and inspecting U.S. containers has increased. Finally, while the goal has always been 100% coverage for U.S.-bound containers, CSI is still only able to pre-screen 80% since its 2002 inception. Industry consolidation provides an opportunity to re-invigorate CSI, which appears to have plateaued.

C-TPAT

While not focused on containerized shipping, C-TPAT is another important CBP program addressing the security of maritime shipping. Since so much shipping consists of containers,

the broad C-TPAT requirements have a distinct impact on the container market. Like CSI, C-TPAT grew out of the response to the September 11, 2001 attacks. Its primary focus is on detecting and interdicting the shipment of Weapons of Mass Destruction (WMD).²⁰ The C-TPAT program officials set guidelines for port security at foreign locations in exchange for preferential treatment and training opportunities.²¹

C-TPAT is distinct from CSI in that C-TPAT allows participation from industry players, whereas CSI focuses on foreign port authorities. In addition, C-TPAT covers other modes of transportation beyond the maritime domain. The primary driver for encouraging participants to increase their own security measures is the financial incentive of quicker customs processing upon arriving into the U.S.²² The concept is similar to the TSA Pre-Check program at U.S. airports. While some individuals will see a distinct financial advantage in bypassing otherwise unreasonable lines (either at the airport or ports of entry), other individuals may see no advantage and therefore little incentive to participate.

U.S. regulators may be able to leverage a consolidated maritime shipping industry to improve C-TPAT's reach and overall effect. Still, given that the program is designed to create incentives for firms conducting business in the U.S., new approaches may be necessary to address the fact that all of the top maritime shipping companies are global operators.

ISPS

The International Ship and Port Facility Code (ISPS) is an international treaty adopted under the Safety of Life at Sea framework.²³ The International Maritime Organization (IMO) developed the code in the aftermath of the September 11, 2001 terrorist attacks in an effort to bolster and standardize security in the maritime domain. As with all international treaties, it is up to individual nations to implement the agreement. The United States has implemented some of the ISPS regulations through the Maritime Transportation Security Act of 2002 and follow-on regulations.²⁴

The ISPS was designed to create a standard for nations to follow, and to assist industry in complying with the landscape of security regulations. While the code applies broadly to many parts of the maritime transportation system, the specific mention of containers is rare. No part of the ISPS code is dedicated to container security or the special considerations necessary for container transport.²⁵

As a framework mechanism to address shipping security, the ISPS code provides an in-place avenue for improving containerized cargo security in the face of the industry's changes.²⁶

Automated Targeting System

CBP uses a system called ATS (Automated Targeting System) to fuse intelligence and law enforcement data for guiding CSI and C-TPAT programs. CBP maintains internal guidance for how and when to use ATS output, but it generally includes information about various shipping elements, such as origin or en route ports of call. As one of the internal CBP products designed to work under both the CSI and C-TPAT frameworks, it provides a tool for managing risk and for smart decision making in maritime transportation security.²⁷

Given its unique situation, straddling many aspects of CBPs security responsibilities, ATS may provide one way to leverage the industry's consolidation into bolstering security in the future, as discussed below.

Economic and Security Effect from Consolidation

The maritime shipping industry's consolidation has substantial ripple effects on economic and security concerns. Economic incentives, such as those under C-TPAT, are closely related to the industry's security posture.

One of the biggest changes coming from consolidation is the formation of new strategic alliances.²⁸ For example, the World Shipping Council now controls approximately 90 percent of global container capacity.²⁹ The development of larger ships puts pressure on shipping rates. Alliances are necessary to compete and maintain profit as shippers face the conundrum of increased capacity and decreased margins.³⁰ Separately, regulatory costs of meeting environmental requirements eat into profits.³¹

As profit margins shrink and shipping companies merge and create alliances, security professionals should take note. While the impact on revenue does not directly affect companies' duty to meet security regulations, it does mean that security must compete with other operational demands. As Hanjin line bled red ink, it is hard to imagine that self-policing their ISPS compliance was a top concern for them. To complicate matters, many security programs have stagnated, including CSI and C-TPAT as described above. With no evolution in the regulatory environment, shippers are incentivized to maintain the status quo.

Some experts believe that maritime security concern has peaked.³² Counter-piracy efforts are effective, while importers and exporters have reached a happy equilibrium with port states.³³ As Bennett notes, "[a]s the perception of threat falls, so will the cost of protection." This may be an industry boon, but it belies the fact that not all parties value security equally. During the zenith of counter-piracy efforts, the extra security efforts in place undoubtedly ensure a safer maritime shipping infrastructure.³⁴

On the positive side, industry consolidation should make inspecting and enforcing compliance easier, with fewer entities to track. As companies go defunct and merge, it becomes one less "account" for C-TPAT.³⁵ While maritime shippers represent a very small part of C-TPAT (less than 1 percent of overall participants), they are some of the biggest players in terms of sheer volume.³⁶ The opportunity for increased per capita engagement is difficult to overlook. None of the biggest maritime shippers are U.S.-based companies. With fewer companies involved, regulators can streamline international outreach and perhaps garner broad agreements on common concerns.

As the shipping industry changes, the economic incentives to "participate" in voluntary security programs may shift. Still, the changes open new avenues of outreach using some of the renewed approaches discussed in the next section.

U.S. Response Proposal

In the face of a changing maritime shipping industry, many agree that it is time to re-evaluate and adjust security strategies. As discussed above, the U.S. has several robust framework programs in place that are capable of providing the foundation for an evolved maritime security system. In order to best respond to the new dynamics of maritime shipping, particularly in containerized cargo, key changes in resources, improved ATS, and higher incentive tiers for C-TPAT and CSI may make all the difference

Resources

The first element of improving security for containerized cargo is bolstering resources. As ships grow and the industry consolidates, shipping containers will become more centralized. While 20,000 TEU destined for the United States may have previously been spread over 3 or 4 vessels, all 20,000 TEU may now be located on a single ship. In order to keep commerce flowing without undue delay, CBP needs additional inspectors. The U.S. Coast Guard needs additional inspectors. Finally, planners must allocate funding resources to improving screening technology.

Profit margins are razor thin, and shipping companies are less likely to pour their own resources into meeting security requirements unless they are absolutely required. Adding resources on the enforcement side will prevent a pendulum swing on the industry side, providing consistency for future changes in the industry. No matter how the industry changes in the future, a robust, fully-resourced enforcement enterprise can respond more nimbly to market dynamics.

Improved ATS

The second most promising mechanism for improving maritime shipping security is developing, growing, and maintaining a robust Automated Targeting System. ATS links the two major U.S. security programs for CBP, CSI and C-TPAT. One can reference the Transportation Security Administration's machinations in trying to keep up with the speed of air travel to show the benefit of "smart" targeting criteria.

While the ATS risk analysis dimensions provide a good baseline, the system can certainly benefit from input improvements. Increased intelligence sharing and gathering, combined with closer partnerships with industry could generate better results.

One of the main benefits of maritime shipping industry consolidation is that there are now fewer entities with which to deal. One can imagine that dealing with fewer entities could mean closer (and better) relationships between industry and regulators. Closer working relationships with major maritime shipping companies will lead to better intelligence and better ATS decision outputs.

Combined with an increase in resources devoted to learning more about the industry, an enhanced ATS can keep containerized cargo secure through better risk-based response

action. It will also ensure that shippers have an incentive to “play along” by streamlining the process and reducing delay which directly eats into their profits.

Higher Incentive Tiers

A final approach that may improve containerized shipping security is providing additional incentive tiers at higher levels. As more and more C-TPAT partners reach top tiers, it may be necessary to create even higher tiers, maintaining an incentive for better-than-average performance. Incentive tiers that increase with time and overall performance are common across disciplines with California low-emission high occupancy vehicle lane access and TSA PreCheck programs as notable examples.³⁷

As more C-TPAT partners reach the highest tier, the marginal benefit of the improved processing time decreases. While one approach may be to make the requirements to reach the tier more restrictive, similar to the California carpool lane example, another option is to add higher tiers, creating additional exclusivity and benefits to the “best” security partners. Only the most sophisticated and capable partners would likely be able to meet increased guidelines.

Consolidated maritime shippers can afford to implement a higher security standard if presented with better incentives. While the incentives may not be worthwhile to smaller entities, the largest companies would perceive a drastic incentive with only a 1 or 2 percent decrease in processing time. New “mega” shipping companies provide an opportunity for regulators to offer such a higher-level incentive.

Conclusion

The maritime shipping industry has evolved. While many of the security programs were developed immediately in the aftermath of the September 11, 2001 terrorist attacks, the past 16 years have introduced a new norm. Industry consolidation, reduced focus on security due to a decrease in perceived risk, and decreased profits have created a new system of incentives for industry partners.

The current maritime transportation regulations provide a good framework. Still, the status quo is not acceptable, and changes are needed. In the face of a changed industry, several strategic changes would create a better system that is capable of responding to current threats while insulating itself against future industry change.

Increased resources, better application of CBP’s ATS, and better incentive tiers are methods of improving the current security system, each with their own benefits. As the industry consolidates, new opportunities to create a safer maritime transportation system are becoming apparent. Regulators should seize the opportunity before the industry changes so much as to render the current framework unusable in attempting to meet future changes.

About the Author

Lieutenant Monacelli currently serves as the Deputy Chief, Command Services Branch, at the Legal Service Command in Alameda. He is responsible to the Staff Judge Advocate for providing enterprise legal services to all mission support elements in the Pacific theater of operations, from the U.S. West Coast to Eastern Africa. With experience in aids to navigation, his prior afloat assignment was in the seagoing buoy tender Sequoia (WLB-215) as executive officer. He was commissioned in 2008 from the U.S. Coast Guard Academy. His education includes a M. Eng. in electrical engineering from Old Dominion University and a J.D. from UC Berkeley School of Law. He may be reached at nmonacelli@gmail.com.

Notes

- 1 "A Complete History of the Shipping Container," *Container Home Plans*, 25 Mar 2015.
- 2 Jean-Paul Rodrigue, "The Geography of Containerization: Half a Century of Revolution, Adaptation, and Diffusion," *GeoJournal*, September, 2008.
- 3 "A Complete History of the Shipping Container," *Container Home Plans*, 25 Mar 2015.
- 4 ISO 338 initially only defined terminology and dimensions.
- 5 This was mainly due to union pressures, with unions fearing the loss of stevedores given that containers required fewer laborers to load/unload than traditional cargo methods.
- 6 These numbers are adjusted for inflation.
- 7 "Global Container Market: Then and Now," *Tuscor Lloyds Global Logistics*, 9 Jan 2017. The top three shippers in both statistics are Maersk Sealand, Evergreen, and P&O Nedlloyd.
- 8 Ibid.
- 9 Ibid.
- 10 Dan Wang, "A Guide to the Largest Ocean Carriers in the World," *Flexport*, Accessed 14 June 2017.
- 11 James Sands, "Maersk Line Increases Market Share During 2016's Tough Container Shipping Line Environment," *Seeking Alpha*, February 12, 2017.
- 12 Michael Edgerton, *A Practitioner's Guide to Effective Maritime and Port Security*, (New York:John Wiley & Sons, 2013):23-24.
- 13 "CSI: Container Security Initiative," <https://www.cbp.gov>.
- 14 Ibid.
- 15 Michael Edgerton, *A Practitioner's Guide to Effective Maritime and Port Security*, (New York:John Wiley & Sons, 2013): 112.
- 16 Ibid.
- 17 Ibid.
- 18 Ibid.
- 19 "CSI: Container Security Initiative," <https://www.cbp.gov>.
- 20 "C-TPAT: Customs-Trade Partnership Against Terrorism," <https://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism>.
- 21 Michael Edgerton, *A Practitioner's Guide to Effective Maritime and Port Security*, (New York:John Wiley & Sons, 2013): 23-24.
- 22 Ibid.
- 23 Maritime (ISPS Code) Regulations, Maritime Transport Decree 2013, International Maritime Organization.
- 24 33 CFR 101-107.
- 25 Maritime (ISPS Code) Regulations, Maritime Transport Decree 2013, International Maritime Organization.
- 26 Ibid.

- 27** Maritime Security: Progress and Challenges in Implementing Maritime Cargo Security Programs, GAO-16-790T, July 7, 2016.
- 28** Greg Knowler, "Global Shippers Sound Alarm on Alliances, Consolidation," *Joc.com*, 29 May 2017.
- 29** Ibid.
- 30** Ibid.
- 31** Mike Antuono, "Plagued Global Maritime Industry Spurs Consolidation," *The Stillman Exchange*, November 15, 2016.
- 32** Thomas Bennett, "Maritime Security at a Crossroads," *The Maritime Executive*, April 26, 2015.
- 33** Ibid.
- 34** Ibid.
- 35** "C-TPAT: Customs-Trade Partnership Against Terrorism," <https://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism>.
- 36** Ibid.
- 37** The California low emission vehicle program allowed certain high efficiency vehicles access to restricted occupancy lanes. As more vehicles reached the standard, regulators increased the standard. For example, while hybrid vehicles were initially eligible, now only purely electric vehicles earn the extra incentive. Similarly, TSA PreCheck began as a system used by relatively few people. Now with more people using the TSA "fast lane," additional service tiers, including programs like CLEAR, require higher standards in exchange for increased incentives. <https://www.arb.ca.gov/msprog/carpool/carpool.htm>

Copyright © 2018 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

A black and white photograph of a person's hands holding several protest signs. The signs are white with bold, black, stencil-style text. The text on the signs reads 'PREVENT', 'COUNTERTERRORISM', '& TERRORIST', and 'RECRUITMENT'. The person is wearing a light-colored, textured garment, possibly a hoodie or sweater. The background is dark and out of focus.

Book Review:
Preventing and Countering Extremism
and Terrorist Recruitment: A Best
Practice Guide by Hanif Qadir
(Melton, Woodbridge: John Catt Educational Ltd, 2016)

Reviewed by Caitlin Ambrozik

Suggested Citation

Ambrozik, Caitlin. "Book Review: *Preventing and Countering Extremism and Terrorist Recruitment: A Best Practice Guide* by Hanif Qadir (Melton, Woodbridge: John Catt Educational Ltd, 2016)." *Homeland Security Affairs* 14, Article 3 (January 2018). <https://www.hsaj.org/articles/14267>

A parent logs into a child's computer and a chat room window pops up on the screen. The parent starts scrolling through the chat history and realizes that the child was speaking to an ISIS recruiter. In this hypothetical situation, the child has not conducted any crime, yet the parent is worried. What should the parent do? Call the police? Is there anyone else that can help the parent with this situation?

Scenarios like this one are why communities and governments across the globe are developing intervention programs to assist vulnerable individuals. Interventions operate primarily within the non-criminal space, meaning that the programs serve individuals who need help, but have not committed any crime. Interventions provide these people with an off-ramp to radicalization by offering individualized plans to increase the subject's resilience against violent extremism.

Other countries, such as the United Kingdom, are leading global efforts in intervention programs, while communities in the United States struggle to implement intervention programs. In the U.S., communities still lack a solid understanding of what interventions are and how to conduct an intervention. A new book, *Preventing and Countering Extremism and Terrorist Recruitment: A Best Practice Guide* by Hanif Qadir, an intervention specialist in the UK, provides needed insights from the practitioner's personal experiences with conducting hundreds of interventions.

The book is structured in four parts. The first part explores Qadir's own personal experience with extremism. The next section outlines current intervention efforts in the UK. This section is followed by an exploration of extremism and the push and pull factors affecting vulnerable people. The book concludes with a theological overview of Islam's view of extremism and terrorist groups.

Qadir starts the book off with his personal journey towards joining Al-Qaeda and then leaving the group. As such, the introductory chapter provides a successful case study of a once radicalized individual turned into a community member who now helps others who fall victim to violent extremism. The chapter details how Qadir created the Active Change Foundation, a community non-profit organization that seeks to help vulnerable youth. It also documents the challenges he faced while trying to operate the organization. After reading this chapter, it is clear to the reader that Qadir is both qualified and experienced to write a book on interventions.

In the next section, Qadir provides an overview of current UK Countering Violent Extremism (CVE) efforts, a program known as Prevent, and describes the underlying issues of violent extremism. Unlike other academics studying radicalization, Qadir emphasizes two contributing factors to the problem of violent extremism: foreign policy and the lack of critical thinking skills amongst the youth. Qadir argues that by ignoring the roles that foreign policy

actions and government treatment of Muslims play in fueling grievances, we contribute to the problem. Moreover, the lack of investment in education to improve critical thinking skills puts the youth at a greater risk of being manipulated by recruiters. The chapter concludes with an overview of future and current challenges wherein Qadir points to issues such as the lack of trust in authority amongst the youth and the adaptability of terrorist groups. This adaptability allows these groups to quickly adjust their strategies in accordance with changes in the world that pose significant challenges to efforts that seek to counter violent extremism.

The book continues with a section on how to tackle extremism. The section includes Qadir's views on the tactics used by recruiters and the push and pull factors affecting vulnerable people. In this particularly useful section for practitioners is a step-by-step guide for conducting interventions. Here, Qadir outlines five key steps for intervention, which include consideration, planning, technical, risk mitigation, and governance steps. The section concludes with seven case studies of interventions that Qadir conducted over his career. Although the case studies are limited in detail for privacy concerns, they still serve as useful examples of how to respond to different scenarios.

The final section of the book is titled "The Islamic Standpoint." In this section, Qadir provides an overview of the historical roots of extremism in Islam. He discusses the origin of Kharijite terrorists and how Kharijites falsify the Quran to promote their worldly objectives. This section provides practitioners with insights on how to counter the narratives of extremist groups.

Qadir's insights on how to ensure that interventions are successful will be valuable to those in the fields of homeland defense and security studies. Interventions and CVE efforts are long-term strategies and should be treated as such. There are no quick-fixes to the problem, rather Qadir argues that practitioners should take the time to understand communities fully, which includes understanding community dynamics. For a successful intervention, Qadir argues that trust is key and factors such as the environment in which the intervention takes place can influence the degree of trust between an intervention provider and vulnerable individual. For instance, police stations do not make ideal environments for an intervention.

Qadir also identifies problems within the UK's Prevent strategy from which practitioners can learn. The UK's strategy is known to promote moderate voices of Islam as a means to silence extremist voices. However, eliminating spaces for individuals to express grievances and debate issues enables recruiters to fill the void and offer subjects a listening ear and alternative. The UK's Prevent strategy is controversial, and Qadir takes note of this, but also proposes ways to mitigate opposition such as highlighting the program's successes. This is advice that CVE practitioners in the U.S. can and should adhere to, especially since there are misperceptions and opposition to U.S. CVE efforts.

The major weakness of this book, the lack of citations and dialogue with current research in this field, can also serve as the book's strength. This type of detailed account of a practitioner's experience with interventions is largely missing from the current literature on countering violent extremism initiatives. However, since the book is based on Qadir's personal experiences with both violent extremism and conducting interviews, the book focuses primarily on Islamic violent extremism. The strong emphasis on this form of extremism should not lead to the take-away that interventions should only attempt to counter efforts by groups such as ISIS and Al-Qaeda. As Qadir argues, interventions should

not focus on one form of extremism. However, it is unclear whether these insights can travel to cases of other forms of radicalization.

Although Qadir offers insights in terms of how interventions should be conducted, the account is scant on recommendations for the structure of intervention programs. Questions left unanswered include who should conduct the interventions and how involved law enforcement authorities should be in the process. Qadir does mention that specialists with knowledge about extremism and interventions and individuals who have credibility within the community should be the ones conducting interventions. However, it is unclear who these ideal intervention providers are and how to determine if an individual meets the requirements. Moreover, Qadir's own personal background with violent extremism begs the question as to whether the ideal intervention provider is a former violent extremist. Several intervention models such as EXIT Sweden and Life After Hate in the United States are also operated by former, albeit right-wing, extremists. Nonetheless, the use of formers in countering violent extremism initiatives, at least in the United States, remains highly controversial.

Despite these unanswered questions, *Preventing and Countering Extremism and Terrorist Recruitment* serves as an excellent resource, and one of the only non-government guides for practitioners conducting interventions. The valuable insights provided in this book warrant the book's place on any CVE practitioner's bookshelf.

About the Author

Caitlin Ambrozik is a PhD. Candidate in Government at Cornell University. Her dissertation explores the implementation of CVE programs in the United States and United Kingdom and public opinion on CVE. She may be reached at cem324@cornell.edu.

Copyright © 2018 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

SCADA Fusion With Commercial Fission

by Matthew Horner



Abstract

Nuclear power plants rely on digital components, like supervisory control and data acquisition (SCADA) devices, to perform daily operations. These devices can contain software vulnerabilities. To address SCADA and other cyber threats, the U.S. Nuclear Regulatory Commission (NRC) has issued directives for licensed operators to submit cybersecurity plans for their facilities. While the guidance is on par with other sectors, the application may be inadequate. Protection against cyber-attacks becomes more important as SCADA systems become more standardized and connected to other networks. In addition to resilient components, improvements like redundancy, whitelisting, and intrusion detection systems can help improve a SCADA network. Ultimately, the nuclear power industry may need to undergo a culture shift in order to reduce the vulnerability of these systems. An information-sharing and analysis center can also provide lessons learned and expertise to the NRC and nuclear power plants in the U.S.

Suggested Citation

Horner, Matthew. "SCADA Fusion With Commercial Fission." *Homeland Security Affairs* 14, Article 4 (April 2018). <https://www.hsaj.org/articles/14317>

Introduction

Like other power plants, nuclear power plants rely on digital components to perform daily operations. Many of these components are supervisory control and data acquisition (SCADA) devices that can contain software vulnerabilities.¹ The Nuclear Energy Institute (NEI) claims that "critical systems" in a nuclear reactor facility are not connected to the Internet or the facility's internal network and therefore that the cybersecurity risk to these critical systems is minimized.²

However, the stakes in nuclear power are always high. Not only do the facilities provide electricity to communities, but they also contain nuclear fuel. Accidents at nuclear power plants are well-publicized. Three Mile Island, Chernobyl, and Fukushima Daiichi are names that invoke the dangers of nuclear power, and they will likely not fade anytime soon. Additionally, terrorists can target nuclear power plants seeking to gain access to nuclear fuel to create a "dirty bomb," or an explosive device meant to spread radioactive particles over a large area.³ Cyber-attacks add to the list of threats to a nuclear power plant, and they have the unique property of attacking from afar and anonymously. This paper will discuss SCADA systems in commercial nuclear power plants in the U.S., focusing on

- incorporation of digital and networked components in U.S. commercial nuclear power plants,
- a summary of policy for cybersecurity in nuclear power plants,
- cybersecurity threats to and vulnerabilities of nuclear power plants, and consequences of a successful exploitation, and
- recommendations to improve the cybersecurity of the nuclear power plant infrastructure.

Incorporation of Digital and Networked Components

The Nuclear Reactors, Materials, and Waste Sector (or Nuclear Sector) of the U.S. is one of the 16 critical infrastructures (CI) as defined in Presidential Policy Directive-21.⁴ A basic understanding of power plant construction and functionality is useful to help the reader appreciate the risk to this sector. Instead of burning fossil fuels, nuclear power relies on a process called fission which involves splitting atoms of a fissile material like Uranium-235. Fission creates thermal energy that can be used to generate electricity. However, it also produces radioactive elements that must be trapped within a containment barrier. If these radioactive elements are released, long-term environmental and public health consequences can result as seen in Chernobyl, Ukraine and Fukushima, Japan.⁵ According to the Department of Homeland Security (DHS), the high-impact consequences of mishandling nuclear assets make the Nuclear Sector the “most highly regulated and heavily guarded” of all the U.S. CI sectors.⁶

A nuclear reactor presents additional challenges over fossil fuel combustion. One challenge is the generation of thermal energy when the reactor is shut down; unfortunately, the meaning of a nuclear reactor shutdown is not synonymous with “no longer producing heat.” Even if the fission reaction is stopped by the reactor’s shutdown mechanism, the radioactive decay of fission products continues to generate thermal energy called “decay heat” that must be removed to prevent damage to the reactor fuel. Coolant must continue to flow through the reactor core to remove this decay heat. If heat is not removed, the core could melt. This situation occurred in the Three Mile Island Unit 2 reactor in Middletown, PA in 1979 where a combination of equipment failures, design flaws, and operator error led to a meltdown of the reactor core even though the reactor was shut down.⁷ The cleanup took approximately 12 years and cost \$973 million.⁸ The public confidence in nuclear power dropped as well.



Figure 1. Three Mile Island Nuclear Power Plant in PA⁹

SCADA System Benefits and Risks

SCADA systems can help reduce the number of personnel required to operate a power plant safely. In nuclear power plants built in the 1960s through the 1980s, SCADA systems were analog systems with hardware and software designed for a specific function, and modifying these systems was more difficult than hacking a networked component because physical access was required.¹⁰ As these legacy systems were upgraded, programmable code usage increased the potential functions of SCADA systems, and because security was not initially designed into these systems, they have increased the vulnerability of a civilian nuclear power plant.¹¹

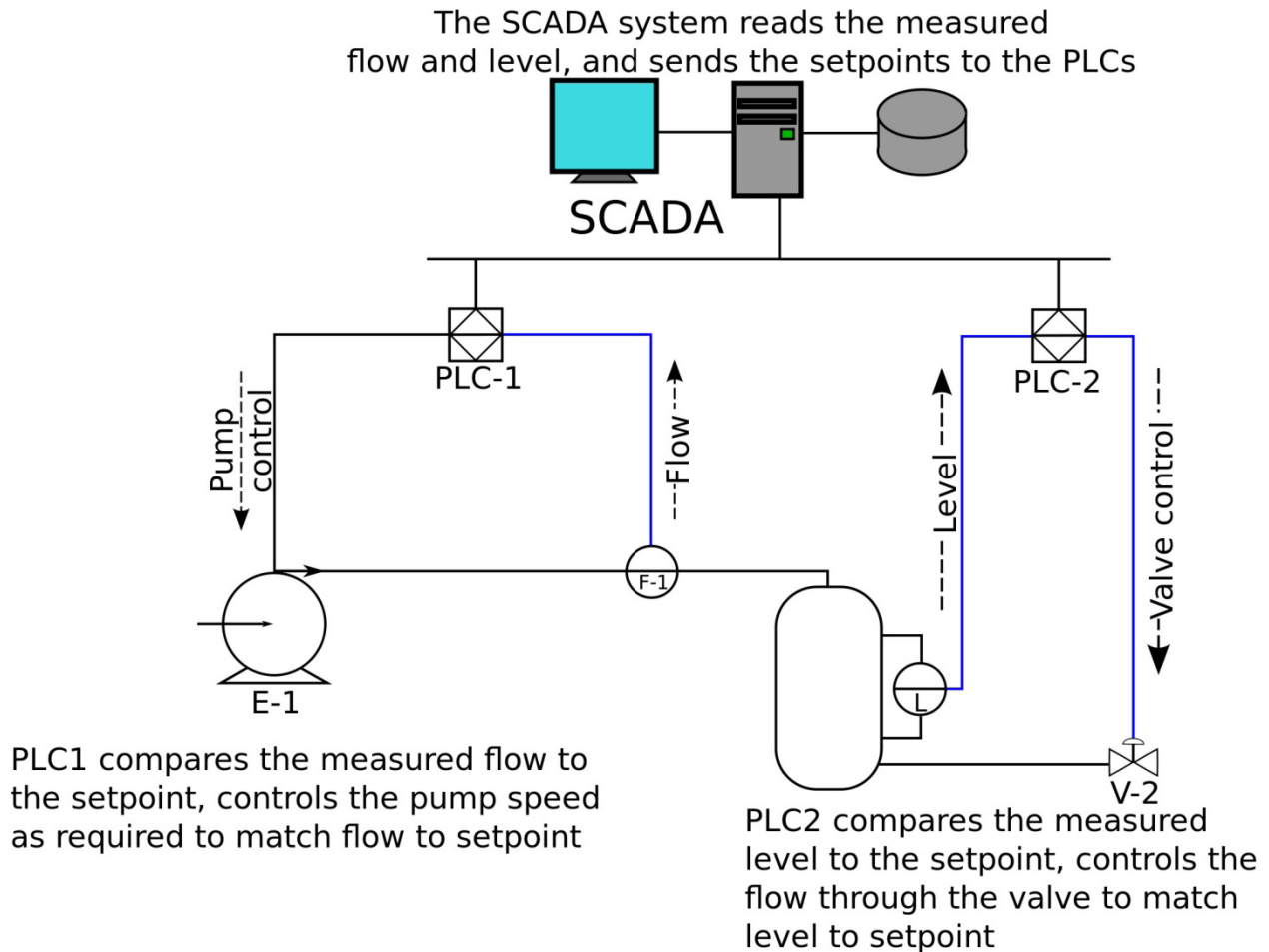


Figure 2. Summary of how a SCADA system with programmable logic controllers (PLC) can work¹²

Nevertheless, the problem posed by programmable code was not initially an alarming issue in systems that used SCADA components. For example, in the case of the Massachusetts Water Resource Authority, operators believed that the isolated SCADA systems were specific to a particular plant, so specialized knowledge and physical access was required to cause real damage.¹³ Over time, SCADA systems have implemented open protocols and commercial off-the-shelf (COTS) software reducing the possible customization in a power plant.¹⁴ Additionally, third parties requesting data from the nuclear power plant typically receive that data through an Internet connection, thus increasing possible avenues of attack.¹⁵

With 100 commercial nuclear reactors in operation at 61 power plants, there are many potential targets.¹⁶ Each of these power plants can contain over one thousand “digital assets” which includes SCADA systems.¹⁷ The opportunity for a cyber-attack exists through these digital assets, but according to the NEI, most of these assets are not connected to radiological safety and security.¹⁸

U.S. Operating Commercial Nuclear Power Reactors

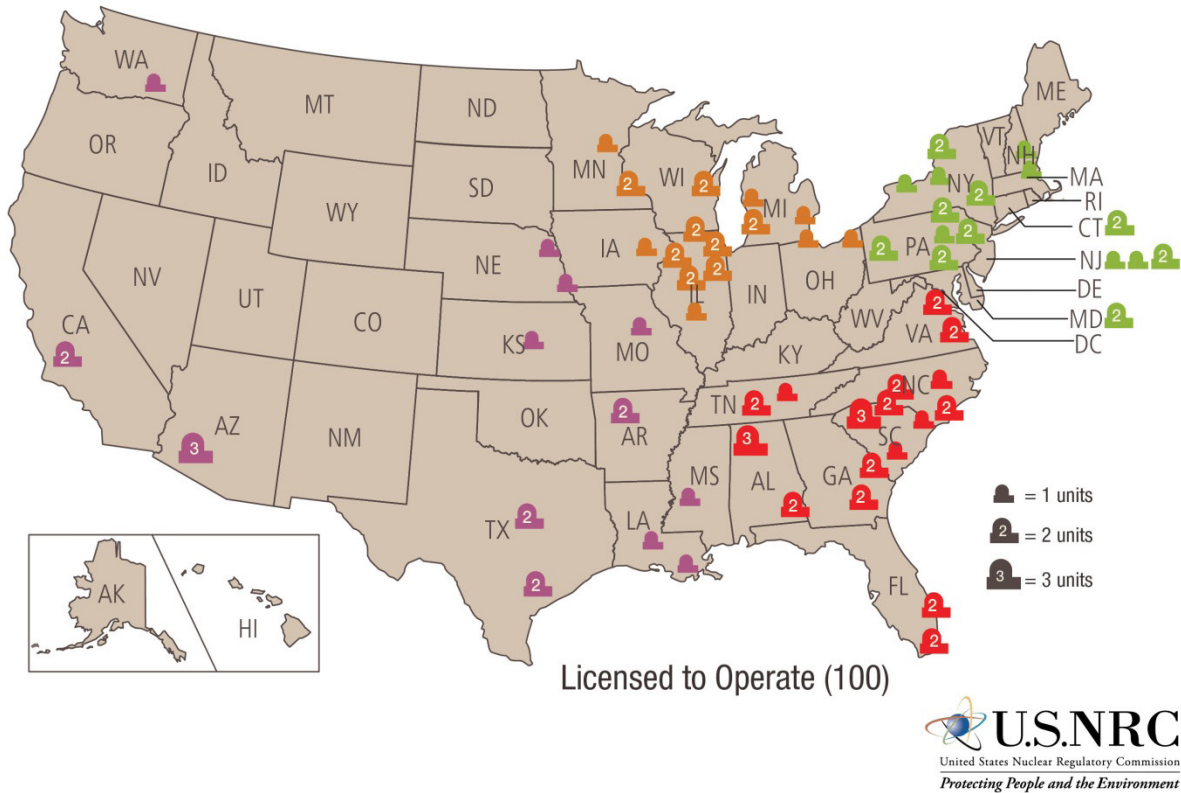


Figure 3. Distribution of nuclear power plants across the U.S. as of November 2015¹⁹

Cybersecurity Policy in Nuclear Power Plants

In the U.S., the Nuclear Regulatory Commission (NRC) is the regulatory body for all nuclear power plants.²⁰ Although the DHS is the sector-specific agency for the Nuclear Sector, the NRC provides oversight.²¹ Thus, nuclear power plants in the U.S. have only one set of rules to follow, which helps simplify the policies and procedures required to operate a nuclear reactor.

After the terrorist attacks of September 11, 2001, the NRC directed nuclear power plant operators to improve the physical security and cybersecurity of their facilities.²² By 2009, the NRC had codified the cybersecurity requirement in CFR Title 10, Chapter 1, Section 73.54.²³ This regulation requires an NRC-approved cybersecurity plan from current operators as well as those applying for a license to operate nuclear reactors. According to this regulation, the cybersecurity plan must protect digital systems, networks, and communications involved with

- safety,
- security,
- emergency preparedness, and
- support systems and equipment.²⁴

The NRC and NEI provide additional guidance through *Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities* and *NEI 08-09 Revision 6 Cyber Security Plan for Nuclear Power Reactors*.²⁵ The description of protected systems is very broad. This is likely due to the variance in design of nuclear power plants, but it forces power plant operators to analyze their own power plants to determine which digital assets would fall under safety, security, emergency preparedness, or support systems.

Nuclear Power Risk Analysis

This determination is similar to a risk analysis where assets are prioritized based on threats, vulnerabilities, and consequences if an asset is damaged or disabled.²⁶ Depending on their connectivity and function, SCADA systems could be classified as high risk. For example, SCADA systems involved with safety, security, or emergency preparedness likely have large consequences if they fail, and if the SCADA system is connected to the Internet through a path like a corporate network, the number of threats increases dramatically because physical access is no longer required. The trend in U.S. nuclear power plants appears to be isolation of SCADA systems connected to “critical safety and security systems.”²⁷

According to the NEI, all licensed operators have cybersecurity plans that have been approved by the NRC.²⁸ Additionally, the NRC has approved the plan of action and milestones (POAM) for each power plant and regularly verifies the status of this POAM.²⁹ For example, the NRC set one milestone to occur by December 31, 2012 and it included requirements such as:

- identification of critical systems and their critical digital assets,
- isolation of critical plant systems allowing outbound communication only,
- implementation of security controls for portable media, and
- implementation of cybersecurity controls for the most important assets.³⁰

Some organizations like the Chatham House, however, believe that there are fundamental flaws in both the timeliness and culture of cybersecurity protection in commercial nuclear power plants.³¹ While power plants may meet the requirements set forth by the NRC, the efficacy of a cybersecurity program is measured using performance against threats, not agreement with regulations.

Cyber Threats, Vulnerabilities and Consequences

There are several cases of a commercial nuclear power plant succumbing to a cyber-attack or malfunction after 2001 that can provide a test of the cybersecurity controls in place. One example is the Slammer worm attack on the Davis-Besse Nuclear Power Station in Oak Harbor, OH in January 2003.³² The Slammer worm infected a contractor network connected to the nuclear power station's business network which bypassed the properly configured firewall of the business network.³³ The worm then infected SCADA systems through a remote computer using a virtual private network (VPN).³⁴ The plant operators eventually lost the Safety Parameter Display System (SPDS) for almost five hours which required operators to walk around and manually check on plant parameters.³⁵ While no power outage occurred, the loss of the SPDS could slow corrective actions if a malfunction occurred within the reactor plant.



Figure 4. Davis-Besse Nuclear Power Station³⁶

The Davis-Besse case highlights the vulnerability of SCADA systems when connected to the Internet. Plant operators desired to monitor plant parameters remotely and connected SCADA systems to the business network.³⁷ Lewis writes that the “openness and connectivity” with internal networks and external business partners is the largest security deficiency in SCADA systems.³⁸ The NEI shares this view, stating that the first line of defense is isolation through air gaps or hardware-based isolation.³⁹ However, external connections to a network can change daily, so believing that an isolated network stays isolated may be optimistic and mistaken.

Hatch Nuclear Power Plant

The Hatch nuclear power plant near Baxley, GA experienced an unexpected shutdown of one of its reactors after a software update on the business network reset data on a control network in March 2008.⁴⁰ The reactor safety program interpreted the reset as a loss of water to cool the reactor core and initiated an automatic shutdown.⁴¹ While no damage occurred, there was a loss of electrical power generation because the plant was shut down for 48 hours.⁴² The parent company, Southern Company, had to purchase electricity from another provider which cost \$5 million.⁴³ The Hatch case shows that SCADA systems that are fed incorrect data can still take physical action based on that data; if connected to these SCADA systems, an attacker could cause a denial of service (DoS) of electrical power or worse.

Browns Ferry Nuclear Power Plant

In August 2006, the Browns Ferry nuclear reactor was shut down manually after two pumps responsible for pumping cooling water through the core failed; these pumps were controlled by variable frequency drives (VFD) which contain microprocessors that send and receive data over the control network.⁴⁴ The VFD failed due to excessive traffic on the control network, and while no damage to critical systems occurred, a loss of electrical power generation occurred similar to the Hatch power plant incident.⁴⁵ This was not due to a cyber-attack, but it shows how fragile SCADA systems can be. An attacker could execute a DoS attack by flooding the control network with useless data, and SCADA systems could fail and prevent critical components from operating, resulting in a loss of electrical power or potential reactor core damage.



Figure 5. Browns Ferry Nuclear Power Plant⁴⁶

Recent Power Plant Hacking

In a recent wave of attacks starting in May 2017, a hacking group targeted the business networks of companies that operate nuclear power plants. One of these companies was the Wolf Creek Nuclear Operating Corporation which operates a nuclear power plant near Burlington, Kansas.⁴⁷ The DHS and FBI reported that an advanced persistent threat (APT) actor was responsible for these attacks.⁴⁸ The attackers generally attempted to exploit the insider threat by spear-phishing, or targeting specific users in order to gain sensitive information or credentials. The APT sent emails containing malicious attachments to senior engineers, hoping to steal the credentials of a recipient who opened an attachment.⁴⁹ The APT used other avenues of attack, like the watering hole attack, where a regularly-visited website is hacked to attack the users who visit, and a man-in-the-middle attack, where attackers route Internet traffic of users and their destinations through the attacker's machine.⁵⁰

APTs differ from other attackers in that they generally focus on intelligence gathering, trade secret theft, disruption of operations, or even physical destruction of equipment; they have many financial and personnel resources, and some are backed by nation states.⁵¹ While these attacks were aimed at the business network rather than the operational network, the information that the APT could gain from infiltrating business networks could make any future attacks on the operational network much more effective and dangerous.

The SCADA Vulnerability Market

In addition to increasing connectivity, power plants are using SCADA systems with open protocols and COTS.⁵² This can allow hackers to gain knowledge about SCADA systems. An attacker can purchase a commercially available SCADA system, probe it for vulnerabilities, and use those discovered vulnerabilities against a power plant using the COTS SCADA system to gain unauthorized access. In fact, there is currently a market for this exact information, and exploits are selling at a relatively low cost.⁵³ For example, while Apple iOS 9 vulnerabilities can sell for up to \$1 million, anonymous users can purchase SCADA vulnerabilities with an \$8,100 annual subscription fee.⁵⁴ Gleg, ReVuln, and Exodus Intelligence are three companies devoted to finding SCADA vulnerabilities, and while their stance is to improve security by discovering vulnerabilities, the companies take no responsibility for what users with ill intentions may do with those exploits.⁵⁵

Recommendations to Improve Cybersecurity

Because SCADA systems can control critical processes in a nuclear power plant, protection of these systems from cybersecurity threats is paramount. However, replacing all SCADA systems with more robust systems, known as "rip and replace," is likely infeasible due to the massive cost and downtime of critical processes required to overhaul control systems. For example, in the oil and gas sector, replacing 200 gas turbine controllers could cost up to \$70 million before accounting for the cost of lost production.⁵⁶ Because nuclear equipment could be radioactive, disposal could further increase the cost of a rip and replace strategy.

Improvement of Control Networks

It may be more economically feasible for older power plants to improve the control networks on which the SCADA systems reside. Specific network improvements include redundancy, whitelisting applications, and adding an intrusion detection system (IDS) to the network.⁵⁷ Redundancy can help with patch management by shifting normal processes to one SCADA component while the other is being updated. Additionally, redundancy can assist with inadvertent activation of automated safety functions. In the case of the Hatch power plant, if two SCADA components were required to activate the safety shutdown, the plant may have avoided the shutdown. Whitelisting can help ensure that only approved applications are allowed to run on control networks that can reduce the potential effects of malware. An IDS can alert operators to abnormal conditions on the control network. In the case of the Browns Ferry shutdown, operators could have been alerted to abnormally high network traffic and mitigated the circumstances that caused the pump VFD to fail.

The conventional wisdom within the NRC, the DHS, and the NEI is that SCADA systems are protected when they are isolated or air-gapped.⁵⁸ However, critics argue that truly air-gapped systems do not exist.⁵⁹ The *Stuxnet* worm demonstrated that even air-gapped Iranian centrifuges were susceptible to infection.⁶⁰ The primary method of infection of *Stuxnet* was through USB flash drives which do not require a network connection.⁶¹ Also, the Davis-Besse case shows that system administrators may be unaware of all connections to its SCADA control network.⁶²

Minimize the Insider Threat

Another significant cybersecurity problem within commercial power plants is the insider threat.⁶³ The Three Mile Island accident highlighted the need for competent operators; as a result, nuclear power plant operators are typically well-trained.⁶⁴ However, this training may entrench nuclear operators in a certain way of performing their duties, and information security personnel may have difficulty trying to steer nuclear operators away from risky activities. One of these activities is connecting an operator's personal computer to the SCADA control network; this can expose the control network to any malware residing on the personal computer.⁶⁵ The attacks in 2017 demonstrate that APTs are relying on the insider threat as one way to hack into networks.

Although the operators interact directly with the control networks, supervisors and senior executives can also benefit from cybersecurity training. While those in a supervisory role are well-versed in physical security for nuclear facilities, cybersecurity is considered a low priority.⁶⁶ This could be a result of recent adoption of digital systems in nuclear power, lack of reported cybersecurity incidents at nuclear facilities, and a focus on physical security.⁶⁷

Nuclear Power Information Sharing and Analysis Center (ISAC)

There may be a dearth of cybersecurity experts in the nuclear field, so a national organization could help provide support to nuclear supervisors. As in other CI sectors, an ISAC could be created for nuclear power plants.⁶⁸ This can be an effective way to concentrate cybersecurity expertise and provide a method for nuclear facilities to disclose anonymously cybersecurity incidents and lessons learned. The NRC could fill this role, but Kesler argues that the NRC lacks cybersecurity expertise.⁶⁹ Additionally, since the NRC functions as a regulatory body, nuclear power plants may be less likely to disclose cybersecurity incidents to the NRC than to an independent organization.

Conclusion

SCADA systems are pervasive throughout commercial nuclear power plants in the U.S. Some of these systems are involved with the safety, security, and emergency preparedness of the power plant, and licensed owners must have an NRC-approved cybersecurity plan for these systems according to 10 CFR 73.54. However, the nuclear sector may be lagging in the application of cybersecurity. Since 2001, two reported incidents involving cybersecurity resulted in a shutdown of a nuclear reactor, and one reported incident was the result of a computer worm. SCADA technology is becoming more standardized and more connected, and there is a market for their vulnerabilities, so protecting these systems is paramount. SCADA systems can be designed to be more resilient against cyber-attacks, but for older nuclear power plants that cannot feasibly rip and replace SCADA systems, improving the control network may be a more economical option. Cybersecurity training for operators and supervisors can improve security, and a nuclear ISAC could provide lessons learned from cybersecurity incidents at nuclear power plants and provide needed cybersecurity expertise to the NRC.

About the Author

Matthew Horner is a Cybersecurity Engineer with Engility Corporation in Bedford, MA assessing the risk of Air Force information systems. He was previously a Lieutenant in the US Navy and served aboard the USS Alabama, a nuclear-powered ballistic missile submarine in Bangor, WA, helping to prevent an unfriendly exchange of nuclear missiles. He may be reached at matthewshorner@gmail.com.

Notes

- 1 Thomas Fox-Brewster, "Want Some Nuclear Power Plant 'Zero Day' Vulnerabilities? Yours for Just \$8,000," *Forbes website*, October 21, 2015.
- 2 NEI, "Cybersecurity Strictly Regulated by NRC; No Additional Regulation Needed," *NEI website*, March 2014, <https://www.nei.org/resources/reports-briefs/cybersecurity-for-nuclear-power-plants> (accessed May 2, 2018).
- 3 "Targets for Terrorism: Nuclear Power Plants," *Council on Foreign Relations*, January 1, 2006, <http://www.cfr.org/homeland-security/targets-terrorism-nuclear-facilities/p10213> (accessed October 2, 2016).
- 4 The White House, *Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*, Washington, DC: US Government Publishing Office, 2013.
- 5 Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks*, (London: Chatham House, 2015).
- 6 DHS, *Nuclear Reactors, Materials, and Waste Sector-Specific Plan*, Washington, DC: Government Printing Office, 2015.
- 7 NRC, "Backgrounder on the Three Mile Island Accident," *NRC website*, December 12, 2014, <http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html> (accessed October 3, 2016).
- 8 World Nuclear Association, "Three Mile Island Accident," *World Nuclear Association website*, January 2012, <http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/three-mile-island-accident.aspx> (accessed October 8, 2016).
- 9 US Department of Energy, *March 28, 1979: Three Mile Island*, <https://energy.gov/management/march-28-1979-three-mile-island> (accessed December 7, 2016).
- 10 Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks*, (London: Chatham House, 2015).
- 11 Ibid.
- 12 *SCADA Schematic Overview*, September 18, 2013, https://commons.wikimedia.org/wiki/File:SCADA_schematic_overview-s.svg (accessed December 7, 2016).
- 13 Scott Berinato, "Debunking the Threat to Water Utilities," *CIO Magazine website*, March 15, 2002, <http://www.cio.com/article/2440931/security0/debunking-the-threat-to-water-utilities.html> (accessed October 3, 2016).
- 14 Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25.
- 15 Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks*, (London: Chatham House, 2015).
- 16 NRC, *Map of Power Reactor Sites*, November 13, 2015, <http://www.nrc.gov/reactors/operating/map-power-reactors.html> (accessed December 7, 2016).
- 17 Jessie Smith, "Cybersecurity is Alive and Well in US Nuclear Power Plants," *National Cybersecurity Institute website*, December 10, 2015, <http://www.nationalcybersecurityinstitute.org/energy-utilities/cybersecurity-is-alive-and-well-in-us-nuclear-power-plants/> (accessed October 3, 2016).
- 18 NEI, "Cyber Security for Nuclear Power Plants," *NEI website*, July 2016, <http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants> (accessed October 3, 2016).
- 19 NRC, *Map of Power Reactor Sites*, November 13, 2015, <http://www.nrc.gov/reactors/operating/map-power-reactors.html> (accessed December 5, 2016).

- 20** US Government, "CFR Title 10 Chapter 1," *GPO website*, 2016, <https://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR&searchPath=Title+10&oldPath=&isCollapsed=true&selectedYearFrom=2016&ycord=285>.
- 21** The White House, *Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*, Washington, DC: US Government Publishing Office, 2013; NEI, "Cybersecurity Strictly Regulated by NRC; No Additional Regulation Needed," *NEI website*, March 2014, <https://www.nei.org/resources/reports-briefs/cybersecurity-for-nuclear-power-plants> (accessed May 2, 2018).
- 22** NEI, "Cyber Security for Nuclear Power Plants," *NEI website*, July 2016, <http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants> (accessed October 3, 2016).
- 23** NRC, "10 CFR 73.54 Protection of Digital Computer and Communication Systems and Networks," *NRC website*, December 2, 2015, <http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html> (accessed September 24, 2016).
- 24** Ibid.
- 25** NRC, "Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities," *NRC website*, January 2010, <http://www.nrc.gov/docs/ML0903/ML090340159.pdf> (accessed October 5, 2016); NEI, "NEI 08-09 Rev 6 Cyber Security Plan for Nuclear Power Reactors," *NRC website*, April 2010. <http://www.nrc.gov/docs/ML1011/ML101180437.pdf> (accessed October 5, 2016).
- 26** NIST, "NIST SP 800-30 Revision 1 Guide for Conducting Risk Assessments," *NIST website*, September 2012, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf> (accessed October 4, 2016).
- 27** NEI, "Cyber Security for Nuclear Power Plants," *NEI website*, July 2016, <http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants> (accessed October 3, 2016).
- 28** NEI, "Cybersecurity Strictly Regulated by NRC; No Additional Regulation Needed," *NEI website*, March 2014, <https://www.nei.org/resources/reports-briefs/cybersecurity-for-nuclear-power-plants> (accessed May 2, 2018).
- 29** Ibid.
- 30** Jessie Smith, "Cybersecurity is Alive and Well in U.S. Nuclear Power Plants," *National Cybersecurity Institute website*, December 10, 2015, <http://www.nationalcybersecurityinstitute.org/energy-utilities/cybersecurity-is-alive-and-well-in-us-nuclear-power-plants/> (accessed October 3, 2016).
- 31** Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks*, (London: Chatham House, 2015).
- 32** Michel Kabay, "Attacks on Power Systems: Hackers, Malware," *Network World website*, September 13, 2010, <http://www.networkworld.com/article/2217684/data-center/attacks-on-power-systems--hackers--malware.html> (accessed October 7, 2016).
- 33** Ibid.
- 34** Ibid.
- 35** Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25.
- 36** NRC, *Davis-Besse Nuclear Power Station, Unit 1*, February 10, 2017, <https://www.nrc.gov/info-finder/reactors/davi.html> (accessed February 15, 2017).
- 37** Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25.
- 38** Ted Lewis, *Critical Infrastructure Protection in Homeland Security*, 2nd. (Hoboken, NJ: John Wiley & Sons, Inc, 2015).

- 39 NEI, "Cyber Security for Nuclear Power Plants," *NEI website*, July 2016, <http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants> (accessed October 3, 2016).
- 40 Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25.
- 41 Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks*, (London: Chatham House, 2015).
- 42 Ibid.
- 43 Terry Hardy, *Software and System Safety*, AuthorHouse, 2012.
- 44 Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25.
- 45 Ibid.
- 46 US Tennessee Valley Authority, *TVA.gov*, https://www.tva.gov/file_source/TVA/Site%20Content/Energy/Our%20Power%20System/Nuclear/Images/Browns-Ferry.jpg (accessed February 15, 2017).
- 47 Nicole Perlroth, "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say," *The New York Times website*, July 6, 2017. <https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html>. (accessed January 18, 2018).
- 48 Ibid.
- 49 Ibid.
- 50 Ibid.
- 51 Symantec, "Advanced Persistent Threats: A Symantec Perspective," *Symantec Corporation website*, November, 2011, https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf. January 18, 2018.
- 52 Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25.
- 53 Thomas Fox-Brewster, "Want Some Nuclear Power Plant 'Zero Day' Vulnerabilities? Yours for Just \$8,000," *Forbes website*, October 21, 2015.
- 54 Ibid.
- 55 Ibid.
- 56 Eric Byres, "Enough Clucking - Start Fixing the SCADA Security Problem," *Tofino Security website*, September 9, 2013, <https://www.tofinosecurity.com/blog/enough-clucking-%E2%80%93-start-fixing-scada-security-problem> (accessed October 8, 2016).
- 57 Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks*, (London: Chatham House, 2015).
- 58 NRC, "Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities," *NRC website*, January 2010, <http://www.nrc.gov/docs/ML0903/ML090340159.pdf> (accessed October 5, 2016); DHS, *Nuclear Reactors, Materials, and Waste Sector-Specific Plan*, Washington, DC: Government Printing Office, 2015; NEI, "Cyber Security for Nuclear Power Plants," *NEI website*, July 2016. <http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants> (accessed October 3, 2016).

- 59** Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25; Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks*, (London: Chatham House, 2015).
- 60** Kim Zetter, "An Unprecedented Look at Stuxnet, The World's First Digital Weapon," *Wired website*, November 3, 2014, <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/> (accessed September 24, 2016).
- 61** Ibid.
- 62** Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25.
- 63** Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks*, (London: Chatham House, 2015).
- 64** World Nuclear Association, "Three Mile Island Accident," *World Nuclear Association website*, January 2012, <http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/three-mile-island-accident.aspx> (accessed October 8, 2016).
- 65** Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks*, (London: Chatham House, 2015).
- 66** Ibid.
- 67** Ibid.
- 68** Ted Lewis, *Critical Infrastructure Protection in Homeland Security*, 2nd. (Hoboken, NJ: John Wiley & Sons, Inc, 2015).
- 69** Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25.

Copyright © 2018 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS). Cover image by Z22 https://commons.wikimedia.org/wiki/File:Three_Mile_Island_Nuclear_Generating_Station.jpg

TERRORISM

Book Review:
Illusions of Terrorism
& Counter-Terrorism
by Richard English

reviewed by Scott Romaniuk



Suggested Citation

Romaniuk, Scott. "Book Review: Illusions of Terrorism and Counter-Terrorism by Richard English (Ed.). Oxford: (Oxford University Press, 2015). 174pp., £40.00 (h/b), ISBN 9780197265901." *Homeland Security Affairs* 14, Article 5 (April 2018). <https://www.hsaj.org/articles/14313>

Terrorism, counter-terrorism, and their intersection have produced painful experiences for peoples and communities in many societies. The convergence of terrorist attempts to harm states and states' attempts to prevent their efforts raises important questions about the influence they have on each other. This relationship forms the core focus of *Illusions of Terrorism and Counter-Terrorism*, proceedings of the British Academy edited by renowned terrorism scholar, Professor Richard English. The nine chapters in this volume are unified by the deceptively simple question: how does one shape the other? If scholars were to take stock of what we have learned about this intimate relationship, they would find that very little actually is known about the interaction between powerful states and individuals, groups, and loose networks of violent extremists devoted to violent acts of aggression.

The introductory chapter exposes the gaps in the existing literature, and establishes the relevance of the book by reasoning that scholars have neglected to produce a robust and multi-disciplinary discussion of the dynamic, interactive relationship between terrorism and counterterrorism. In spite of the existence of valuable pioneering scholarship that was subsequently "complemented by a vast explosion of research and publication after 9/11," there is a need for "a more comprehensive and candid assessment of the ways in which terrorism and counter-terrorism operate" (p. 3). English highlights the problematic nature of engaging with the definition of terrorism and determining whether current definitions are fitting with current international terrorist practices. Additionally, he underscores the importance of re-assessing issues of proportionality and success in countering post-9/11 terrorist threats. Over-reliance on existing policies and practice without understanding what a *good* counter-terrorism model actually looks like creates a quagmire for scholars and practitioners. The analytical challenges illustrated by English and reinforced by the financial expenditures measured over nearly two decades include the unknown effects of the over-application of force, insufficient understanding of what role regimes play in terrorist support, and misreading the psychological structures of terrorists. The aim of the book is to push the debate on these issues and the broader topic forward through multidisciplinary dialogue among scholars embarking on variegated substantive approaches.

In chapter two, Alia Brahimi contextualizes the major themes of the book and embeds them in the "9/11 decade." This decade shows, according to the author, that the broad and overarching sledgehammer approaches to combating terrorism, much like the narrower and precision counter-terrorism operations of the Obama years, have done much to reinforce the illusory promise of military power as the ideal counter-terrorism prescription (p. 38). Brahimi analyzes many of the factors that have led to counterterrorism successes and failures and posits valuable counter-terrorism lessons for the future.

Rashmi Shingh, in chapter three, builds on the products of the counter-terrorism operations that took place under the rubric of the “Global War on Terror” over the past decade and a half. Shingh explores three major lessons extrapolated from this securitization program under the GWOT label. First, she scrutinizes the most significant changes that have taken place in the strategic character of warfare. Second, she examines the “law of unintended consequences” (p. 45). Third, she assesses the extent to which the “Global War on Terror” has enhanced al-Qaeda’s ability to mobilize and has strengthened its violent ideology. Western approaches have by and large misread the degree to which people support radical Islamic views, extremist groups like al-Qaeda, and ISIS. There has also been a misunderstanding of the effects of the over-application of military force.

In chapter four, David Omand considers the limits of Western counter-terrorism policy and attempts to ascertain where those limits ought to lie. The author develops the concept of the “‘thermodynamics’ of counter-terrorism,” and applies it to a comparative analysis of British and American experiences in counterterrorism. His analysis culminates in the question: “[h]ow can a government best exercise its primary duty to protect the public in the face of a severe terrorist threat and yet maintain civic harmony and uphold democratic values and the rule of law at home and internationally?” (p. 57) This question exposes the crisis of public confidence regarding government efforts in the “Global War on Terrorism.”

Chapters five and six by Conor Gearty and Adrian Guelke, respectively, delve into the tension that exists between effectively countering terrorism and respecting and defending human rights and civil liberties. This is an inadvertent and unfortunate by-product of the war against terrorists who may or may not be aware of the strain that the threat of terrorism alone places on the preservation and protection of liberal democratic principles and freedoms. The result is a discussion about “taming democracy” (p. 77-83) and the cultivation of “militarized” and “imperialist” democracy (pp. 83-90). Achieving a fresh and effective approach to counterterrorism, notes Guelke, can be next to impossible, given the “blowback from the actions of [previous administrations such as] the Bush Administration.” (p. 109)

Chapter seven by Audrey Kurth Cronin hits at the heart of the concept of “ghost chasing,” as the FBI terms it, with authorities pursuing an illusion of terrorism and terrorist threats that are oft-times conflated. State portrayal of terrorism stems from state-level overreaction, resulting from the unpredictability of future threats, thus imbuing terrorists with the confidence to continue acting in pursuit of their violent doctrines. This leads to a tendency for states to drape themselves in the mantle of victimhood. The author illustrates that understanding terrorists’ true capabilities is critical for the ability of states to act on counterterrorism opportunities.

In chapter eight, English analyzes contemporary dissident Irish Republicanism as a case for explaining terrorism’s endurance. The chapter paints a convincing portrait about the mutual relationship between terrorism and counter-terrorism. It drives home the point that misreading the societal roots of terrorism will ultimately lead to flawed approaches in countering it. English argues that effective counterterrorism policy requires greater awareness of how terrorism is grounded in societal level forces.

The proportionality dimension and potential repercussions of state counter-terrorism policies and practices are fleshed out in chapter nine by David A. Lake. The author analyzes the extent to which state counterterrorism responses are proportional to the threat posed by terrorism.

This volume brings together leading scholars and experts from across academic fields and subfields to examine the intricate dynamics of counter-terrorism after 9/11. The relationship between terrorists and state actors combating this international threat in the post-9/11 security environment provides the unifying framework of the volume. It is evident that the book has been designed in a way so that academics and practitioners can engage the content with relative ease. *Illusions of Terrorism and Counter-Terrorism*, accordingly, achieves its stated objectives. Although one might expect a volume comprised of expert-written chapters to provide all the answers, effectively countering terrorism in the unpredictable security environment of the 21st century requires counterterrorism experts to pose more questions and engage further with empirical data to first produce a clear picture of the threat. This concise volume is packed full of valuable perspectives on a costly era of confrontation between states and terrorist networks. It identifies multiple avenues for further in-depth research and investigation of the complicated relationship between terrorism and counterterrorism. It would be useful reading for scholars, practitioners, and students of terrorism and counterterrorism.

Copyright © 2018 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

Operator Driven Policy: Deriving Action From Data Using The Quadrant Enabled Delphi (QED) Method

By Lilian Alessa, Sean Moon, David Griffith & Andrew Kliskey



Abstract

To close the gap in operator-driven policy for the homeland security enterprise, we argue for a bottom-up policy process that acknowledges operator knowledge and opinions. We propose a practical approach to enable policy-makers to incorporate operator knowledge and experience, or operator driven policy (ODP), into policy through the Quadrant Enabled Delphi (QED) approach. We set out the theoretical requirements for QED, based on cognitive science. Using the EARTH-X QED workshop as a case-study, we demonstrate the application of QED focused on emerging Arctic security threats, and highlight key lessons for applying QED. Finally, we recommend an appropriate operator-driven policy-making process that incorporates the QED approach as a bottom-up policy process.

Suggested Citation

Alessa, Lilian, Sean Moon, David Griffith & Andrew Kliskey. "Operator Driven Policy: Deriving Action From Data Using The Quadrant Enabled Delphi (QED) Method." *Homeland Security Affairs* 14, Article 6 (September 2018). <https://www.hsaj.org/articles/14586>

Introduction

Operators are the tip of the spear for the security enterprise; they are the boots on the ground and the hands that bear the brunt of ensuring a mission succeeds. "Operators" in the context of this paper are those personnel working on field-level operations (for example, Coast Guard officers and sailors assigned to sectors or stations, and Customs and Border Protection Officers assigned to Ports of Entry). It is they who willingly go into harm's way to protect, serve and safeguard the American people. Despite this, there does not exist a consistent, structured methodology for eliciting operator input at all levels of strategic development.¹ Policy that does not include consideration of operator needs is policy that can inadvertently increase the difficulty of mission performance and introduce vulnerabilities into the homeland security enterprise. We seek to change this pattern through the development of Operator Driven Policy (ODP). Toward this end, we offer the Quadrant Enabled Delphi (QED) method as a mechanism for systematically working with operators to better understand their operational needs and construct policies that best serve them to engage in continuous versus rigid planning. The article first introduces the policy process and the role of operator perspectives; then it considers the strength and weaknesses of the classic Delphi method as an approach for incorporating operator perspectives; finally it sets out theoretical underpinnings for an operator driven approach, and details the QED method as an alternative to the standard Delphi approach. We use a case-study to demonstrate the QED method and approach, and to highlight lessons learned in applying QED. Finally, we propose an ODP process for using QED to incorporate operator perspectives within the policy process.

Transforming Policy to Serve Operators

Policy-makers generally define policy as a course of action adopted and pursued by a government, political party, or other body.² From the standpoint of meeting an organization's mission objectives in support of national and homeland security, however, a more useful interpretation is that "policy" is the intersection of politics and performance. Put another way, it is the point at which "will" or "guidance" as expressed by law, regulation, or authoritative direction, is interpreted in such a way as to drive strategies, plans, and tactics toward realizing that will or guidance in support of sustained and successful outcomes. One can view policy as the joining of requirements with the abilities, capabilities, and constraints of operations, but frequently policies are viewed as originating from the leadership of an agency or government office.³ ODP is proposed as a less expensive and more effective form of policy-making than current approaches. ODP is based on acquiring and synthesizing information on the needs and concerns of operators (our clients) to frame strategic planning, implementation, and resourcing while also meeting legal and enterprise-wide requirements.⁴ In short, ODP is a hybridized bottom-up approach to policy-making in contrast to conventional top-down approaches.⁵ By ensuring that policy and strategic development are fully informed by both political (e.g., societal drivers as expressed through legislative or executive action) and operator levels (e.g., practical constraints on enforcement actions or implementation of strategy), the homeland security enterprise will be more effective in executing its mission while achieving cost-savings. To serve ODP, we developed the QED method as a practical approach to enable policy-makers to solicit and incorporate such information into Operator and Headquarters-driven policy development. The premise here is that good policy should incorporate the perspectives of operators in concert with those of experienced policy-makers, rather than valuing one perspective over the other. This premise was demonstrated when President Trump specifically tasked executive departments and agencies with conducting a bottom-up review of all immigration policies, asking law enforcement professionals (i.e., operators) to identify reforms to protect national interests. In his October, 2017 letter to House and Senate leaders, he noted that those professionals identified dangerous loopholes, outdated laws, and easily exploited vulnerabilities.⁶

Operator-Driven Data and the Need for Systematic Policy Development

Operator needs span the continuum from procuring equipment to the means to acquire, share, and act on information through communication and coordination. Needs in the field can include everything along this continuum, often in a rapidly evolving incident setting where there is little stability. While certainly important to the enterprise, the critical distinction between operators and rear echelon personnel is the direct and immediate service of a mission imperative (although rear echelon personnel can also be operators, provided they have experience at the field level). For example, operations centers need to be in constant communication with higher-level unity of command centers to receive regional alerts and requests to respond. Specificity and precision of situational awareness are important to ensure that resources, assets, and responses are utilized in the most efficient manner. This seemingly straightforward process belies the complex (i.e., emergent) and complicated

nature of field operations and the policies that enable or constrain them. To address this complexity through a dynamic process of strategic planning, resourcing, and execution, we need to examine the current process by which policy is formed.

The prevalent model of policy development is a top-down process typically driven by senior management in Washington, DC.⁷ Senior leadership, often politically appointed and lacking in field operations experience, interprets political signals or statutory imperatives to drive planning, programming, budgeting, and execution decisions.⁸ Leadership reinforces this model in organizational structures where they select primary policy-makers from external sources such as academia or think tanks, or where there is no requirement of relevant field experience.⁹ To underscore this point, consider that as of June 2018, the “Strategy and Analysis” subunit within DHS Policy has no permanent personnel with operational field experience, being entirely staffed by individuals with academic or headquarters-level civil service backgrounds. This results in a Dunning-Kruger effect in which policy-makers may not understand field conditions and are potentially unaware that they lack such understanding.¹⁰ While there are some benefits to creating policy at a high organizational level (e.g., headquarters units tend to have broader viewsheds than field units, they are closer to political and economic realities, and have access to the resourcing necessary to implement policy), they frequently omit the operators from the decision-making process, relying instead on working groups of administrators who are readily available in Washington, DC, rather than allocating often limited resources to bring field personnel to the table. A partial exception to this is when subordinate Headquarters units are staffed predominantly by field personnel, such as the U.S. Coast Guard where Headquarters tours are part of an overall rotation and assignment process that focuses predominantly on field operations. This situation means that when resourcing occurs, the need to include views from the ground is not always met.

Consider the following real-world example of this type of top-down decision-making process and its consequences. In 2006, Congress created a requirement that the DHS implement a program in at least three foreign ports to test the feasibility of screening 100% of maritime cargo containers destined for U.S. ports.¹¹ Before the pilot program was fully implemented or the feasibility of the screening approach could be assessed, in 2007 Congress passed and the President signed another law establishing a July 1, 2012 deadline requiring that 100% of all U.S.-bound cargo from foreign ports be scanned.¹² The statute authorized the Secretary of Homeland Security to extend the initial 2012 implementation deadline for two additional years every two years, repeatedly, provided that DHS met certain conditions. The implicit policy of the Department, that the conditions preventing implementation exist and remain true, has been consistently communicated to Congress on a biannual cycle. However, the explicit policy of the Department has been that DHS would make every effort to comply with the law. Had field operators been consulted by those preparing the SAFE Port Act or the 9/11 Act or had they been allowed to provide input during the biannual review cycle, certain fundamental policy failures would have been readily identified. It would have become clear that the cargo screening requirement would produce only a slight increase in security while imposing impossible-to-meet operational burdens, because of the obvious issues with implementing an unenforceable policy requiring significant expenditures by trading partners in their own port facilities. Additionally, the policy required the installation by foreign partners of equipment originally manufactured only in the United States and slowed commerce with every cargo container scanned. The policy also failed to create the institutional capacity to review the 20 million or more images that would be produced a year by successful scanning. Instead, due to the divergence of top-down policy and in-the-

field reality, the implementation deadline for the law has been extended three times since it came into effect, but the law continues as written despite the recognition by Congress that the requirements are infeasible and would come at an unacceptably high cost both monetarily and in terms of displacement of other effort.¹³

While there are no guarantees that policy-makers will heed operator insights and inputs, in cases such as the 100% scanning deadline, doing so could have prevented an unenforceable law from being enacted. Addressing why the law and its resultant policies persist is beyond the scope of this article, though it is frequently discussed in trade journals dedicated to global supply chains. The critical factor is that, absent input from people who actually understood field operations and could have immediately identified the challenges, a seemingly reasonable but impractical mandate was issued.

Soliciting Operator Inputs: Re-Thinking the Delphi Method

To solicit systematically the input of operators, the authors examined various methods for acquiring information from experts in a field, starting with the Delphi Method. We found that the Delphi Method, originally developed by the RAND Corporation in the early 1950s to solicit and understand the view of experts related to national defense, is a well-used methodology for gathering and creating consensus among subject matter experts.¹⁴ The term originates from Greek mythology – Delphi was the site of the Delphic oracle, the most important oracle in the classical Greek world. The Delphi method can be characterized as a method for structuring information derived from a group of experts to derive a consensus on the best available knowledge with respect to a complex problem.¹⁵ In general, the approach utilizes standard survey instruments and the subsequent synthesis of the results to acquire expert opinions.¹⁶ The historic strength of the Delphi method was that it provided a structured approach for eliciting and reporting expert knowledge, and in some cases systematically achieving consensus among subject matter experts. It is still used today by the RAND corporation to do their futures scenarios planning.

However, the Delphi method has several shortcomings. Due to the overuse of surveys, individuals are less likely to respond unless they have extremely strong opinions and are more outspoken. There has also been a decline in response rates during iterative surveys, particularly those involving three or four rounds.¹⁷ Additionally, use of pre-workshop surveys as a core component of the Delphi approach is not optimal because it creates a strong group bias (among the survey preparation group) that is not necessarily representative of collective experience or knowledge of the experts. This predisposes subsequent Delphi-based workshop rounds to this bias, rendering the outputs less accurate.¹⁸ Finally, the traditional RAND Delphi does not take into account the plurality of cognitive skill-sets of participants involved in the process and often introduces significant bias into the outputs in other ways. Introduced biases can result from: pre-determined scenarios and/or surveys sent to workshop participants that introduce a first level bias; facilitators who are not trained in cognitive elicitation methods and who may not be able to work with a plurality of individual communication and interpretation styles; lack of standardization in methodology, both across and within the method and its applications that may produce qualitative data that cannot be compared; and preference for participants who are available versus those

who are truly expert attendees (see the “Participant Backgrounds” Section, below). These, among other factors, can yield results that may be inaccurate or misleading.¹⁹ To address these shortcomings, we developed the Quadrant Enabled Delphi (QED), and propose that the QED is needed to solicit expert input that serves the development of precise and targeted ODP based on the critique above.²⁰

Theoretical Basis for an Operator-Driven Policy Approach

Two main bodies of knowledge inform the structure of Operator-Driven Policy developed through the Quadrant Enabled Delphi: theories of human organization, specifically agent types, and theories of cognition.

Human Organization: Agent Types

Each of us behave as autonomous agents (e.g., individuals) and possess cognitive elements, which are subject to social influence and infrastructural (e.g., economic) constraints.²¹ The concept of “agents” and “roles” is not new and occurs in diverse fields of study ranging from artificial intelligence²², to sociology²³, to psychology.²⁴ A cognitive agent (i.e., a person) has three key features: cognition (perception), reason (preferences), and purpose (intentions).²⁵ These features encompass the general concept that agents are intelligent actors who respond to social and institutional stimuli in multiple ways including hysteresis (e.g., not responding to a stimulus until it carries risk), learning (e.g., becoming more efficient), and values (e.g., the Prisoners’ Dilemma).²⁶ Roles are carried out by agents based on both their formal and informal situation within a network or group.²⁷ The dynamics of human responses to change are often studied at the scale of institutions and/or populations.²⁸ Agents can be categorized into three broad categories: “initiators” (or alpha agents); “supporters” (or beta agents); and “opportunists” (or gamma agents).²⁹ Agent types can be likened to the theoretical and empirical roles of leaders and followers in a group context concerned with achievement of a common goal.³⁰

In the context of expert workshops, alphas can be outspoken and persuasive, are often articulate, and are generally concerned with moving toward a unity of effort regardless of personal gain or opinions. Betas represent most attendees who are willing to listen to a range of inputs and form conclusions based on discussion. Gammas are individuals, who, like alphas, are often outspoken and persuasive but are focused on advancing a specific agenda regardless of whether it advances unity of effort. Each class of participant requires different interactions with facilitators to ensure their voices are heard and their expertise is equally represented in products. For our purposes, this must be accomplished as part of an operator-driven approach.

Decision Making and Cognition

An extensive body of knowledge provides relatively deep, but highly variable, insights and data regarding the mechanisms of decision-making and cognition. Despite the general thought that “better data equal better decisions,” there is overwhelming evidence that emotions strongly influence cognitive decision processes.³¹ Quantitative evidence further supports the idea that perception, rather than objective data, often drives decisions.³² As a consequence, we propose incorporating several specific processes into consideration for an operator-driven approach: cognitive traps/biases, cognitive walkthroughs to access both explicit and implicit knowledge possessed by workshop participants, and distinguishing types of knowing and knowledge.

Cognitive Traps (CTs)

For many settings across government, especially at the federal level, decision-making is handled by a group of individuals who come together as representatives of different agencies and services. Such interagency decision-making processes result in a series of “cognitive traps” (CTs, also referred to as “Cognitive Biases”): that is, an inability to explore mentally new strategies or actions beyond those that are well known and familiar. Such cognitive traps must be addressed to enable operator-relevant and effective decision-making.³³ CTs help us to understand the resultant processes that can enhance or impede decision making during an operator-driven process, particularly with respect to knowledge of agent types (individuals) and social niches (in professional teams). For groups of participants that have legacy issues (see Addressing Elephants below), repeated actions may be an impediment to listening to alternative viewpoints due to conditioned actions and responses.³⁴

The dynamics resulting from the interactions of these different kinds of cognitive biases in a group produce coordinating cues and signaling behaviors, which are often relayed subconsciously as well as overtly.³⁵ Visual and verbal cues signal to others the status of a given agent in the group.³⁶ These fundamental qualities of individual and group behaviors must be considered in the context of the explicit and implicit knowledge of the participants.

Cognitive Walkthroughs

The use of cognitive walkthroughs is a critical component of an operator-driven approach and is based on observations that daily interactions with computers and other digital technologies are changing the way we perceive, analyze information, and make decisions.³⁷ The use of cognitive walkthroughs ensures that these emergent cognitive patterns are leveraged, particularly among younger participants. For example, Norman’s Human Action Cycle describes the steps a person takes when interacting with a computer system,³⁸ starting with the formulation of the user’s goals through to accomplishment of those goals.

Knowing

Explicit knowledge is generally defined as “knowledge that the knower can make explicit by means of a verbal statement that can be elicited from them by suitable enquiry or

prompting.”³⁹ Implicit knowledge is generally defined as any other kinds of knowledge including those often characterized by phrases such as ‘gut feelings’ and ‘I just know,’ or other complex, subjective, and subconsciously, driven means of coming to a decision fork and/or conclusion.⁴⁰ In this construct, implicit knowledge corresponds roughly to what Polanyi called “tacit knowing”: we can know more than we can tell, but such knowledge is difficult to describe linearly and relay.⁴¹ Doctors and decision-makers in the military and law enforcement rely on tacit knowledge in decision-making contexts.⁴² In the military, especially, tacit knowledge is often identified as intuition and cultivated to support rapid decision making in complex and urgent situations.⁴³ The original Delphi Method primarily addressed explicit knowledge, allowing “experts” to provide question-answer information that was compiled into a report. Operator-driven approaches are designed to acquire and enhance both explicit and implicit knowledge, as the latter is often possessed and valued by the most experienced, effective, and expert operators. We propose augmenting these types of knowing with something called “local and place-based knowledge” (LPBK), which can provide location-specific context for decision-making: a critical component of operator-driven policy which can ensure that decisions are relevant to the geographic and temporal scales on which field agents conduct operations. Since collective knowledge constructs institutions, policy development strategies which don’t capture the diversity of knowledge available (explicit, implicit, and LPBK) necessarily fail to address real-world scenarios while also generating outcomes based on incomplete or flawed data inputs.⁴⁴

The QED Methodology

The QED methodology was designed by the University of Idaho’s Center for Resilient Communities to serve ODP and is built on the cognitive science and human organization principles described above. QED replaces the traditional Delphi pre-workshop survey with recursive, in-person social processes. Facilitators bring experts together in-person, elicit subject-area knowledge, and build consensus while iteration occurs through a series of both structured and semi-structured sessions in 1-2-day long workshops.

In QED, facilitators initially present a series of carefully crafted challenge questions to a diverse group (the Delphi group) to initiate discussion. These questions are specific to the topic at hand but crafted so as not to introduce bias. Facilitators then oversee responses of the panel of experts, helping them express their opinions concisely and accurately while recording the points raised. Facilitators select members in consultation with the organizing or hosting agency because they are subject matter experts in fields related to the challenge questions; they represent a broad range of relevant organizations and agencies; and they provide a diverse mix of operator experiences. The success of this process depends on the expertise, professionalism, and communication skills of both participants and facilitators. We describe a case study of the implementation of QED below in order to explain the methodology, and we then describe the core elements of QED.

Case-Study– Emerging Arctic Threats

The workshop on Emerging Arctic Threats (EARTH-X) convened in Washington, D.C. on February 1 and 2, 2017, and was attended by 85 security and intelligence professionals from over 35 U.S. and Canadian federal and state or provincial agencies. The workshop

was held under the Chatham House Rule: individual participants were not named, although the names of agencies and institutions represented were recorded, to ensure anonymity in workshop reporting and to foster open dialog during the meeting. The workshop goal was to establish an understanding of the emerging security landscape in the Canadian-United States (CANUS) Arctic by eliciting the most severe emerging security threats, developing a consensus on the highest priority threats, identifying capability gaps in tackling these threats, and generating consensus recommendations in response to the identified threats and gaps.⁴⁵ The workshop employed the QED methodology using a sequential and recursive format, a quadrant layout for facilitation, and the 80/20 rule for prioritization of data.

1 – Sequential and Iterative Phases

The QED structure for the EARTH-X workshop entailed four iterative phases of facilitated brainstorming, discussion, rating, and consensus-building.

Phase 1 involved horizon scanning during which major security threats in the Arctic and the severity of those threats were identified through facilitated brainstorming. The workshop domain experts enumerated collectively 198 threats in the Arctic security sector.

Phase 2 involved prioritization of the major security threats for the Arctic through the Red dot/Green dot exercise (see below). The 80/20 rule dot method resulted in 14 threats ranked as highest severity, ranging from “Dark Target Tracking in Theater” to “Effects of Thawing Permafrost on Critical Infrastructure.” After narrowing the threat list to the most serious threats for the maritime, air, cyber, land, and all security domains, the threats were ranked in terms of overall priority, timescale, and spatial scale.

Phase 3 involved framing the threat continuum by identifying and prioritizing capability gaps in responding to the threats through facilitated rating. Following threat identification, participants identified 47 capability gaps hindering effective security operations in the Arctic domain. In a similar manner to Phase 2, participants ranked the capability gaps. The highest-ranked capability gaps ranged from “[L]ack of Persistent Sensors / Surveillance Frameworks” to “[L]ack of Situational Awareness.” This phase also enabled extraction of serious barriers to effective security operations in the Arctic, for example, the lack of critical information and information-sharing protocols.

Phase 4 involved identifying and prioritizing solutions through facilitated brainstorming and rating of solutions. The final outcome of the QED process at EARTH-X, based on the enumerated threats and the capability gaps, was a set of consensus recommendations on potential solutions to enhancing CANUS Arctic security. Participants achieved consensus through a facilitated group discussion of the group rankings of proposed solutions, that is, as a collective social process between facilitators and participants. For example, the group resolved to “revisit a comprehensive strategy for surveillance as a process” and to “develop tools and processes for better situational awareness for ground operations.”

2 – Quadrant Layout and Facilitation

The meeting venue with seated participants (i.e., operators) was divided into quadrants with a facilitator (or “quadrant manager”) for each quadrant (see Figure 1). The central facilitator (or “room manager”) coordinated the overall discussion and roamed among the different

quadrants. Each quadrant facilitator engaged the participants in their quadrant through verbal, visual, and physical cues. Quadrant facilitators also liaised with the central facilitator to adjust information elicitation based on the agent types in their quadrant. During the two-day EARTH-X workshop, the central facilitator role was shared between two people, alternating between primary and secondary roles.

For the EARTH-X workshop, quadrants represented air, maritime, land, and cyber domains. The quadrant facilitator in each quadrant had operational expertise specific to that domain, and this allowed them to not only serve as a resource to the participants in their quadrants but also to understand the comments recorded for their quadrants.

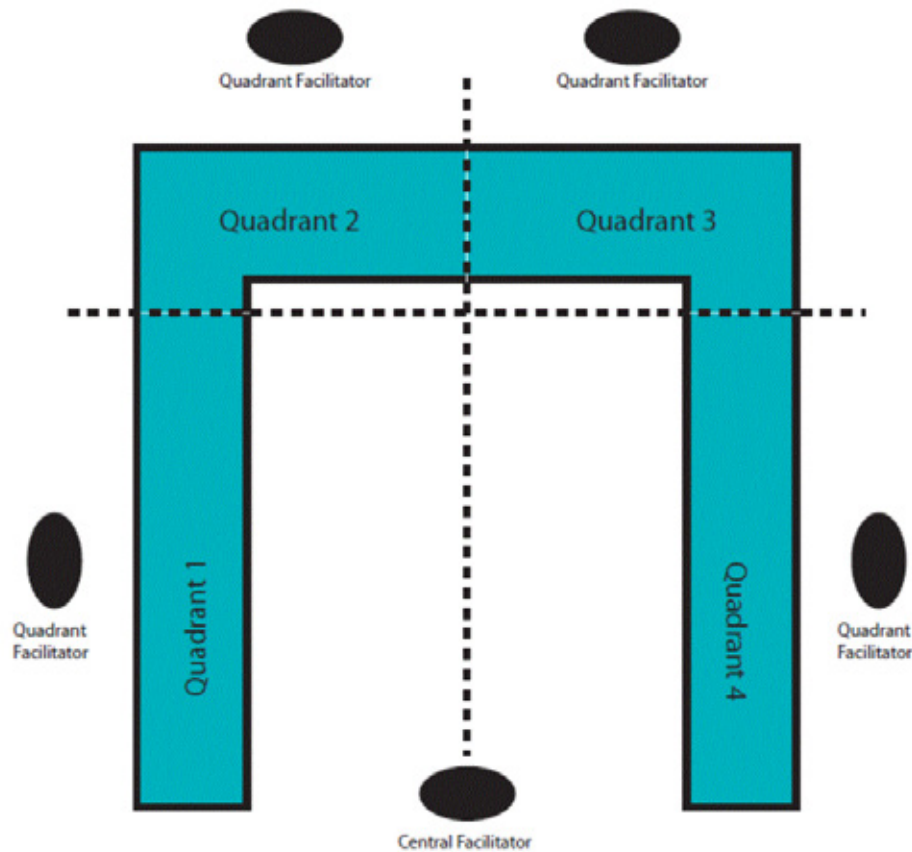


Figure 1. Quadrant layout for group facilitation in Quadrant Enabled Delphi (QED) method. Note that quadrants are defined by participant numbers, e.g. seats at the table, not quartering of the workspace

3 - The 80/20 Rule

As a means of leveraging the collective intrinsic and extrinsic knowledge of participants, QED uses the 80/20 rule to allow for rapid prioritization and sorting of group inputs. The 80/20 rule stems from the “Pareto Principle” which has multiple interpretations and applications depending on the context used, but is simply phrased as “80% of the output results from

20% of the input” and has been applied to quality control in electrical circuits, business management, and human decision-making processes.⁴⁶

During the EARTH-X workshop, reaching a consensus on ranking, for example, the vulnerabilities of critical infrastructure in the Arctic was accomplished through a series of iterative sessions including group generation of vulnerabilities and threats, group rating of those vulnerabilities and threats, and spatial mapping of vulnerabilities and threats. The ranking sessions involved participants placing color-coded adhesive dots on tabulated sheets generated during brainstorming to differentiate items and to assist with prioritizing them.

Key definitions used for the application of the 80/20 rule for ranking results in EARTH-X included:

- **Severity** - defined as the impacts and consequences of an event occurring: Severe (Critical)=immediate loss of safety and/or life, and/or critical infrastructure to multiple people; Significant (Acute)=predisposes the loss of safety and/or life and/or critical infrastructure within weeks; Moderate=may predispose the loss of safety and/or life and/or critical infrastructure within months.
- **Timescale** - defined as the time period in which a threat was most likely to manifest: Horizon 1 (1 to 5 years); Horizon 2 (5 to 10 years); Horizon 3 (10 to 30 years).
- **Spatial scale** - defined as the scale of impact of a threat or vulnerability: Local, National, and International.

The 80/20 rule modification guided the numbers of dots each participant received and how many cycles of the dot exercise were conducted for rating severity, timescale, and spatial scale for the generated vulnerabilities and threats (see Figure 2 for one visualization of results from ranking threats).

Accessible Outputs—Reporting Back and Actionable Data

After the first day of the EARTH-X workshop, the team conducted an analysis of the output. This generated a ranked and weighted score from the first 80/20 rule refinement, resulting in sets of 3-8 consensus “highest priority” threats and capability gaps. Those data were then discussed at the beginning of the second day and used as inputs for the next rounds of 80/20 rule exercises. Once the workshop had concluded, the leadership team produced a draft summary (within two weeks) and distributed it to the participants for comment and to verify and validate the results.⁴⁷

Once the participants had validated the report, it was provided to policy-makers (who were also participants in the exercise) engaged in developing strategies related to the Arctic, where it became the basis of strategic risk landscape analysis. This ensured that operator input was embedded in the strategy development process, while also enabling broader issues such as national objectives to be accommodated.

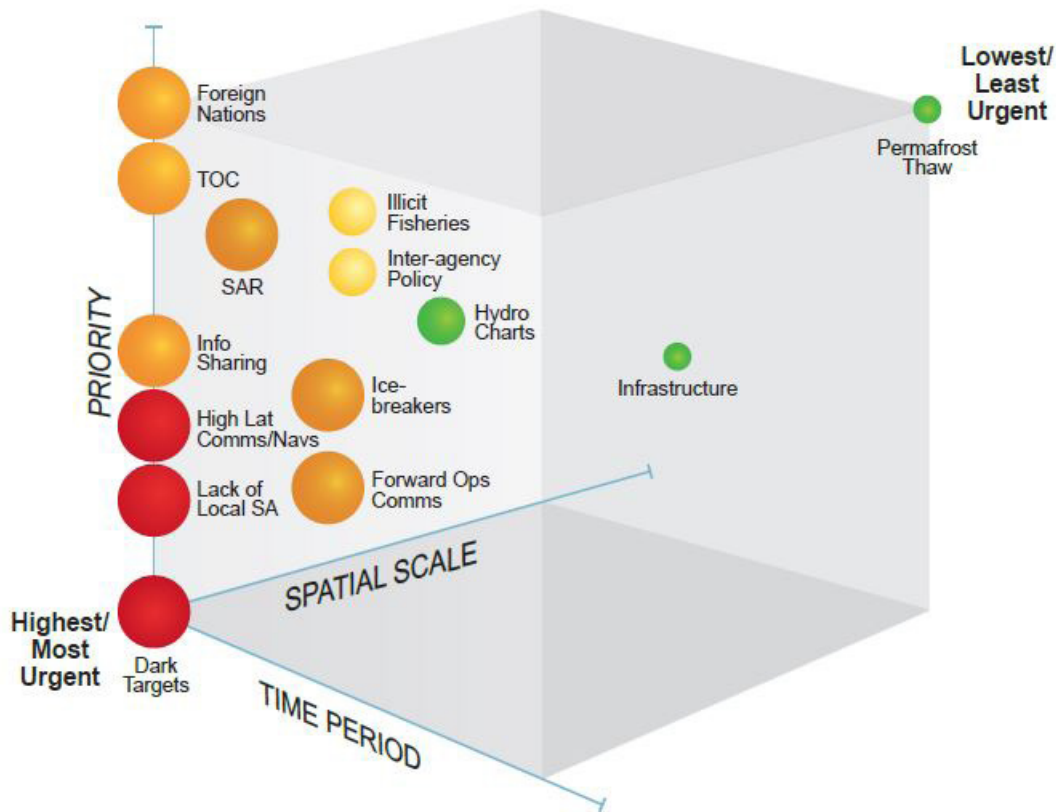


Figure 2. Cube framework for representing Emerging Arctic Threats from the EyesNorth QED Workshop held in 2017 (Alessa et al. 2017).

Lessons for the Application of QED

The QED method was developed and refined to ensure that systematic and rigorous data are acquired directly from the operators themselves. A closer examination of the QED methodology includes the following key components:

1. careful consideration of participant demographics, identifying and enlisting subject experts;
2. consistent methodology across QED sessions including operator selection;
3. establishment of trusted spaces for maximizing free expression of ideas;
4. rigorous validation and prioritization of information using a 80/20 rule exercise, and;
5. accessible and comparable outputs between and across QED events.

QED can establish settings where operators can express their expert perspectives and field-informed views without fear of reprisal or stigmatization. Additionally, QED leverages cognitive science and principles of human organization to enable data collection at the individual and group level. It also reveals group dynamics which can be used as proxies to understand broader-scale dynamics at agency and department levels. Finally, it also reveals the “unknown unknowns” by accessing, structuring and analyzing the tacit and implicit knowledge of a group of carefully selected expert “human databases” whose collective reasoning leads to insights that are otherwise not visible.

In addition to the facilitated discussion and brainstorming sessions, the QED method includes a written information submission mechanism that increases the number of solutions generated by larger groups, particularly by allowing beta agents, who often have well thought-out opinions but may not be comfortable vocalizing in a larger group, to express them freely. It also allows a larger number of inputs in a much shorter period, leading to concept diversity and a more robust set of decision options. Our experiences are consistent with data suggesting that in response to three different problems requiring creative thinking, the number and quality of inputs produced by “nominal groups” (whose members spent reflective periods working alone after or during group sessions) was of higher utility to decision makers.

Participant Background

A critical starting point for a successful QED process is ensuring that the attendees are representative of the appropriate subject matter expertise and roles that constitute the operational landscape from unity of command to unity of effort. Workshop attendees cannot be random or opportunistic, but should be carefully identified through an “ideal participant paragraph” in the participant solicitation and through leveraging peer networks. Here is an example of an Ideal Participant Paragraph:

Observing and monitoring system designers, data managers, and the operational users of the data generated by these networks are ideal participants for these workshops. Individuals whose responsibilities include processing, analyzing, and disseminating data for resource management, security and defense operations are also encouraged to attend. These include watch-standers for natural disasters such as wildfires, search and rescue, and humanitarian and disaster response. Individuals involved in countering illicit activities such as illegal, undocumented and unreported fishing (IUUF), and local stakeholders whose place-based knowledge can provide context to regional datasets are also welcome to attend.⁴⁸

Ensuring that participants have appropriate backgrounds also entails ensuring that the room is secure (peers respecting peers) and that new individuals cannot freely enter and engage with the QED cohort.

Quadrants

The “Q” in QED is critical because it structures the room and the participants into four sections or quadrants (Figure 1). This was based on our experience with the EARTH-X workshop and several other QED workshops that were run in 2017 and 2018, in which it emerged that there are typically four domain areas of critical interest, e.g., marine, air, land, and cyber domains in the case of EARTH-X. The use of four quadrants also allows for a straightforward room layout utilizing the four corners of a rectangular meeting space. Nevertheless, it is possible to run the process using say, 3 or 5 domain areas. However, use of a quadrant-based structure is also resonant with whole-brain theory, also known as the Four Quadrant Model, in which a quadrant-setting supports “Creators,” “Investigators,” “Activators,” and “Evaluators,” as subsets of agent-based operators.⁴⁹ The selection and use of quadrant facilitators/managers allows for a diverse team of facilitators who have the knowledge necessary to work the given subject during elicitation. Each quadrant represents a key area of focus for a given challenge in the issue at hand. Facilitator expertise, knowledge, and process understanding are critical to quality assurance and accuracy. If clarification is necessary, facilitators can pose the correct questions. This construction of information inputs is particularly important to the 80/20 rule dot exercise phase of the QED process.

Facilitators – Forming the QED Team

One of the more critical factors that determines the success of a QED workshop is the training and quality of the facilitators themselves. Facilitators must have the following qualities:

1. possess field and/or operator-relevant experience;
2. can parse information and inputs in the context of domain expertise;
3. possess outstanding listening and intervention skills, and;
4. have training in QED facilitation.

Beyond content expertise, quadrant managers are systematically trained in the QED approach to acquire specific skills that allow them to engage attendees and ensure that they participate in ways best suited to their personalities. Skilled facilitation may be necessary to ensure all opinions and views are safely elicited, and to maintain the professional decorum of the group. If not carefully managed, strongly expressed opinions or shared experiences may result in confrontations between participants. A quadrant manager uses a range of techniques to interact with attendees, ensuring that the entire suite of agent types is engaged appropriately. These include cognitive and trust-based interventions tailored to each participant that may be detached or overt.⁵⁰

Rotating the central facilitator role between sessions prevents fatigue during QED sessions and allows each to utilize and leverage individual strengths in group management and content expertise. The quadrant-enabled aspect of QED helps ensure harmonization of participation and improves the quality of information provided by the group. Ultimately, QED provides a structured, trust-based information exchange space where operators can provide honest input in the task of informing superiors within their organizations.

Selection of facilitators for QED is based on nomination and invitation. Trusted, capable facilitators are identified by already qualified personnel and generally vetted by being invited to serve as a quadrant facilitator during a workshop. Once identified and vetted, prospective facilitators undergo a 3-day training program that provides the key background (scientific theory), critical interaction skills (toolbox), and processes (workflows and analytical tools). The course takes place in a neutral location where students can freely explore a range of topics under each of these three areas. The third day is composed of a compressed QED workshop process with actual participants.

Trust Spaces

A critical component of QED is that of trust. We use the term “trust” here to mean the emotional state in which individuals feel secure enough to freely express their professional opinions in a setting free of perceived or actual consequences to personal or professional safety.⁵¹ Constructing trust spaces hinges on asking the right questions, those that specifically serve the resolution and illumination of the issue, and providing the means for the respondents to give honest answers without fear of repercussions. Facilitators can utilize several means, outlined below, to ensure that they construct adequate trust spaces.

Chatham House Rule

The Chatham House Rule originated at the Royal Institute of International Affairs, a non-profit, non-governmental organization based in London whose mission is to analyze and promote the understanding of major international issues and current affairs. The Chatham House Rule is designed to provide anonymity to speakers to encourage openness and sharing of information. It is used throughout the world as an aid to free discussion. The Chatham House Rule reads as follows:

When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.⁵²

Social Reinforcement and Trust Building in Real Time

Trust spaces rely on several layers of social intervention that can be difficult to balance, depending on the dynamics of the expert group physically present in the room. Ultimately, it begins with a strong and cohesive QED facilitation team whose backgrounds make them capable of empathy and relativity to the attendees themselves. A capable and empathetic, yet disciplined QED team conveys confidence in both their knowledge of procedure (i.e., confidentiality and respect) as well as their content expertise. More functionally, a trust space must be physically constructed by holding the workshop in a secure room where outsiders cannot randomly come and go, by constantly reminding attendees of the gravity of the Chatham House Rule and its origins, and by requesting that digital devices be put

away (a request that the facilitation team can reinforce by securing their own devices in an obvious fashion). Activities such as photographs and social media are prohibited (except for providing digital records of facilitation tools and products as an aid to later analysis). To reinforce these rules and create a common normative behavior set, facilitators require the attendees to exercise the highest level of their professional responsibilities. In almost all cases, they will respond favorably and collectively create and uphold shared trust both during the QED process and following it.

The “Magic Box”

Communication styles vary among individuals. In general, alphas and gammas are more likely to speak out than are betas. Among betas, there are sub-categories, which generally include active (B_{α}), obligate (B_{σ}), and passive (B_{π}). Active betas are more likely to provide verbal input followed by written comments after adequate information/evidence has been heard from the group. Obligate betas generally will “go with the flow” and provide the bulk of their inputs via written comments once they have assessed the majority sentiments. Passive betas usually either feel inadequate in terms of domain expertise and/or occupy a social niche which is subjugated to other betas and alphas in the broader group network. This does not mean that passive Betas do not have opinions, expertise, or inputs, but rather that they are unlikely to express that knowledge verbally and are more likely to provide only written comments. Individuals of all personality types may consider written comments to be a more accurate or considered format as the act of writing allows time to reflect and analyze. Additionally, written comments also engage different cognitive processes than verbal exchange, potentially leading to ideas or concepts that would not be accessible in a discussion. For example, it is not uncommon for written comments to reflect on the nature of the QED workshop, challenge questions, or facilitation team, and this can lead to improvements of execution (or even of the method itself). A secure box (or secure boxes – with one in each quadrant) is provided in QED for all such comments with the understanding that every comment is considered, incorporated, and kept secure in the final written analysis. The safe space is further reinforced by ensuring participants that physical written comments will be destroyed once the information is transcribed by the QED team analysts. In the EARTH-X QED Workshop, a total of 412 comments were received in the Magic Box.

Acknowledging Elephants

Among a targeted and carefully considered group of experts, there will be legacy challenges that create tension.⁵³ Having these called out at the beginning of the meeting by a skilled group of facilitators will accomplish three things:

1. clarification of the scope and details of the problem;
2. gauging the severity of any disparity between participants’ views and the workshop objectives in impeding the QED process; and
3. acknowledging that there are multiple viewpoints which will need to be harmonized and that consensus may or may not be achieved.

Acknowledging elephants is not done as a matter of regular practice and requires a high level of skill, knowledge of the issue-scape, and ability to rein-in discussions should they become heated. It should only be attempted when the QED team is pre-briefed on thresholds at which hard-stops dictate a transition to a new discussion phase and/or QED activity.

Story Telling

The types of experts that constitute the range of field operators to command center and support personnel bring with them a rich set of experiences, and hence stories. Telling these stories in a safe space is a critical piece of the QED method. In the EARTH-X QED Workshop, an initial story was offered by both Central Facilitators as a way to link the discussions and their content to a real-world experience. This assisted the group to further understand and relate, not only to each other, but also to the reasons behind the workshop and the information elicitation itself. The benefits of team building are well-documented in industry but have not been readily transferred to the homeland security enterprise where a “Unity of Effort” is overly generalized and difficult to tangibly construct.⁵⁴ In our experience, storytelling has been a powerful unifying force that both humanizes attendees, decreases isolation, and builds empathy. In EARTH-X, the empathy and team-building that was generated by storytelling opened several lines of communication and identified key convergence and leveraging points between operators across DHS components involved in securing the Nation’s borders.⁵⁵

Data Analysis and Cross Validation of Information

Information solicited through QED is acquired in a systematic fashion, ensuring that each phase of the method is consistent, so that data from each phase are comparable with each other and with few deviations. A consistent method across QED workshops also ensures that data from diverse topics can be cross-compared further and evaluated for overlaps and/or divergences. Types of analysis can include:

1. Rank ordered lists of elicited information using numerical normalization techniques;
2. Iteratively refined inputs using normalized scores (i.e., taking a top-5 and doing a next round based on them);
3. Dimensional frameworks produced by plotting normalized, ranked scores on multiple dimensions (see figure 2); and
4. Qualitative summarization of the remainder of the data.

Analysts can produce quantitative textual analysis by feeding all inputs and comments into open-source software such as AIDA.⁵⁶ It should be noted that there may not be enough data from a single workshop to produce statistical inference or analysis, but repeated workshops

using consistent methodologies can produce enough data to use chi-square or similar statistical methods to compare proportionate responses from workshop to workshop.

Supporting an Operator-Driven Policy Process

A key purpose of QED is to provide a way to solicit operator input more effectively, in concert with policy experts, for informing precise and effective ODP. In contrast to a conventional, top-down policy-making process (Figure 3a), an ODP leverages the QED methodology as a means for incorporating operator knowledge and opinion in the policy-making process (Figure 3b) – alongside those with policy experience. Where the need for new or updated policy via operator input (i.e., QED) is recognized, or the potential for a strategic initiative is identified, agency personnel with a strategic policy role (the policy champions) will designate a project lead or team who may in turn establish working groups. Where the potential need for a strategic initiative is identified, the process next requires a validation cycle. Traditionally, this validation step is a high-level overview of the topic, its risk environment, and potential partners, etc. As a basis for ODP, inserting a QED approach to provide input from field-level operators ensures that accurate information on the real-world environment is incorporated. The research cycle in strategy development is the primary mechanism for identifying and detailing the operational space and risk environment that the strategy is intended to address. It is an iterative process wherein the policy champions shape concise descriptions of the strategic environment using: open source and/or classified information; national, department or interagency policy statements; statutes/authorities/regulations; interagency consultation; and engagement with academia and/or think tanks. It informs the background, and guides strategic principles, partnership identification, and current efforts by partner's sections of the strategy. Where QED is used, the background statements also form the basis of the QED workshop materials, affording an opportunity for the expert operators to inform the basic substance of the strategy by influencing what would normally be a headquarters staff-level assessment process – thus validating it or adding real-world input.

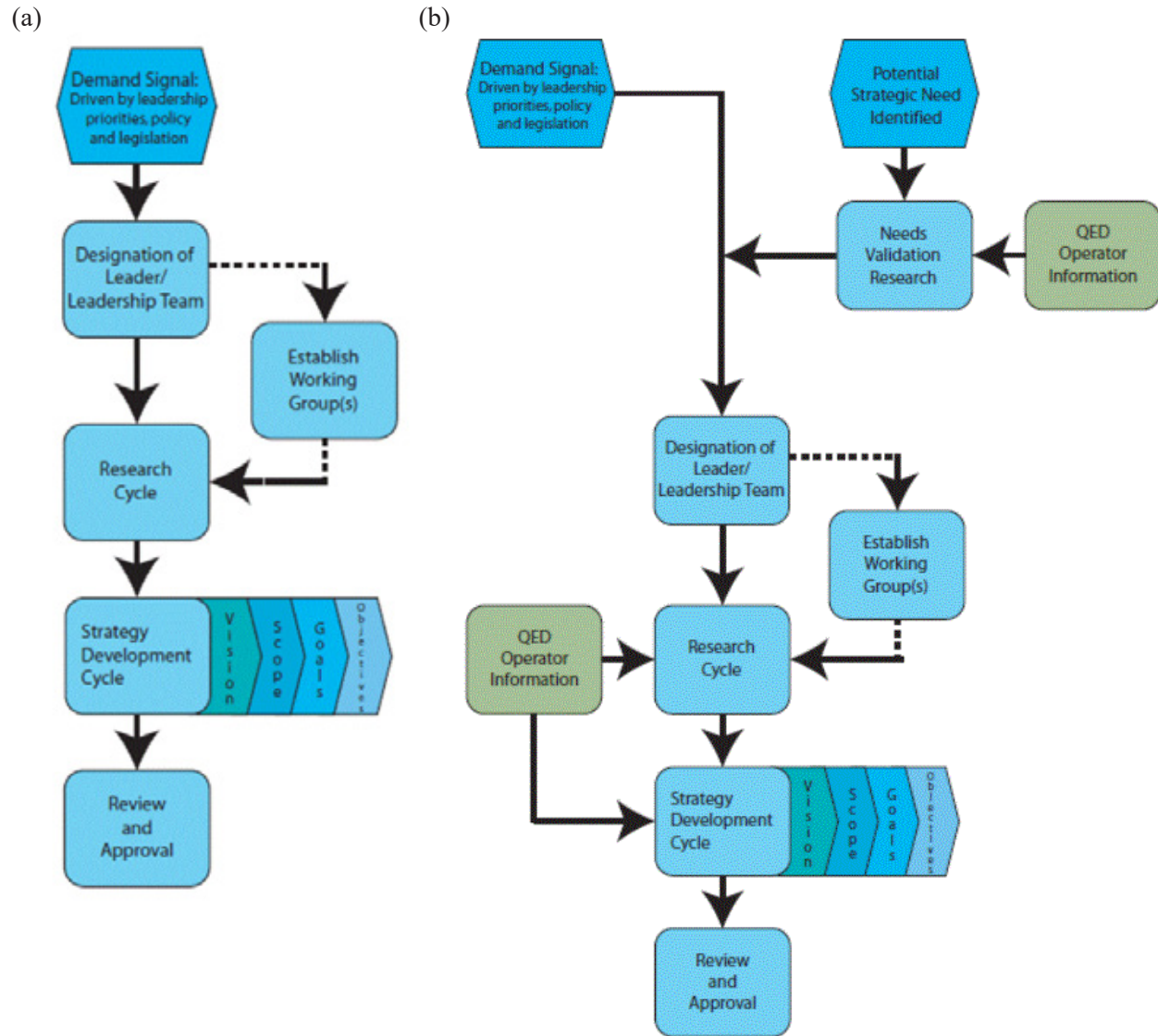


Figure 3. Diagrams of: (a) Traditional top-down policy-making process, and; (b) Policy-making process modified by the bottom-up Quadrant Enabled Delphi approach incorporating operator-driven input.

It should be noted that the application of QED does not necessarily guarantee that the operational perspectives and voices elicited through the workshops are heeded by policymakers and subsequently translated into policy. Nonetheless, the formalization of an alternative policy process (Figure 3) with QED embedded in it may increase the likelihood of ODP being developed. The gap between knowing what to do and what policy actually can be adopted is not addressed here and is beyond the scope of this article.

Conclusion

The process of policy development is optimized with timely and robust input from operators. Like any other complex system, the homeland security enterprise can be improved by addressing multiple scales of risk, needs, and practices. ODP allows field-scale challenges and opportunities to be meaningfully incorporated into strategy and planning in concert with the expertise of policy champions. This inclusion of a bottom-up policy perspective refines end-products by improving the applicability of the resultant policies as well as cooperation between components that improves Unity of Effort overall. The QED method was developed specifically to accomplish these goals in a manner that is unbiased, transparent, cost-effective, and adaptive. The establishment of a federal QED cohort of facilitators will create the means to rapidly assess demand signals and quickly develop policies that seamlessly integrate with operations on the ground, while the QED needs assessment is a valuable tool for validating the need for strategic planning. Operator Driven Policy through the QED represents an innovation in policy-making and planning while also ensuring that the U.S. government is able to grow its own capacity to respond effectively to the ever-changing global dynamics with which it must contend on a daily basis. The cost-savings and precision of progressing to this approach will ultimately benefit the American people by ensuring that the front-line operators, those who serve to keep this Nation safe, are better able to execute their missions.

About the Authors

Dr. Lilian Alessa is a Defense Intelligence Senior Leader (Intergovernmental Personnel Act) with the National Maritime Intelligence Integration Office (NMIO) and President's Professor at the University of Idaho's Center for Resilient Communities (CRC). She also serves as Deputy Chief of Global Strategies in the U. S. Department of Homeland Security Office of Policy, Washington, D.C. She received her Ph.D in cellular (systems) biology and cognitive psychology from the University of British Columbia and has worked as a maritime field operator. She has advised agencies in both Canada and the United States on designing resilient landscapes for national security and the maritime domain, emphasizing critical gaps, vulnerabilities, and approaches to addressing them. She sits on several national committees including the Science, Technology and Education Advisory Committee for the National Ecological Observing Network (NEON) through Batelle Corporation. She may be reached at lilian.alessa@hq.dhs.gov .

Sean Moon is the Chief of Global Strategies in the U. S. Department of Homeland Security Office of Policy, Washington, D.C. Among other projects in his portfolio, he is the Policy lead for Arctic strategy development. Between 2011 and 2016, he served the Department as Director, Transportation and Cargo Policy and chaired the Asia-Pacific Economic Cooperation Sub-group for Maritime Security. A 1985 graduate of Willamette University in Salem, Oregon, he spent four years in the private sector before joining the U.S. Coast Guard in 1989. Over the course of a 20-year career, he specialized in port operations and emergency management, community engagement, commercial and passenger vessel and facility safety and security programs, waterways management programs, and oil/hazardous materials and natural disaster response operations. He may be reached at sean.moon@hq.dhs.gov .

Dr. David Griffith is an Intelligence Community Postdoctoral Fellow at the Center for Resilient Communities at the University of Idaho. He received his Ph.D in Environmental Science from the University of Idaho in 2015, with specializations in plant-fungal symbiosis and social-ecological systems science. His subsequent research has focused on community-based observing and the use of indicators to anticipate socio-environmental instability and emergence regimes. Community-based observing networks and systems (CBONS) provide data that are interoperable with other observing systems so that early warning systems can be developed for social conflict, emergent environmental security threats, and transition states. He may be reached at griffith@uidaho.edu .

Dr. Andrew Kliskey is Professor of Social-ecological systems and Director of the Center for Resilient Communities (CRC) at the University of Idaho. Originally from Aotearoa / New Zealand, he trained as a land surveyor, resource planner, landscape behavioral geographer, and landscape ecologist. He has spent the last 18 years working with communities in New Zealand, northwestern and south central Alaska, and in Idaho to co-develop adaptive responses to environmental change. He has co-led several large team-based interdisciplinary research projects funded by the National Science Foundation in Southcentral Alaska, the Bering, Chukchi, and Beaufort Seas, and in the Upper Snake River Basin, Idaho. He may be reached at akliskey@uidaho.edu .

Acknowledgements

The authors are grateful to the National Science Foundation for award ARC 1642847, and to the U.S. Department of Energy and the Office of the Director of National Intelligence for an Intelligence Community Postdoctoral Research Fellowship, which supported this work. Any opinions, findings, or recommendations expressed in this report are those of the authors and do not reflect the views of NSF, DoE, or ODNI.

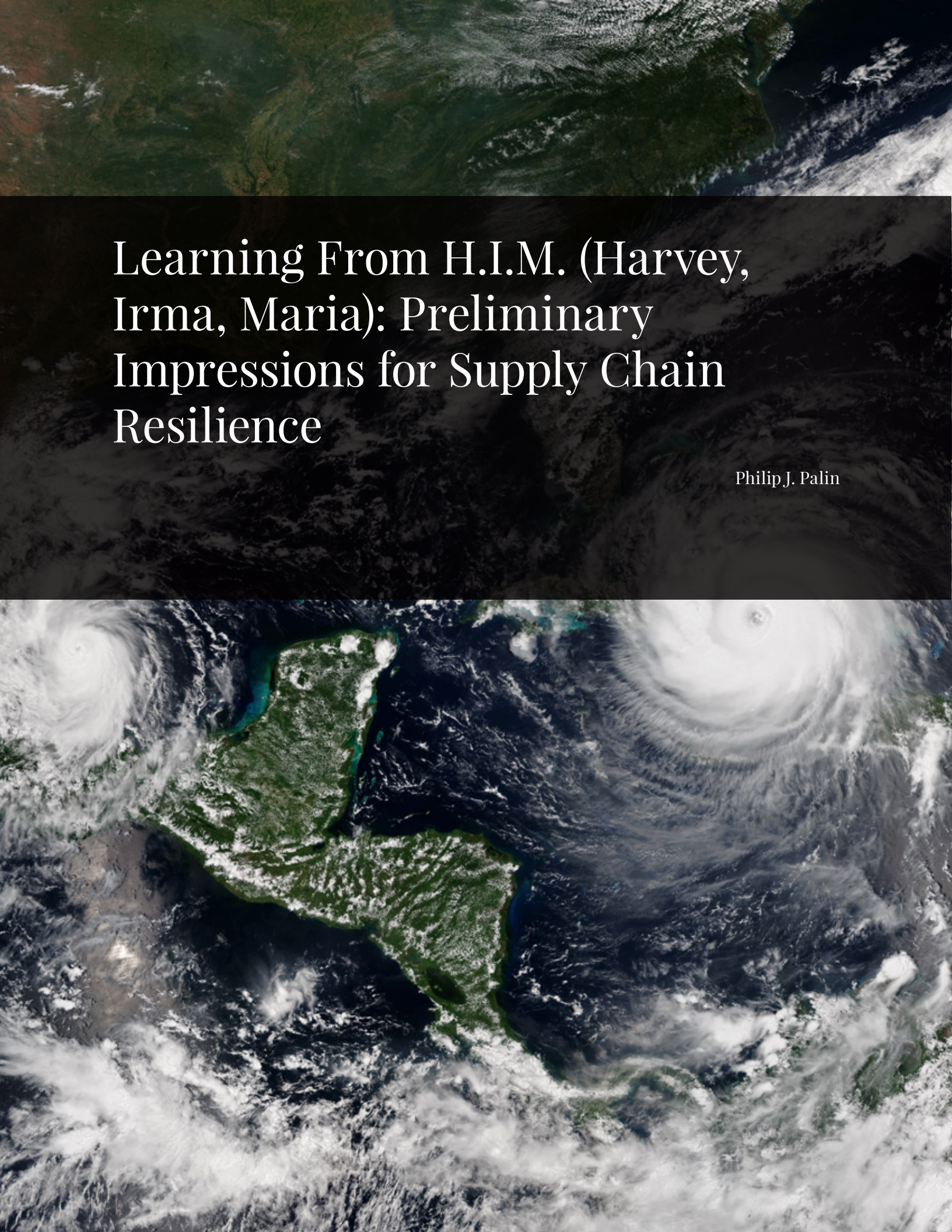
Notes

- 1 Ernest Sternberg and George Lee, "Meeting the Challenge of Facility Protection for Homeland Security," *Journal of Homeland Security and Emergency Management* 3, no. 1 (2006): <https://doi.org/10.2202/1547-7355.1153>.
- 2 Joe Garcea, "Studying Public Policy: Policy Cycles and Policy Subsystems," *Canadian Journal of Political Science* 29, no. 1 (1996): 169-170.
- 3 Martin Alperen, ed., *Foundations of Homeland Security: Law and Policy* (Hoboken, NJ: John Wiley & Sons, 2017).
- 4 U.S. Department of Homeland Security, *U.S. Department of Homeland Security Strategic Plan for Fiscal Years 2012 – 2016* (Washington, DC: Department of Homeland Security, 2012): <https://www.dhs.gov/sites/default/files/publications/DHS%20Strategic%20Plan.pdf>.
- 5 Paul Sabatier, "Top-Down and Bottom-Up Approaches to Implementation Research: A Critical Analysis and Suggested Synthesis," *Journal of Public Policy* 6, no. 1 (1986): 21-48.
- 6 President of the United States of America, "President's Letter to House and Senate Leaders and Immigration Principles and Policies," accessed October 8, 2017, <https://www.whitehouse.gov/briefings-statements/president-donald-j-trumps-letter-house-senate-leaders-immigration-principles-policies/>.
- 7 Paul Sabatier, "Top-Down and Bottom-Up Approaches to Implementation Research: A Critical Analysis and Suggested Synthesis," *Journal of Public Policy* 6, no. 1 (1986): 21-48 ; U.S. Department of Homeland Security, Office of Strategy, Policy, and Plans, "Strategy, Plans, Analysis & Risk," accessed September 7, 2017, <https://www.dhs.gov/strategy-plans-analysis-risk>.
- 8 Martin Alperen, ed., *Foundations of Homeland Security: Law and Policy* (Hoboken, NJ: John Wiley & Sons, 2017).
- 9 Ibid; Charles R. Wise, "Organizing for Homeland Security," *Public Administration Review* 62, no. 2 (2002): 131-144.
- 10 David Dunning, "The Dunning-Kruger Effect: On Being Ignorant of One's Own Ignorance," *Advances in Experimental Social Psychology* 44, (2011): 247-296.
- 11 *The Security and Accountability for Every Port Act of 2006 (SAFE Port Act)* (P.L. 109-347) §232.
- 12 *Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act)* (P.L. 110-53) §1701.
- 13 U.S. Congress, House, *Department of Homeland Security Appropriations Act, 2010*, 111th Cong., 1st sess., 2010, H. Rep. 111-298.
- 14 As well as controversial sociopolitical areas of discourse. See Harold Sackman, *Delphi Assessment: Expert Opinion, Forecasting and Group Process* (Santa Monica, CA: RAND Corporation, 1974). See also Rodney Custer, Joseph Scarcella, and Bob Stewart, "The Modified Delphi Technique - A Rotational Modification," *Journal of Vocational and Technical Education* 15, no. 2, (Spring 1999), <http://scholar.lib.vt.edu/ejournals/JVTE/v15n2/custer.html>.
- 15 Olaf Helmer, H.A. Linstone, and M. Turoff, *The Delphi Method: Techniques and Applications* (Newark, NJ: New Jersey Institute of Technology, 2002). See also Lilian Alessa et al., "The Arctic Water Resources Vulnerability Index: An Integrated Assessment Tool for Community Resilience and Vulnerability with Respect to Freshwater," *Environmental Management* 42 (2008): 523-541.
- 16 Gene Rowe and George Wright, "The Delphi Technique, A Forecasting Tool: Issues and Analysis," *International Journal of Forecasting* 15 (1999): 353-375. See also Helmer et al.
- 17 Chia-Chien Hsu and Brian A. Sandford, "The Delphi Technique: Making Sense of Consensus," *Practical Assessment, Research & Evaluation* 12, no. 10 (2007): 1-8.

- 18** Sinead Keeney, Felicity Hasson, and Hugh P. McKenna, "A Critical Review of the Delphi Technique as a Research Methodology in Nursing," *International Journal of Nursing Studies* 38, no. 2 (2001): 195-200.
- 19** Jon Landeta, "Current Validity of the Delphi Method in Social Sciences," *Technological Forecasting and Social Change* 73, no. 5 (2006): 467-482. See also Keeney *et al.*
- 20** See Dsam Scheele, "Reality Construction as a Product of Delphi Interaction," in *The Delphi Method: Techniques and Applications*, eds. Harold Linstone and Murray Turoff (Reading, MA: Addison Wesley Publishing Company, 1975), 37-71. See also Roy Schmidt *et al.*, "Identifying Software Project Risks: An International Delphi Study," *Journal of Management Information Systems* 17, no. 4 (2001): 5-36. See also Celeste Lyn Paul, "A Modified Delphi Approach to a New Card Sorting Methodology," *Journal of Usability Studies* 4, no. 1 (2008): 7-30.
- 21** For examples, see Cristiano Castelfranchi, "Modelling Social Action for AI Agents," *Artificial Intelligence* 103, no. 1-2 (1998):157-182. See also Cristiano Castelfranchi, "Engineering Social Order," in *International Workshop on Engineering Societies in the Agent's World* (Berlin: Springer, 2000): 1-18. And see Rosaria Conte *et al.*, "Sociology and Social Theory in Agent Based Social Simulation," *Computational and Mathematical Organization Theory* 7, no. 3 (2001): 183-205.
- 22** John Perry, "Indexicals, Contexts, and Unarticulated Constituents," in *Proceedings of the 1995 CSLI-Amsterdam Logic, Language, and Computation Conference*, (Stanford, Calif.: CSLI Publications, 1998).
- 23** Evan Fales, "The Ontology of Social Roles," *Philosophy of Social Sciences* 7, no. 2 (1977):139-161.
- 24** Bruce J. Biddle, *Role Theory: Expectations, Identities, and Behaviors* (New York: Academic, 2013).
- 25** Cristiano Castelfranchi, "The Theory of Social Functions: Challenges for Computational Science and Multi-agent Learning," *Cognitive Systems Research* 2, no. 1 (2001): 5-38.
- 26** Timo Steffens, "Adapting Similarity-Measures to Agent Types in Opponent- Modeling," in *Workshop on Modeling Other Agents From Observations at AAMAS* (New York: Autonomous Agents and Multiagent Systems, 2004): 125-128.
- 27** Evan Fales, "The Ontology of Social Roles," *Philosophy of Social Sciences* 7, no. 2 (1977):139-161.
- 28** David Cash *et al.*, "Scale and Cross-Scale Dynamics: Governance and Information in a Multilevel World," *Ecology and Society* 11, no. 2 (2006): 8.
- 29** Lilian Alessa and Andrew Kliskey, "The Role of Agent Types in Detecting and Responding to Environmental Change," *Human Organization* 71, no. 1 (2012): 1-10.
- 30** Martin M. Chemers, "Leadership Effectiveness: An Integrative Review," in *Blackwell Handbook of Social Psychology: Group Processes* (Malden, MA: Blackwell, 2001): 376-399. See also Jeffrey C. Johnson, James S. Bolster, and Lawrence A. Palinkas, "Social Roles and the Evolution of Networks in Isolated and Extreme Environments," *The Journal of Mathematical Sociology* 27, no. 2-3 (2003): 89-122. See also Peter G. Northouse, *Leadership Theory and Practice, 3rd ed.* (Thousand Oaks, CA: Sage Publications, 2018).
- 31** For reviews, see: Norbert Schwarz and Gerald L. Clore, "Feelings and Phenomenal Experiences," in *Social Psychology, 2nd ed.* (New York: The Guilford Press, 2013): 385-407; and Joseph P. Forgas, "Mood and Judgment: The Affect Infusion Model (AIM)," *Psychological Bulletin* 117, no. 1 (1995): 39-66.
- 32** Paula Williams *et al.*, "Community-Based Networks and Systems in the Arctic: Human Perception of Environmental Change and Instrumented Data," *Regional Environmental Change* 18 (2017): 547-559.
- 33** Nicolao Bonini and Massimo Egidi, "Cognitive Traps in Individual and Organizational Behavior: Some Empirical Evidence," *Revue D'Economie Industriale* 88, no. 1 (1999): 153-186. See also Martin Hilbert, "Toward a Synthesis of Cognitive Biases: How Noisy Information Processing Can Bias Human Decision Making," *Psychological Bulletin* 138, no. 2 (2012): 211-237.
- 34** Tom M. Mitchell, "Mining Our Reality," *Science* 326: 1644-1645.
- 35** Shrikanth Narayanan and Panayiotis G. Georgiou, "Behavioral Signal Processing: Deriving Human Behavioral Informatics from Speech and Language," *Proceedings of the IEEE* 101, no. 5 (2013): 1203-1233.
- 36** *Ibid.*

- 37** Unpublished data from CRC and Proteus, Inc. on "Technologically Induced Environmental Distancing." Contact authors for more information.
- 38** Donald Norman, *The Psychology of Everyday Things* (New York: Basic Books, 1988).
- 39** Michael Dummett, *The Logical Basis of Metaphysics* (Cambridge, MA: Harvard University Press, 1991); Bill Brewer, "Mental Causation: Compulsion by Reason." *Proceedings of the Aristotelian Society, Supplementary Volume* 64: 237-253.
- 40** Dianne C. Berry and Donald E. Broadbent, "Interactive Tasks and the Implicit Explicit Distinction," *British Journal of Psychology* 79, no. 2 (1988): 251-72.
- 41** Michael Polanyi, "Sense-Giving and Sense-Reading," *Philosophy* 42, no. 162 (1967): 301-325.
- 42** See Robert Sternberg and Joseph Horvath, *Tacit Knowledge in Professional Practice: Researcher and Practitioner Perspectives* (Mahwah, NJ: Lawrence Erlbaum Associates, Publishers, 1999). Also see Jennifer Hedlund et al., "Identifying and Assessing Tacit Knowledge: Understanding the Practical Intelligence of Military Leaders," *The Leadership Quarterly* 14, no. 2 (2003): 117-140.
- 43** Todd B. McCaffrey, "Gut Feel: Developing Intuition in Army Junior Officers," Strategy Research Project, <http://www.dtic.mil/docs/citations/ADA468976>.
- 44** Chrystostomous Mantzavinos, Douglass C. North, and Syed Shariq, "Learning, Institutions, and Economic Performance," *Perspectives on Politics* 2, no. 1 (2004): 75-84.
- 45** Lilian Alessa et al., *Report of the Emerging Arctic Security Threats Matrix (EARTH-X) for Improved Canada-United States (CANUS) Arctic Security Workshop, February 1-2, 2017* (Moscow, ID: Center for Resilient Communities, University of Idaho, 2017).
- 46** Robert Sanders, "The Pareto Principle: Its Use and Abuse," *Journal of Services Marketing* 1, no. 2 (1987): 37-40. Also, see Ralph C. Craft and Charles Leake, "The Pareto Principle in Organizational Decision Making," *Management Decision* 40, no. 8 (2002): 729-733.
- 47** The EARTH-X report and data contain sensitive security information, and are only available for Official Use.
- 48** Lilian Alessa et al., *Data Integration and Information Sharing (DIIS) Workshop, February 26-27, 2018* (Moscow, ID: Center for Resilient Communities, University of Idaho, 2018).
- 49** Ned Herrmann, "The Creative Brain," *Journal of Creative Behavior* 25, no. 4 (1991): 275-295.
- 50** Gediminas Adomavicius and Alexander Tuzhilin, "Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions," *IEEE Transactions on Knowledge and Data Engineering* 17, no. 6 (2005): 734-749.
- 51** David J. Lewis and Andrew Weigert, "Trust as a Social Reality," *Social Forces* 63, no. 4 (1985): 967-985. See also David W. Johnson, Roger T. Johnson, and Karl Smith, "The State of Cooperative Learning in Postsecondary and Professional Settings," *Educational Psychology Review* 19, no. 15 (2007).
- 52** See <https://www.chathamhouse.org/about/chatham-house-rule> for history and origins of the Chatham House Rule.
- 53** Welton Chang and Philip E. Tetlock, "Rethinking the Training of Intelligence Analysts," *Intelligence and National Security* 31, no. 6 (2016): 903-920.
- 54** Thad W. Allen, "Confronting Complexity and Creating Unity of Effort: The Leadership Challenge for Public Administrators," *Public Administration Review* 72, no. 3 (2012): 320-321.
- 55** Lilian Alessa et al., *Report of the Emerging Arctic Security Threats Matrix (EARTH-X) for Improved Canada-United States (CANUS) Arctic Security Workshop, February 1-2, 2017* (Moscow, ID: Center for Resilient Communities, University of Idaho, 2017).
- 56** Mark Altaweel, Lilian Alessa, and Andrew Kliskey, "Visualizing Situational Data: Applying Information Fusion for Detecting Social-Ecological Events," *Social Science Computer Review* 28, no. 4 (2010).

Copyright © 2018 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS). Cover image by KufoletoAntonio De Lorenzo and Marina Ventayol.

A satellite image of Earth showing a large, swirling storm system over the Atlantic Ocean. The storm has a distinct eye and is surrounded by dense, white clouds. The surrounding ocean is dark blue, and the landmasses are visible in shades of green and brown. The image is split horizontally, with the top half showing a different view of the storm and the bottom half showing a closer view of the storm's eye and surrounding clouds.

Learning From H.I.M. (Harvey, Irma, Maria): Preliminary Impressions for Supply Chain Resilience

Philip J. Palin

[The observations and analysis offered reflect the author's best judgment as of late 2017. The essay is intended to encourage more detailed research and deeper consideration.]

Abstract

The 2017 Atlantic hurricane season challenged critical infrastructure and key resources across a wide area. Harvey, Irma, and Maria each exposed different aspects of how density, dependencies, and distance impact expression of risk. Each event was dramatically different in terms of context, inputs, and outputs. But taken together this real-world stress-test of engineered systems, supply chains, and related networks offered helpful strategic insights. Survivor-facing lifelines are complex adaptive systems that tend to resist command-and-control, but are often predisposed to resilience, and can be influenced by effectively targeted choices. The author outlines several key factors that decision-makers should monitor to inform their choices.

Suggested Citation

Palin, Philip J. "Learning From H.I.M. (Harvey, Irma, Maria): Preliminary Impressions for Supply Chain Resilience." *Homeland Security Affairs* 14, Article 7 (September 2018). <https://www.hsaj.org/articles/14598>

Introduction

On August 26, 2017, Hurricane Harvey came ashore at Rockport, Texas. The next week Irma was pounding the Caribbean and targeting Florida. On September 20, Hurricane Maria barreled across Puerto Rico. This quick succession of three hard-hitting storms exposed several aspects of Supply Chain Resilience¹ (and non-resilience).

Supply Chain Resilience assumes that in advanced economies, considerable robustness and adaptability exists in the depth and overlap of diverse networks of supply and demand, such as those that characterize the eastern third of North America. Disruption – and even destruction – of network elements can be mitigated by additional resources being quickly attracted into the surviving network.²

There is, however, a risk of network fracturing and seriously delayed recovery if 1) multiple **dependencies** within the system fail, disrupting the preexisting supply and demand network, 2) demand is separated from sources of supply by significant geographical **distance**³, and 3) population **density** is beyond the capacity of "replacement" supply networks to match demand.

The consequences of Harvey, Irma, and Maria offer provocative evidence for both systemic resilience and the risk of catastrophic failure. The lessons taught by H.I.M. extend from the tactical to the doctrinal. This research highlights the following five structural issues that have potential strategic value for preparedness and response to future extreme events.

- Force on Target
- Critical Infrastructure as target
- “Super-Nodes” as target
- Population behavior (and ability to track population behavior)
- Availability of trucks, truckers, and fuel

This analysis pays particular attention to outcomes in the Houston, Miami, and San Juan metropolitan areas. Density of demand and multiple dependencies found in urban areas tend to amplify the risk of catastrophic cascades, but in all three hurricanes, non-urban areas were also seriously impacted. In Puerto Rico, the non-urban impacts have been especially troublesome and long-lasting. In many cases, rural areas are increasingly dependent on sourcing and distribution from urban areas. As a result, the five structural issues outlined are fundamental to effective preparedness, response, and recovery in both urban and rural contexts.

Houston: Rapid Recovery

The Houston Metropolitan Statistical Area has a population of 6.5 million with a density of roughly 630 persons per square mile. Houston is embedded within a very dense socio-technical-economic web. Proximity to the Dallas-Fort Worth Metropolitan Statistical Area (240 miles) and the San Antonio MSA (200 miles) creates a diverse, resource-rich matrix. The so-called Texas Triangle is a mega-region of 18 million people encompassing over 70 percent of the state’s population and an even larger share of its economy.

Harvey made landfall roughly 190 miles southwest of Houston as a strong Category 4 Hurricane. While quickly downgraded to a tropical storm, Harvey stalled over Eastern Texas for most of four days inundating the region with up to 64 inches of rain.

Over 80 Texans died. One month after the event more than 60,000 were still in temporary housing. Early estimates of financial loss ranged between \$50 billion and \$150 billion. However, there were also systems that showed remarkable resiliency. Below are three important examples of this resiliency in key systems.

- The electrical grid and natural gas networks continued to operate at more than 90 percent of capacity during the event. Only six of 230 electrical substations serving metro Houston were flooded.⁴
- Telecommunications services — including cellphone and internet connections — were widely available. Only 3.8 percent of wireless cell sites serving Houston were non-operational on August 31.⁵
- The treatment and delivery of clean water to residents of metropolitan Houston continued without significant interruption, despite serious disruption of major facilities.⁶

Given the outsize character of this extreme event, the resilience of these critical infrastructures is worth better understanding. Failure of any of these systems would have amplified negative consequences. The failure of even one of these networks can often

initiate a catastrophic cascade. Supply Chain Resilience especially examines the interplay of densities, dependencies, and distance. Inside its urban loop, Houston's population density exceeds 4700 persons per square mile. Roughly 25 percent of the nation's refining capacity is in the Houston area. These sorts of concentrations create complex dependencies and interdependencies. The destruction and disruption in Houston caused by Harvey resonated across several national—and even international—networks.⁷ From Saturday afternoon, August 26, to at least Wednesday afternoon, August 30, Houston's surface transportation network was so seriously disrupted as to be essentially impassable. For most goods – including food, pharmaceuticals, medical goods, and fuel – the supply chain stopped on Friday evening, August 25 and did not resume until Thursday, August 31. Yet by Saturday, September 2 most grocery stores were re-stocked and hospitals, clinics, and pharmacies had what they needed.

Consumer hoarding of gasoline complicated recovery of the fuel supply chain across East Texas.⁸ The production, transmission, and delivery of refined fuels continued to be seriously disrupted for weeks. But given the controlled shut-down of most refining in the region and the surge-in-demand associated with hoarding, even the fuel supply chain did better than might reasonably be expected. All in all, given how hard Harvey hit, it is an extraordinary demonstration of supply chain resilience. How did it happen? What can we learn? There were substantive – and continuing – problems, including the following.

- Close to fifty percent of regional refining — over 20 percent of national capacity — was shut down in advance of Harvey and was not yet fully operational when Maria hit Puerto Rico.
- In the days following Harvey, regional demand for refined fuels increased by multiples of 2 to 4 in many locations, presenting a significant challenge for fuel distribution and delivery.
- The loss of network integrity involving Colonial Pipeline connections west of Lake Charles seriously reduced the system's capability to supply roughly 60 percent of the gasoline consumed between Atlanta and Baltimore.
- The failure of pumping at the Beaumont city water system—serving more than 120,000 residents 80 miles east of Houston—demonstrated the potential of analogous system failures.
- Most distribution centers, fulfillment centers, and warehouses were not flooded. But many of the most important supply nodes were surrounded by flood waters making distribution impossible for nearly one week.
- The surface transportation network in metropolitan Houston was under water in so many different places that the system came to a standstill. But once the water drained, most of the network was able to immediately return to full operations.
- Trucks and trailers were more available than drivers. More of each were needed. Spot prices for trucking soared. There was a lack of outbound loads to match inbound loads.

Despite this litany of disruption, the supply chain problems caused by Harvey had transitory or modest impacts on sources of supply; most supply nodes survived, and demand – while temporarily separated from supply and sometimes relocated – remained close to the same as before the event. In the case of oil refineries and the Beaumont water pumping stations,

there were serious disruptions of current supply capability, but *capacity* survived, pending repair and restart.

A simplified abstraction of the supply chain consists of demand nodes, supply nodes, and links. In Houston, Harvey had a dramatic—but temporary—impact on links. Other supply chain elements either remained functional or quickly restarted once the flooding drained. Even in the case of the links—pipelines and road networks—the most serious disruptions were limited to a matter of days, not weeks. Further, in contrast to many similar events, freight movement was allowed to utilize the surface transportation network as it became available, accelerating supply chain adaptability and recovery.⁹

Potential Strategic Implications of Harvey

1. *Differentiating Capacity from Capability Matters.* In assessing supply and demand networks, it is helpful to differentiate between short-term disruptions of capability and longer-term destruction of capacity. Capabilities can usually be replaced more quickly and flexibly than capacity. Where more capacity persists, less investment is needed for surge and/or replacement.
2. *Which Part of a Network is Impacted Matters.* In assessing supply and demand networks, it is helpful to differentiate between effects to different elements of the supply chain, including sourcing, making/processing, distribution, delivery, and consumption. The farther “up” the chain the source of disruption or place of destruction, the more difficult to recover capacity. The higher up the impediment, the more surge and/or replacement investments are needed.
3. *Highway Infrastructure Matters a Great Deal.* Considering the consequences of Harvey for Houston, what if the disruption of the surface transportation network had involved much more destruction? What are the implications of Harvey-in-Houston for a major seismic event in California, the Pacific Northwest, or mid-Mississippi Valley?

Miami: Very Close Call

With over six million people, the Miami-Ft. Lauderdale-West Palm Beach Metropolitan Statistical Area is crowded into a roughly twenty-five-mile-wide strip between the ocean and the Everglades. In the urbanized core of the area, population densities exceed 4400 persons per square mile. In Miami’s Brickell neighborhood, densities exceed 27,000 persons per square mile. In contrast with Houston, the Miami MSA is less part of a matrix and much more an appendage extending from sources of supply concentrated around Orlando (240 miles) and Atlanta (660 miles).

On Sunday, September 10 after striking the Florida Keys as a Category 4 hurricane, Irma had a second landfall as a CAT-3 near Marco Island Florida, 100 miles west of Miami.

Over eighty people in Florida died of storm-related causes. One month after the storm, damage estimates were in the \$60 billion dollar range. Millions of people were evacuated. In the Florida Keys, roughly 25 percent of homes were destroyed.

Irma was an enormous and powerful storm that threatened to encompass the entire Florida peninsula. Many meteorologists and insurance executives have commented that if Irma's track had been even 20 miles farther east along the Gulf Coast, financial damages could easily have tripled.¹⁰ As it happened, metro-Miami was spared a direct hit. Tampa did not receive the catastrophic storm surge a slightly different track would have generated. Irma wobbled erratically from west to east to west.

She was bad, but Irma's track spared the densest concentrations of population and infrastructure. Nonetheless destruction and disruption were widespread.

- On Monday night September 11, about 62 percent of Florida's electric customers, over six million households, did not have electricity. This included every urban area in Florida except Pensacola, and even there residents were fascinated to watch Irma's winds push the water out of Pensacola Bay.¹¹
- On Tuesday morning September 12, 72 percent of cellular service in Collier County, home of Naples, was non-operational, while 42 percent of cell towers in Miami-Dade were non-operational. 7.2 million landlines across Florida were not functioning.¹²
- In Monroe County—the Florida Keys—it is estimated that 90 percent of homes sustained serious damage; the electric distribution network needed to be rebuilt, while 89 of 108 cell towers were non-operational on Tuesday morning.¹³

Given the forecast, operators of critical infrastructure were ready. An estimated 20,000 utility workers from across the nation were staged for the Florida rebuild. A nuclear power station was powered down. Fuel stocks were well above seasonal averages before the storm.

Pre-event demand surge to support the evacuation and hurricane-hoarding seriously challenged fuel and food supply chains for the entire period September 4-9. Further analysis is needed, but on Labor Day Monday, September 4, consumers with the day-off seem to have been inspired by dramatic images from Hurricane Harvey's impact on Houston and the foreboding forecast for Irma to begin a spike in demand earlier and larger than the supply network expected.

Consumers arriving in stores on Tuesday found empty shelves and the hoarding response was fully ignited. On Wednesday, September 5, there were widespread retail shortages of food, fuel, batteries, and bottled water especially in metro-Miami and in Gulf Coast urban centers as well.

There is some evidence that a Wednesday forecast for Irma to shift east eased demand on the Gulf Coast and allowed supply chain operators – with significant effort and creativity – to maintain minimally sufficient flows of supply into metro-Miami. Actual events proved this forecast to be inaccurate.

On Sunday and Monday (September 10-11), Irma slowly careened north. Given Saturday's forecast map, many supply chain operators had moved their truck fleets around and north of Jacksonville, fully fueled and loaded to begin rolling south as early as Monday afternoon. Instead Irma spent much of Monday depositing an event-total of 11 to 15 inches of rain between Jacksonville and Fort Pierce. High winds also took out power all along the I-95 corridor between Jacksonville and Miami. By Monday evening, supply chain operators were concerned they would only be able to make one massive delivery into metro-Miami late on Tuesday, but then – due to unavailability of fuel – would have to stop resupply until Thursday

or Friday depending on when power-to-pump and fuel-in-the-ground was available. Continuous resupply was considered crucial to preempt hoarding behavior, especially in metro-Miami.

On Monday night and Tuesday morning (September 11-12), power was restored to many truck stops and other locations along I-95. Key fuel supply nodes at Port of Tampa and Port Everglades were not seriously impacted by Irma. Both had significant reserves in their terminals and were able to re-start truck-rack operations by Tuesday morning. Both ports were re-opened by Tuesday afternoon and began off-loading new refined product into the system. By late Tuesday, the availability of power and fuel supported surge operations overnight and Wednesday. Most crucial supply chains were largely back to a semblance of normality by Thursday. By Friday, September 15, traffic congestion was the most often-referenced impediment to supply chain resilience.

Potential Strategic Implications of Irma

1. *Force-on-Target Matters.* Irma was huge and very powerful, but her actual trajectory happened to avoid most key nodes for critical infrastructure and supplies. (Harvey was an extraordinary event. But if flooding is kept below a certain velocity, the impact of mass is not amplified by speed.)
2. *Concentration of Supply Matters.* If the fuel capacity at Port of Tampa and/or Port Everglades had experienced long-term disruption or destruction, the post-Irma story would be very different. Similar concentration of capacity exists in many supply chains. Attention to protection, risk mitigation, and resilience of this kind of key node is fundamental. Diversification and geographic distribution are very helpful. Identification and qualification of the risk before a crisis will enhance response.
3. *Population Behavior Matters,* Hoarding was the single largest experienced threat to the Florida supply chain. The surge in pull-signals nearly overwhelmed existing supply capabilities and seriously complicated what was already a difficult transportation environment. The largely successful evacuation of several metropolitan areas reduced population risk effectively. It is worth considering whether the evacuation would have been as successful if Harvey had not so recently demonstrated potential outcomes. Will the next evacuation order benefit from what Floridians have seen transpire in Puerto Rico?

San Juan: Very Hard Hit

The entire island of Puerto Rico is smaller than the Miami-Ft. Lauderdale-West Palm Beach Metropolitan Statistical Area. The population of the U.S. Commonwealth is 3.4 million, with about 2.3 million concentrated in the San Juan metropolitan area. The density of this urban expanse is roughly 5,100 persons per square mile. Most of Puerto Rico's supplies arrive into the Port of San Juan from Port of Jacksonville, Florida (1,300 miles).

On September 20, Maria struck Puerto Rico as a high-end Category 5 hurricane. The storm encompassed the entire island with sustained winds above 60 miles per hour and gusts of

up to 118 miles per hour. In some areas, rainfall exceeded 35 inches in less than 48 hours. The death toll remains uncertain.¹⁴

The electrical grid of Puerto Rico was fragile before Maria hit. Financial problems at the electric power authority resulted in many years of delayed maintenance and other debilitating issues. The storm seriously damaged the transmission network connecting generation facilities in the south to the metro-San Juan area.¹⁵ In the three weeks following the storm, no more than 16 percent of electrical customers were reconnected to the grid and restoration one day could be followed by loss of power the next day. Lack of available funds and credit seriously constrained pre-deployment of response and recovery assets.

Given the long-time fragility and unreliability of the Puerto Rican electric grid, an extensive collection of private diesel and gasoline generators was in place. Many individual homes and commercial establishments were prepared to supply basic electrical needs (e.g. refrigeration, pumping, check-out) for several hours or up to a few days. Many hotels feature complete power plants. But this back-up capacity depends on a refueling capability that did not anticipate simultaneous island-wide demand. Even in early October 2017 it was widely acknowledged that substantive grid restoration would require at least 100 days and much longer for remote locations.¹⁶

In its September 21 Hurricane Maria Status Summary, the Federal Communications Commission reported, "Overall, 95.2% of cell sites are out of service. All counties in Puerto Rico have greater than 75% of their cell sites out of service. 48 out of the 78 counties in Puerto Rico have 100% of their cell sites out of service." Three weeks later the FCC reported, "76.1% (down from 77.6% yesterday) of the cell sites are out of service. 14 (down from 15 yesterday) out of the 78 counties in Puerto Rico have 100% of their cell sites down." The FCC estimated that by October 12, roughly 60 percent of the Puerto Rican population had access to wireless communications.¹⁷ Recovery of the wireless network was complicated both by damage to towers and by the island-wide loss of the grid.¹⁸

In the immediate aftermath of Hurricane Maria, the transportation network in Puerto Rico was seriously disrupted by debris in roadways, flooding, bridges lost, landslides, and other impediments. In most of metro-San Juan one week later, most debris had been cleared and the urban network was operational.¹⁹ But in mid-October the Commonwealth's Department of Transportation identified 27 impassable primary or secondary roads and 550 transportation impediments, including 17 damaged major bridges, needing quick repair. Outside the metro-San Juan area some of these impediments cut off neighborhoods and communities from any delivery of supplies.

In late September, several tropical storms with heavy rains exacerbated damage to infrastructure that Maria had already hit hard. Especially in the mountainous interior of Puerto Rico, landslides and flooding undid road repairs and created new impediments to surface transportation networks.²⁰

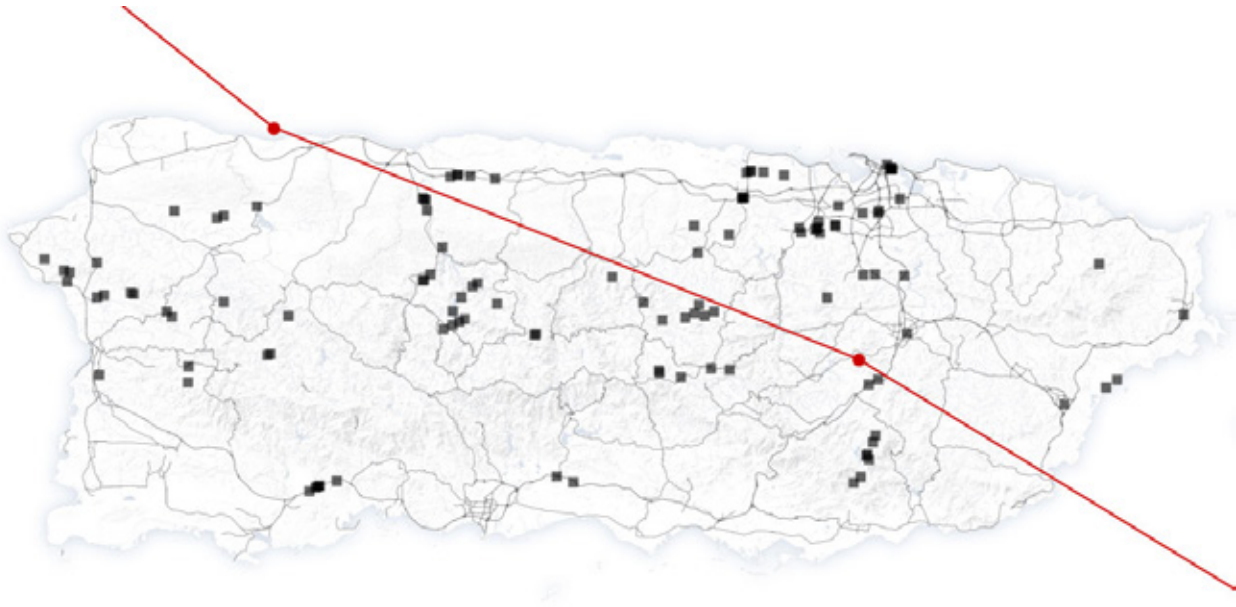


Figure 1: Major Road Impediments as of September 28 (FEMA and the New York Times). Red line is the path of Hurricane Maria's eye.

Significant disruption of these three key critical infrastructures – power, telecommunications, and the transportation network – seriously complicated the resilience of Puerto Rico's supply and demand networks. The telecommunications network's dependence on the grid made it almost impossible for consumers to express demand effectively using credit or debit or Electronic Benefit Transfer (EBT) cards.

Ninety-six percent of Puerto Ricans depend on the public water utility. The Puerto Rico Aqueduct and Sewage Authority (PRASA) operates 246 wells and 126 water treatment facilities.²¹ In the first week following landfall, roughly 45 percent of customers had water service restored largely because of either gravity feeds or existing back-up generation for pumping. Boiling tap water for drinking purposes was sometimes needed but difficult given the lack of electricity. By October 6, 55.5 percent of customers had water services restored. This addition was facilitated by repairs and new backup generation. One month after the September 20 landfall, 69.5 percent of customers were receiving water from the system (90 percent of San Juan-Metro area customers).

Because of the compromised quality of public water and the number of customers without access to the water system, demand for bottled water surged in the weeks after Maria's impact. Prior to the storm, the bottled water market in Puerto Rico was mostly supplied by local producers, especially Coca-Cola, Pepsico, and Cristalia. These local suppliers indicated that demand had doubled.²² As of October 18, FEMA alone had delivered over 23.6 million liters (6.2 million gallons) of bottled and bulk water sourced both on and off the island.²³

Prior to Hurricane Maria there were 471 supermarkets in Puerto Rico, about one for every 7500 persons.²⁴ In the first week after landfall, many grocery stores did not open. Lack of electricity and absent employees were the principal concerns. As those stores with back-up power reopened, lack of resupply became an increasing concern. Most food products arrive at the Port of San Juan via ocean-going barge, originating at the Port of Jacksonville, Florida.²⁵

Crowley, Tote, and Trailer Bridge are the principal shippers. As with the rest of the island, dock operations depended on back-up power and several cranes sustained considerable damage. But there was not significant storm surge. Containers already landed survived with their products and dock operations restarted over the first weekend after the storm.

Significant foodstocks were available on the docks and continued to be received at or above the typical flow. But during the first week after landfall, fewer trucks than usual arrived to pull containers off the dock and distribute food or other products into the retail sector. By the end of September, many grocery stores were severely low on food stocks and concerns were rising regarding how people would be fed. On September 29, the Governor of Puerto Rico announced, “[w]e have taken the initiative today to call all elements of the private sector to tell them that they must move the containers, or we are going to buy them and move them quickly and distribute them throughout Puerto Rico.” The government probably did not have the legal authority or the functional capability to do this, but this rhetoric suggests how even nine days after landfall, distribution/delivery capacity was not fully – or sufficiently – operating.²⁶

It now seems that trucking operations were delayed by several actions, none of which were originally focused on truckers or trucking per se. All are in one way or another related to retail supplies of gasoline and diesel fuel.

The widespread use of generators created a demand surge for fuel that exceeded the capability of the fuel distribution network to deliver.²⁷ Prior to Maria’s impact, the distribution network had never needed to supply the full set of private generators simultaneously. Post-event demand for diesel has been about 5 times pre-event.²⁸ Even if every pre-existing fuel tanker had been operating twenty-four hours a day, there was not sufficient capacity to meet this unprecedented demand. Transportation impediments and other complications also reduced existing delivery capabilities.

To better balance supply and demand of fuel, two measures were taken: 1) an official nighttime curfew was put in place that disallowed most retail operations but was meant to allow wholesale distribution²⁹ and 2) many fuel retailers imposed an informal quota on the purchase of fuel.

Unfortunately, the curfew was initially misunderstood as restricting all operations (and, in any case, nighttime deliveries were discouraged by lack of lights). The quota system was even more troublesome. These informal quotas were often set at \$10-to-\$15, which would not fill most trucks. The quotas resulted in consumers constantly returning to refill their cars and fuel containers for private generators, creating huge lines. Both the quotas and the resulting lines discouraged – and arguably, did not allow – many truckers to refuel. A significant number of truckers stayed home even after the ports had reopened and many roads had been cleared. Otherwise they risked being stranded out-of-fuel.

Once the sales quota on fuel for vehicles was made illegal³⁰ and the curfew was curtailed and clarified, trucks began operating at levels comparable to before September 20. Between September 30 and October 15, port operations steadily improved and were quickly at 80 percent of pre-event normal, *as well as* handling the increased through-put of arriving FEMA supplies.³¹ Once trucking operations substantively restarted – during the first week in October – most aspects of the grocery supply network in Puerto Rico restarted. One month after landfall 417 of 471 grocery outlets had reopened.

But a full month after landfall a key element of the demand network continued to be disrupted. More than 40 percent of Puerto Ricans depend on an Electronic Benefits Transfer (EBT) card to purchase most of the food they consume. The EBT card requires telecommunication capabilities that in most cases were not available in the immediate aftermath of Maria. Before September 20 about 2500 retail locations processed the Nutritional Assistance Program EBT card (also known as the Family Card or PAN card for *Programa de Asistencia Nutricional*). On October 20, only 983 or 39 percent of these retailers were open and able to conduct transactions with the PAN card. Outside the San Juan metropolitan area, the percentage of retail outlets accepting the PAN card was even smaller.

Up to 1.3 million people had their ability to express demand for food reduced by sixty-percent or more. Grocery stores that could not transact PAN payments lost that portion of their usual cash-flow. Over the same period costs increased, especially costs associated with maintaining generator power. Price freezes on several food products were legally imposed September 3 in anticipation of Hurricane Irma and were continued.³² This combination of reduced demand, increased costs, and the inability to increase prices put many grocery stores at risk of failure.

Adding to this suppression of retail grocery resilience, the Commonwealth and Federal governments launched an ambitious effort to supply all Puerto Ricans with relief supplies of water and food. On October 19, FEMA indicated it had distributed “more than 600,000 meals a day..., more than 10 million liters of bottled water, and more than 3.6 million gallons of potable bulk water.”³³ Given the inability of many PAN card holders to purchase groceries, this is obviously life-saving work. But it also reflects a loss of cash-flow that otherwise would have sped the recovery of the grocery sector in Puerto Rico (and probably competes for shipping into Puerto Rico). By October 23, 93 percent of PAN beneficiaries were making transactions with their EBT card.³⁴

Between September 20, 2018 and February 1, 2018, FEMA and its mass care partners distributed over 60 million meals in Puerto Rico. While an enormous and helpful gap-filling service, this represented roughly four to six percent of total calories consumed. Survivors of Maria continued to be fed – primarily – by the preexisting grocery supply chain operating under profound operational and financial duress.³⁵

Potential Strategic Implications of Maria

1. *Preexisting network dependencies and interdependencies matter.* Prior to Maria, the Puerto Rican electrical grid was unreliable, as a result a large and widely-distributed set of private electrical generation capability was already in place. The preexisting water system was fragmented and inefficient; after the event, this negative arguably became a positive. The interface between the port and on-island distribution hubs was complicated and recovery was delayed by heretofore “hidden” network elements.
2. *Distance and other impediments to the flow of re-supply matter.* Perhaps the most serious and longest-lasting challenge to many supply chains was reestablishment of a predictable – and accurately demand-reflecting – flow of supply. The “pipeline” from Port of Jacksonville to Port of San Juan surged, but given the wide array of disruptions, this surge often reflected wild guesses related to actual demand causing a long-term bullwhip effect across many supply chains.

3. *Persistence of pre-existing supply and demand networks matters.* The grid was down. Telecommunications was spotty or non-existent. It required several weeks for fuel distribution to reach an equilibrium with demand, but – somehow – within two weeks the grocery network was mostly operational. Especially important was the ability of consumers to express demand – using both cash and non-cash financial signals. If this had not happened, the crisis would have been significantly amplified.

Preliminary Impressions Related To Systemic Outcomes

The complexity of Harvey, Irma, and Maria cannot be captured in ten pages. But this outline may point to opportunities for more detailed study and analysis, especially related to the network effects of supply and demand in these three crises. When the focus of attention is narrowed to Houston, Miami, and San Juan, these were three very different events. But substantial coherence can be found in how supply and demand networks behaved. This analysis has produced three high-level – mostly unsurprising – take-aways.

1. Where and when the grid persists, resilience tends to abide. The greater the scope of grid failure (both in terms of time and space), the greater the challenge to Supply Chain Resilience.
2. Especially if there has been grid failure, the survival and continued operation of “super-nodes” within supply networks becomes even more important (examples of super-nodes include: water treatment and pumping facilities, fuel storage and distribution facilities, docks and other especially large network junctions such as distribution centers).
3. Even when system capacity has survived an extreme event, the continued *capability* of the road network, fuel network, trucks and truckers become especially important for supply capacity to be meaningfully deployed into demand.

There are also some emerging lessons-learned related to how demand is expressed (or the implications when demand *cannot* be effectively expressed). These outcomes are more complicated than what can be captured in one or two sentences and are given more attention below.

In considering systemic outcomes, it is worth noting that preexisting systems in Texas, Florida, and Puerto Rico – all in densely populated areas featuring vast interdependencies – are mostly *not* the product of systematic planning and design. These complex realities emerge incrementally over-time, usually from the accumulation of individual decisions that are, from a systems perspective, random. The interdependent “structures” described below have, for the most part, not been carefully designed to achieve Supply Chain Resilience. Rather, they have emerged through trial, error, and learning specific to time, place, and thousands of sometimes contradictory purposes. Reflecting these preconditions, one set of structures is differentiated from others and more or less resilient to particular threats. But as a system this is much less the outcome of human intention than the flux of a complex adaptive system interacting with its environment.³⁶

Force on Target

The force that hit Houston was heavy but comparatively slow. Miami itself received a glancing blow. What hit San Juan was heavy and fast. In each case, targets included the electrical grid, telecommunications, road networks, and much more. Recognizing these force differentials can be crucial to framing an appropriate response strategy.

In classical physics, force is equal to mass multiplied by acceleration. Measuring hurricanes – and potentially other extreme events – by terajoules or by geographic scope (not quite mass, but indicative) *and* speed (wind, seismic waves, blast effects, etc.) can offer a helpful way to more clearly contrast events.³⁷ When Harvey made landfall at Rockport it was measured at 28 terajoules, then dramatically lost speed, becoming almost stationary over Houston to Beaumont, and dropping 30 to 60 inches of rain. When Irma made landfall on the Gulf Coast of Florida, it was measured at 100 terajoules, quickly lost considerable speed over less populated central Florida, and kept moving north where it briefly dropped Harvey-like rainfall totals on Northeast Florida. When Maria made landfall at Yabucoa, it was the strongest hurricane to hit Puerto Rico since 1928. Sustained winds were measured at up to 155 miles per hour; wind gusts of more than 110 miles per hour encompassed the entire island for over thirty hours, and rain fell about one-inch per hour in many locations. Observations were not as precise for Maria (National Weather Service radar was lost in the hurricane), but a rough measure of up to 116 terajoules at landfall in Puerto Rico has been suggested.³⁸

In each of these three extreme events, the force expended by the hurricane was very significant at specific points in time and space. But only in one case did the event's full force encompass essentially the entire network supporting a population of 3.4 million people.

For over three days, flooding in Houston largely eliminated the road network. Harvey's force threatened similar disruption to the local water network, which just barely survived. But electrical and telecom networks continued to operate and the extended regional – even continental – networks for these critical infrastructures and most key supply chains were not seriously impacted by Harvey. Once the flood waters drained, these surrounding networks "flooded" Houston with resources, some desperately needed and others not so much.³⁹

Miami may have been within 12-to-18 hours of not being resupplied in the aftermath of Irma. But the capability gaps opened by grid and fuel disruption were filled in time by resources comparatively close at hand. While Miami may be more a dense network appendage than a connecting node, there are robust connections to truly dense nodes at Orlando and Jacksonville and Atlanta.

The island of Puerto Rico is a very different target because it is a very different network. Where Houston is deeply embedded in a network of networks, San Juan is the dense node in a fairly thin and largely separate network. Miami is 236 miles by truck from Orlando; San Juan is 1300 miles by sea from Jacksonville. Harvey and Irma seriously disrupted pieces of very large interdependent networks. On Puerto Rico, Maria disrupted, and sometimes destroyed, much of an isolated network. The distance of San Juan's network from similar networks, combined with the density of population depending on the network, significantly increased the risk of catastrophic consequences. Less than 50 miles separate the San Juan docks from survivors in the mountains, but access was often treacherous.

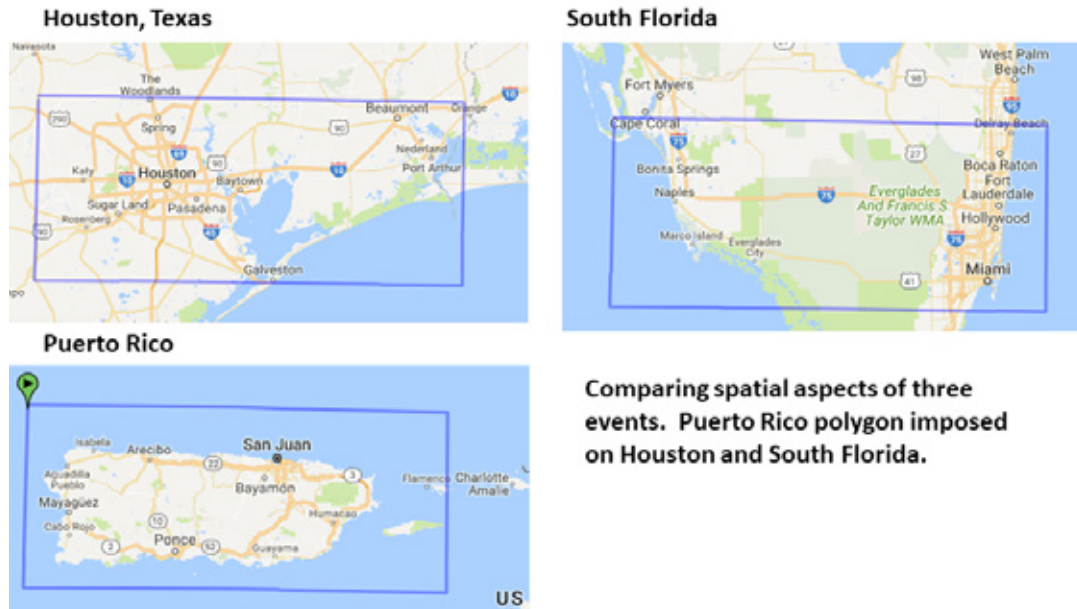


Figure 2: Spatial comparison of the three events

If the force of Hurricane Maria had hit similar targets in Houston or Miami or Tampa, certainly the preconditions in each of these places would have produced different results. It is also true that Maria hit San Juan with roughly 4-times the energy as Harvey-at-Landfall. The differential was even greater by the time Harvey was over Houston. Regardless of preconditions, when this kind of force hits any dense urban area with its web of interdependencies, the outcomes will be ugly.

Critical Infrastructure as Target

The US Department of Homeland Security identifies sixteen critical infrastructures.⁴⁰ In thinking about Supply Chain Resilience, it can be helpful to differentiate between “content-agnostic” infrastructures and “content-committed” supply chains. Both can be understood as infrastructure – meaning underlying (sometimes hidden) structures on which achieving purposes depends – but some infrastructure is committed to specific purposes while other infrastructure facilitates multiple purposes.

Given this framework, electrical power, telecommunications, and road systems are content-agnostic, facilitating the movement of many kinds of content. Water and fuel systems are content-committed. The food network is content-committed but ecumenical. The same functionalities that move food may also move bottled water and cleaning supplies and, sometimes, bags of charcoal, paper products, baby diapers, and much more. The pharmaceutical supply chain, in contrast, is much more parochial even when it is delivering to a grocery store. Medical goods distributors are nearly as ecumenical as food supply chains. More attention is given below to trucking (is it content-committed or content-agnostic?).

In all three extreme events, these networks were threatened. In the case of Harvey-in-Houston, while the grid and telecommunications largely persisted, actual movement of goods was temporarily halted by the road network being flooded. In Florida, power outages

meant truck stops could not pump fuel, threatening supplies of bottled water and groceries, but continued persistence of telecommunications allowed this problem to be identified, prioritized, and solved in the nick of time.⁴¹

The quick recovery of supply chains in Houston was allowed by sufficient robustness – resistance to change – embedded in the design and construction of the urban highway network. The effective response in Florida was enabled by significant investment in the robustness of the electrical transmission network.⁴² This prior investment in mitigation allowed for more timely attention to specific distribution problems, such as reconnecting power to truck-stops on I-95. In either case, would these networks have been as effective resisting four-times the force-on-target? What about eight-times force-on-target?

In Puerto Rico, the electrical grid was not robust.⁴³ The long-term failure of the grid disrupted fuel distribution, delayed full recovery of telecommunications, and complicated use of EBT cards at grocery stores, among many more troubles. Without a reliable fuel network, pushing supplies became much more difficult. Without the ability to use EBT (and other) cards, demand-pull was seriously muted and thereby reduced. But despite long-term problems with content-agnostic infrastructures, even in Puerto Rico, content-committed infrastructures – especially supply chains – were able to demonstrate considerable resilience. For example, five weeks after Hurricane Maria's hard-hit on all of Puerto Rico, less than 30 percent of the electrical grid had been restored and only 42 percent of cell sites were functional. But 80 percent of water customers were being served; over 80 percent of gas stations were operating; 90 percent of grocery stores were open, and most were accepting EBT, debit and credit cards for transactions.⁴⁴

Given the failure of the Puerto Rican electrical grid, the resilience of the Puerto Rican water system might surprise many water-system operators. But the design – perhaps more accurately, the non-design – of the Puerto Rican water system is key to this advantage. Unlike many urban systems, the Puerto Rican water network depends on many sources – 246 wells and 126 water treatment facilities – nearly half of which allow for gravity distribution and require sufficiently modest pumping operations that can be supplied by commercial off-the-shelf back-up generation. The lack of a centralized source and the diversity of system components continued to operate in the way many contemporary (and more efficient) water-systems would not.

A tantalizing implication emerging from Harvey, Irma, and Maria is that content-agnostic infrastructures especially benefit from robust engineered systems that minimize the risk of disruption, while content-committed infrastructures benefit more from diversity, adaptability, and – in a word – resilience. If this impression is confirmed with more rigorous analysis, it could have significant impacts on mitigation measures and response strategy.⁴⁵

“Super-Nodes” as target

Over time large networks tend to be characterized by increasing concentration or what is sometimes called network centrality. The greater a network’s centrality, typically the more efficient the network’s flow. Li et al. note,

[i]n modern society, lives depend more and more on infrastructure networks, such as the power grid, Internet, transportation networks and the financial networks, and so forth. The overall efficiency of these network systems is being increased, while the internal connections and the dynamical characteristics within the networks are becoming more close and complex. These behaviours make the networks more vulnerable and increase the possibility of system crash.⁴⁶

In the case of Harvey, Irma, and Maria it was possible to observe this vulnerability playing out in real time and space. In both Houston and Miami, the risk of a cascading failure often seemed imminent, yet was mostly avoided. In the case of San Juan, a cascading failure was experienced. But even in San Juan – and in Miami and Houston – the persistence and resilience of key “super-nodes” kept the human consequences from being much worse.

Under Harvey’s sustained impact, at least three super-nodes in the Houston metropolitan region experienced considerable duress. Nearly forty percent of Gulf Coast refining capacity—or about twenty percent of national capacity—was shut-down in advance of the hurricane. Even three weeks later, as Irma threatened Florida, only about half of this capacity had been reclaimed.⁴⁷

The ability to distribute refined product was also diminished when Colonial Pipeline experienced a loss of network integrity because of the unprecedented flooding. According to the Energy Information Administration,

Colonial connects 29 refineries and 267 distribution terminals and carries up to 2.5 million b/d of gasoline, diesel, and jet fuel from Houston to as far north as New York Harbor. Colonial typically operates at or near full capacity, but as a result of Hurricane Harvey and the decreased supply of petroleum products available to ship, Colonial Pipeline briefly curtailed operations and shipped products intermittently before resuming operations at reduced rates of flow on September 6.⁴⁸

A 2012 study of Houston’s infrastructure by the American Society of Civil Engineers gave the water system a passing Grade of C for resilience. The ASCE authors noted, “[s]hould a natural disaster occur, the current systems have made provisions after Hurricane Ike to back up water facilities with generators to maintain water supply to residents.”⁴⁹ Harvey, however, was a disaster that exceeded any design target. According to several reports, at least one of the principal water treatment facilities was “within hours” of shutting down and much of its equipment was operating under water.⁵⁰ In nearby Beaumont, the water system serving 120,000 persons lost both its primary and secondary pumping stations to flooding.⁵¹ After about 48 hours the system was partially restored with extraordinary measures.⁵²

As Irma churned up Florida’s Gulf Coast, many eyes were on the Port of Tampa and especially the Kinder-Morgan Fuel Terminal and associated Central Florida Pipeline.⁵³ This is, essentially, a single point of failure for the fuel network serving the Tampa-Clearwater-

St. Petersburg and Orlando metropolitan areas. Early weather forecasts suggested the possibility of destructive storm surge. It did not happen. The Port of Tampa, including Kinder-Morgan, experienced very little disruption. But some pointed out this was mostly just a random case of “meteorological luck.”⁵⁴ It could easily have been much worse. In 2016 the risk assessment firm Core Logic estimated that storm surge comparable to that produced by Hurricane Katrina would flood over 450,000 homes and cause over \$80 billion in damages in Tampa alone.⁵⁵ Irma did not hit this target with its greatest force. The fuel terminals at Port Everglades north of Miami are as crucial to South Florida as Kinder-Morgan is to Central Florida. Similar risks apply to both super-nodes.

Puerto Rico sources the vast majority of groceries, pharmaceuticals, medical goods, and fuel products from off the island. Eighty-four percent of all in-bound shipments move through the Port of San Juan.⁵⁶ Maria moved across the island on September 20-21. The Coast Guard reopened the Port of San Juan on Saturday, September 23.⁵⁷ Supplies were being unloaded that same day. Despite early worries otherwise, there has always been sufficient water, food, and fuel in Puerto Rico to meet demand. It has not always been possible to distribute and deliver supplies when and where needed, but the resources have been available. The quick recovery of the Port of San Juan allowed for sustained replenishment of supplies. This is despite loss of electricity and other severe complications resulting from Hurricane Maria. A very tough story would have been even more difficult if the Port of San Juan had been lost.

There are other super-nodes related to each of these extreme events. The previous are only a few examples of a suggested type, and in the case of H.I.M. are perceived as “near-misses.”

In each of these examples, loss of a super-node can have an amplified effect across several networks by reducing the fundamental capacity of the system. To a greater or lesser degree, recognizing a super-node acknowledges there are network junctions where otherwise distinct content-movements are deeply interconnected. Nine weeks after Harvey hit Houston, fuel prices in Puerto Rico were roughly 16 cents per gallon higher because of the slow recovery of Gulf Coast refineries.⁵⁸ Sustained loss of the Port of San Juan or the Port of Tampa or the Port of Jacksonville would have had cascading effects across any supply chain depending on fuel for distribution or delivery, which is to say all of them. In the case of the Port of San Juan, the fundamental capacity to receive almost any product – food, pharmaceuticals, fuel – would have been seriously reduced without recovery of the port. Replacement of this huge share of capacity, at least for a system as densely populated as Puerto Rico, seems very unlikely. The super-node either survives or the population does not.

Ted Lewis has observed,

[c]omplex networks evolve over time and tend to transform (re-wire) themselves, evolving from random interconnections to structured interconnections that increase the likelihood of cascade failures. In general, the transformation increases the overall number of links (percolation), the number of links connecting a favored node (hub), and the number of paths running through a favored node or link (betweenness). As a consequence, the number of nodes impacted by a failure in one node is magnified by percolation, hub size, and betweenness size. As these networks evolve, they increase the self-organized criticality of the network itself, which increases its overall risk of cascade failure – both the likelihood and size of the collapse in terms of affected nodes and links.⁵⁹

Harvey, Irma, and Maria each – in a different way – point to the value of pre-identifying these crucial nodes and links.

Population Behavior

Contemporary supply chains depend on receiving accurate – and reasonably coherent – expressions of demand. These are sometimes called “pull-signals” inasmuch as supply is pulled toward the sources of demand. For most major U.S. retailers and their distributors, demand is algorithmically monitored at the point-of-sale and orders reflect near real-time shifts in inventory.

The prospect of extreme events – such as blizzards and hurricanes – generates historically predictable permutations in pull-signals. In advance of hurricane season, extra stocks of bottled water, batteries and other emergency supplies are pre-deployed to distribution centers in anticipation of demand spikes. But as was seen in Houston, Miami, and San Juan, at certain volumes a demand surge will always “break” the supply chain. This happens most often when distribution capabilities are not able to match an initial wave of demand. When consumers see empty shelves or other signals that suggest supply is uncertain, this often prompts a category-bursting feeding frenzy. Actual shortage of supply is a much rarer event.

In the aftermath of Harvey, there was considerable gasoline hoarding in a wide area of East Texas. Given the uncertainty associated with refineries coming back online, the behavior was predictable. It was nonetheless troublesome and it deepened what was a slight diminution of actual supply. Writing in *Forbes*, Michael Lynch explains,

[c]onsumers fearing gasoline shortages rush to fill up their tanks. That, in turn, creates gasoline lines and removes millions of barrels of gasoline from retail storage (gas stations) to consumer storage (vehicle tanks). This can overwhelm the retail sector's ability to replenish inventories as well as cope with the surge in customers.⁶⁰

There are only so many fuel tankers and the miles between tank farms and gas stations remain the same. A refueling route entirely sufficient for 1x demand will never be sufficient for 2x or more. A huge spike in demand will cause individual retail locations to run-out between deliveries and reinforce the sense of uncertainty that motivates the hoarding.⁶¹

The dramatic events of Harvey-in-Houston clearly influenced the behavior of Floridians when two weeks later Irma was forecast to hit even harder. The entire week prior to Irma's landfall was a battle of distributors trying (and mostly failing) to meet sharp increases in demand for almost everything on a grocery shelf. Because of Labor Day Monday, demand may have peaked earlier than usual, putting the supply chain behind from the beginning. But the tsunami of demand was also the result of Irma's size and projected power. Only two days before landfall there were entirely credible forecasts⁶² that suggested an impending statewide catastrophe. Some grocery distributors told their retail clients to “turn off your computers,” otherwise inventory algorithms would anticipate the continuation of indiscriminate hoarding behavior and overwhelm the network. Stores were told to place manual orders for essentials.⁶³

The increased demand for fuel in Florida was less a matter of uncertainty and hoarding than the result of millions of Floridians simultaneously driving north to escape Irma. Similarly, in

Puerto Rico there was a fundamental uptick in demand for diesel fuel. As noted above, the fuel needed to energize the sudden and simultaneous use of private back-up generators was probably 500 percent of pre-hurricane demand. This sort of sustained spike in demand would overwhelm most supply chains, and certainly an isolated network serving an island.

Puerto Rico's seeming demand-shift for food was less dramatic, yet if anything, more treacherous. Need for food did not decline. But forty percent of the population could not express demand when they could not use their PAN EBT cards. These pull-signals suddenly disappeared along with dial tones and cell sites. What could the algorithms or store managers (or emergency managers) do with this silence?

The contemporary supply chain has been organized to reflect population behavior. Sudden changes in population behavior can complicate – even confuse – supply chains. In the case of Harvey, Irma, and Maria, however, the dramatic shifts in pull-signals were all “predictable surprises.”⁶⁴

We know when, where, and how demand is expressed. We know how these expressions pull supply. We know how demand is influenced by uncertainty. We can know (even if we do not always know) how extreme events physically disrupt supply and demand networks. We have an increasing understanding of how these disruptions influence population perceptions. Depending on the operational context, we have several options for mitigating the perception of uncertainty and overcoming the physical challenges to effective operation of post-disaster supply and demand networks. In Harvey, Irma, and Maria, supply chain owners and operators and others interested in supply chain resilience were often surprised by population behavior. It is possible to be less surprised.

Availability of Trucks, Truckers, and Fuel

In each of these extreme events, the delivery of groceries, pharmaceuticals, medical supplies, fuel, bottled water, and much more usually depended on someone driving a truck. This is often referenced as the *last-mile problem*.

For Houston it was the problem of trucks from San Antonio (200 miles) and Dallas (240 miles) being able to deliver. In the crucial 48 hours after Irma's passing, the 350 miles between Jacksonville and Miami was where lack of fuel almost stopped the Northern Fleet from delivering into Southern Florida. For nearly a week after Maria, many were complaining that truckers had not returned to work in Puerto Rico. But what some seemed to suggest was a character problem, has since seemed more likely a problem with fuel, demand expression, storage capacity, port-accessibility, and other impediments that could have been more effectively addressed if recognized earlier in the process.

Resilience is often the outcome of self-organization and adaptability.⁶⁵ Truckers and trucks depend on engineered systems. Highways must survive and be passable. Re-fueling must be possible. The operational requirements of these engineered systems require considerable robustness – resistance to change. In earthquake country, highways should sway a bit. Fuel pipelines should feature some flexible joints. But mostly, we want these infrastructures to be conserved to facilitate the creativity of truck-drivers to find what has survived, where there is (potentially unexpressed) demand, and how to get stuff from where it is to where it is needed.⁶⁶

If Houston, Miami, and San Juan are good case studies, truckers are premier agents of resilience.

The closer a piece in the network gets to trucks and truckers, the more resilient it needs to be to optimize their resilience. Truck stops – preexisting or post-hoc – are key to “re-fueling” both trucks and truckers. In Florida the feeding and other biological requirements of truckers were seriously complicated by over-crowding of truck-stops during the evacuation and loss of power in the aftermath.

It is, however, possible to over-estimate the flexibility of truckers and trucks. This retrieves the issue raised above related to content-agnostic or content-committed infrastructures. To those outside looking in, trucks can seem content-agnostic (like the grid), the same trailer *can* carry groceries or many pharmaceuticals or medical goods or waste paper or a wide range of products.

But most trucks and trailers and their drivers spend most of their time content-committed. It might be a different trailer, but the same truck and usually the same driver makes the same recurring run to a certain set of delivery locations. This commitment enhances creativity in case of disaster. Truckers know their local context well-enough to adapt to sudden changes.

But a freezer unit is bad for fresh produce. A flatbed is non-optimal for fresh seafood. A 53-foot trailer is not well-suited for the narrow streets of Old San Juan. Not every truck has a contract or security clearance to pick-up at the port. A dry van will never deliver bulk fuel. In desperation, some in Puerto Rico were trying to convert trucks that vacuum out septic tanks to deliver diesel fuel. This unlikely attempt at re-use may demonstrate both the adaptability and the content-commitment of trucking. There is a predisposition to resilience, but trucking is much more content-committed (like a water system) than content agnostic (like the grid).

The potential capacity for post-disaster response would be significantly enhanced if there were a way for trucks to become more content-agnostic. There were lots of trucks available in Puerto Rico the first week after Maria. But most of them do not call regularly at the Port of San Juan, and most are not usually involved in delivering groceries or water and certainly not relief goods. In any case, most of them could not get the fuel they needed to deliver anything.

Given the essential role of trucks, truckers, and fuel to serving survivors of a catastrophic event, how well are these network-players understood? Can some of these predictable issues be engaged in advance? How can the resilience – adaptability and self-organization – of these diverse agents-of-resilience best be enhanced?

Slouching toward Catastrophe?

Texas is not Florida, and neither of them are Puerto Rico. Harvey, Irma, and Maria were each very different beasts. Yet all three were hurricanes. All impacted dense urban areas and much less populated exurban stretches. There were several entirely comparable network effects.

The Monday, August 28 front page of USA Today declared Harvey-in-Houston a catastrophe. The same designation has been used for the Florida Keys and most – if not all – of Puerto Rico. In each place the consequences continued to unfold weeks after the precipitating event.

Is it meaningful to label each a catastrophe?

In Houston, local language tends toward “back to business.” In the Keys, “resilience” may be a bit more common. In Puerto Rico, there are many references to “nueva normalidad” (new normal). Do these point to meaningful distinctions? If so, do the comparable network effects help explain the language differences? Which network connections, dependencies, and interdependencies held? Which ones failed? Which network elements persisted despite failures all around the and why?

When things fall apart, can we show how? When darkness drops again, can we better understand how to reclaim the light? Can we help the center hold? And if the center implodes, is there a better way to pick up the pieces?

About the Author

Philip J. Palin is the principal investigator for Supply Chain Resilience at the not-for-profit Institute for Public Research of the CNA Corporation. He serves as staff consultant on Supply Chain Resilience with the Program on Risk, Resilience and Extreme Events of the National Academies of Sciences, Engineering, and Medicine. Mr. Palin is the subject-matter-expert supporting the FEMA-National Integration Center Technical Assistance Program on Supply Chain Resilience.

Notes

- 1 For the purposes of this discussion, the supply chain is the socio-technical network by which demand is identified, targeted, and fulfilled. It is the process of deciding what, when, how, and how much is to be moved where. Supply Chain Resilience is the theory and practice of enhancing the ability of the supply chain to recover from or adapt to major disruptions.
- 2 Philip J. Palin, *The Role of Groceries in Response to Catastrophes*, CNA Institute for Public Research, 2017.
- 3 Distance and access are closely related. Short-distances that are made inaccessible can produce network and human consequences similar to the complications and delays innate to great distances.
- 4 ABC13 News, 96 percent of Centerpoint Customers have Power, August 29, 2017.
- 5 Federal Communications Commission, FCC Status Report, August 31, 2017.
- 6 CBS News, Harvey Floods Left Houston Water Plant Hours Away from Failure, September 5, 2017.
- 7 Platts, Oil Prices Soar on Harvey-Related Outages, August 31, 2017.
- 8 J.P. Lawrence, "Hoarders Blamed for Aggravating Run on Fuel," *San Antonio Express-News*, September 3, 2017.
- 9 Truckers widely reported the absence of all but the most essential security perimeters in the aftermath of Harvey. More extensive perimeters were considered, but there were higher priority claims on public safety personnel.
- 10 Amy O'Connor, "Florida's Hurricane Irma Recovery: The Cost, The Challenges, The Lessons," *The Insurance Journal*, November 30, 2017.
- 11 Energy Information Administration, Irma Cut Power to Nearly Two-Thirds of Florida's Electricity Customers, September 20, 2017.
- 12 Federal Communications Commission, FCC Status Report, September 12, 2017.
- 13 Alex Harris, Florida Keys Live Blog, *Miami Herald*, several posts September 11 to 19, 2017.
- 14 Fatalities related to Hurricane Maria's impact on Puerto Rico range from a low below 100 to more than 1200. In February, 2018 the Government of Puerto Rico commissioned an independent study of fatalities by George Washington University, see: "Puerto Rico Deaths Related to Hurricane Maria Continued for Months," *LA Times*, February 28, 2018.
- 15 Laura Quintero, "Repairing Damaged Towers Connecting Metro Area," *El Vocero*, October 23, 2017.
- 16 These preliminary impressions were submitted to *Homeland Security Affairs* on December 14, 2017. Following peer review and edits, the final draft was completed on March 4, 2018. On Thursday, March 1 most of metropolitan San Juan experienced another in a series of extended black outs and several communities in the mountainous interior have remained off the grid since September 20.
- 17 Federal Communications Commission, FCC Status Report for Areas Impacted by Hurricane Maria, October 12, 2017.
- 18 *El Nuevo Dia*, "Falta de Electricidad Pone en Peligro Servicios de Telefonía et Internet," October 18, 2017.
- 19 At least three long-term transportation impediments continue to complicate traffic in the San Juan Region: the intersection of PR 165 and PR2, PR-177 at Ave. Lomas Verdes, and PR-176 at Ave. Victor M. Labiosa.
- 20 Laura Quintero, "Aumentan Derrumbes de Tierra Colapsos de Puentes," *El Vocero*, October 19, 2017.
- 21 Wanda L. Molina-Rivera, US Geological Survey, Estimated Water Use in Puerto Rico, 2014.
- 22 Marian Diaz, "Demand Triples After the Passage of Maria," *El Nuevo Dia*, October 23, 2017.

- 23** John D. Sutter, About One Million Americans without Running Water, *CNN*, October 18, 2017.
- 24** The U.S. average is over 8800 persons per supermarket. Between 2000 and 2016, the population of Puerto Rico fell by about 400,000 or 10 percent. News reports suggest at least 200,000 Puerto Ricans have relocated since September 20, 2017. Consolidation of the grocery retail sector is likely in 2018.
- 25** Will Robinson, "Puerto Rico Devastated by Maria, Looks to Jacksonville Businesses for Help," *Jacksonville Business Journal*, September 21, 2013.
- 26** Paola Arroyo Guzman, "Government to Buy Stranded Containers in Ports," *El Vocero*, September 29, 2017.
- 27** To underline an important distinction: the fuel *capacity* available on the island was greater than the distribution capacity. There was never a shortage of fuel available to be distributed. But the distribution capacity – and the *delivery capability* – of the fuel system was not sufficient to meet a sudden and substantial increase in demand. In contrast there was a preexisting and surviving capacity to distribute and deliver non-fuel products. The capability to express this non-fuel capacity was constrained by the impediments noted above.
- 28** Marian Diaz, "Puerto Rico Fuel Market Transformed," *El Nuevo Dia*, October 25, 2017.
- 29** Some sources claim that wholesalers were initially excluded from curfew operations and the eventual inclusion and claim of "confusion" was an ex post facto assertion by the government.
- 30** Sharon Minelli Perez, "DACO Prohibits Businesses Limiting the Sale of Gasoline," *Primera Hora*, September 28, 2017.
- 31** *Container Management*, San Juan Back to 84 Percent Capacity Following Hurricane Maria, October 16, 2017.
- 32** *Caribbean Business*, Price Freeze on Basic Necessities Extended in Puerto Rico, September 13, 2017.
- 33** Federal Emergency Management Agency, Hurricane Maria Update, October 19, 2017.
- 34** Gloria Ruiz Kuilan, "Thousands of PAN Beneficiaries Cannot Use Their Card," *Primera Hora*, October 24, 2017.
- 35** Palin interviews with FEMA officials.
- 36** For more on this interplay between human design and complex adaptive emergence, see Geoffrey West, *Scale: The Universal Laws of Growth, Innovation, Sustainability, and The Pace Of Life In Organisms, Cities, Economies, And Companies*, (New York: Random House, 2018).
- 37** According to the British Dictionary, a joule is the International System of Units measure of work or energy; as when at the point of application, the force of 1 newton is displaced through a distance of 1 metre in the direction of the force. 1 joule is equivalent to 1 watt-second, 10⁷ ergs, 0.2390 calories, or 0.738 foot-pound. A terajoule is one trillion joules.
- 38** RMS, Insured losses from Hurricane Maria, September 28, 2017.
- 39** Annie Lowrey, "Americans are Sending Too Much Stuff to Houston", *The Atlantic*, October 25, 2017.
- 40** Department of Homeland Security (PPD-21), Critical Infrastructure Sectors, July 2017.
- 41** Marcia Heroux Pounds and David Fleshler, "85 Percent of Central Florida Cell Towers Now Restored," *Orlando Sentinel*, September 13, 2017.
- 42** Ibid.
- 43** Jeremy I. Fisher and Ariel I. Horowitz, Expert Report, Synapse Energy, November 2016.
- 44** Government of the Commonwealth of Puerto Rico, StatusPR, October 29, 2017.

45 The distinction between robustness and resilience is helpfully summarized by Mens et al. ("Developing System Robustness Analysis for Drought Risk Management: An Application on a Water Supply Reservoir," *Natural Hazards and Earth System Sciences*, January, 2015): "The concept of robustness originates from the engineering literature, where it is defined as the ability of systems to maintain desired system characteristics when subjected to disturbances" (Carlson and Doyle, 2002). A similar concept, resilience, originates from the socioecological resilience community and is defined as the ability of ecosystems or socio-ecological systems to absorb disturbances without shifting into a different regime (Holling, 1973; Walker and Salt, 2006; Folke, 2006; Scheffer et al., 2001). Robustness and socio-ecological resilience are comparable concepts (Anderies et al., 2004), but robustness is considered more suitable for systems in which some components are designed (Carpenter et al., 2001). While supply chains are more-or-less designed, I would argue they are – increasingly—much more emergent socio-technical systems than engineered systems. Therefore resilience is a more promising framework for enhancing the survivability of content-committed infrastructures.

46 Li, et al., "Identifying Vulnerable Nodes of Complex Networks in Cascading Failures Induced by Node-Based Attacks," *Mathematical Problems in Engineering*, 2013 , Article ID 938398.

47 Matt Egan, "Texas Oil Refineries Still Hurting from Harvey," *CNN Money*, September 11, 2017.

48 Energy Information Administration, Hurricane Harvey Caused U.S. Gulf Coast Refinery Runs to Drop, Gasoline Prices to Rise, September 11, 2017.

49 American Society of Civil Engineers, Report Card for Houston Area Infrastructure, 2012.

50 CBS News, Harvey Floods Left Houston Water Plant Hours Away from Failure, September 5, 2017.

51 Alex Samuels and Cassandra Pollock, "Beaumont Loses Water Supply," *Texas Tribune*, August 31, 2017.

52 *Beaumont Enterprise*, "Beaumont Has Running Water Again—to a Degree," September 1, 2017.

53 Kinder-Morgan, Tampa Fuel Terminal, 2015.

54 Henry Fountain and Brad Plumer, "The Monster Surge that Wasn't," *New York Times*, September 11, 2017.

55 Core Logic, CoreLogic Storm Surge Analysis, June 2016.

56 US Army Corps of Engineers, Waterborne Commerce of the United States (WCUS) Part 2 – Gulf Coast, Mississippi River System, and Antilles, 2010.

57 US Coast Guard, Port Condition Updates, September 23, 2017.

58 Marian Diaz, No Truce in the Demand for Fuel, *El Nuevo Dia*, October 30, 2017.

59 Ted G. Lewis, Center for Homeland Defense and Security, *Risk Methods and Models*, 2014.

60 Michael Lynch, "Best Oil Lesson of Harvey: People Hoard," *Forbes*, September 7, 2017.

61 From indirect evidence, I think it is very likely that fuel supplies in areas dependent on the Colonial Pipeline were significantly reduced during most of early September. But considerable effort was made by the US Department of Energy, Colonial Pipeline, and its clients to avoid exciting consumer uncertainty. As a result, retail networks were mostly kept minimally supplied, hoarding was avoided, and a real supply crunch was thereby avoided.

62 CNN Weather, A Day by Day Look at Hurricane Irma, September 8, 2017.

63 Post-Irma, many Miami retail locations did not open. In the case of several retail chains, up to two-thirds of storefronts remained closed for two to three days as electricity was restored. But those locations that were operating – often on generator power — were fully stocked and effectively re-supplied. By design or accident this "re-sizing" of the retail network allowed distribution/delivery assets to meet demand, avoid sending signals of uncertainty, and prevent hoarding behavior.

64 Michael Watkins and Max Bazerman, "Predictable Surprises: The Disasters You Should Have Seen Coming," *Harvard Business Review*, 2003.

65 Philip J. Palin, "Supply Chain Resilience: Diversity+Self-organization =Adaptation," *Homeland Security Affairs* 9, No. 14, (August 2013).

66 Given the creativity, adaptability, and self-organization required in extreme events, I worry about the – now apparently inevitable – development of autonomous vehicles as the core of mid-century trucking fleets. This sounds like another optimization setting-up catastrophic cascades.

Copyright © 2018 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis

By Eric F. Taquechel & Marina Saitgalina



Abstract

Measuring things that do not occur, such as “deterred” or “prevented” terrorist attacks, can be difficult. Efforts to establish meaningful risk-based performance metrics and performance evaluation frameworks based on such metrics, for government agencies with counterterrorism missions, are arguably in a nascent state. However, by studying program theory, logic models, and performance evaluation theory, as well as studying how risk, deterrence, and resilience concepts may be leveraged to support antiterrorism efforts, one may propose a framework for a logic model or other performance evaluation approach. Such a framework may integrate these concepts to help proxy performance measurement for agencies with prevention and/or deterrence missions. This effort would not be without challenges.

Suggested Citation

Taquechel, Eric F. & Marina Saitgalina. “Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis.” *Homeland Security Affairs* 14, Article 8 (December 2018). <https://www.hsaj.org/articles/14598>

Introduction

Performance measurement is critical to effective government, as it is intended to help improve public management and program outcomes.¹ Performance measurement, when properly done, operationalizes abstract goals, specifies policies, and informs management decisions. However, certain government functions and missions are difficult to measure.² Specifically, adversarial missions such as antiterrorism and law enforcement which center on prevention and/or deterrence may make useful performance evaluation challenging. Therefore, this essay will examine considerations for performance evaluation frameworks that may be useful for assessing agency prevention or deterrence missions. Intended audiences of this research include program managers, performance analysts, policy evaluators, budget analysts, and Congressional budget oversight committees.

Context

Risk management is a critical aspect of CIKR (critical infrastructure/key resources) protection efforts for the Department of Homeland Security (DHS). Risk management may encompass efforts to deter attacks thus reducing threat, protect CIKR thus reducing vulnerability, and increase CIKR resilience thereby reducing consequence. It may also entail simultaneous execution of such efforts. Threat is the likelihood that an attack occurs, and that likelihood includes attacker intent and attacker capability, estimated as probabilities.³ Vulnerability is the likelihood an attack is successful given that it is attempted.⁴ Consequence is the effects of an attack.⁵

Together, these three elements—threat, vulnerability, and consequence—can be combined to form a quantitative approximation of terrorist attack risk. Since performance metrics are also critical to effective government,⁶ the status of efforts to create meaningful performance evaluation systems for antiterrorism programs that specifically leverage risk metrics warrants review.

Importance

The New Public Management (NPM) framework of public administration focuses on outcomes instead of inputs and processes.⁷ This focus has been reaffirmed in the context of exploration of homeland security performance metrics. For example, some analysts claim that outcome-oriented performance management has increasingly supplanted output and process management.⁸

If we believe that the outcome-oriented focus of NPM is still relevant today, despite the alternative theoretical framework of New Public Service (NPS) which prioritizes citizen engagement and inclusiveness (c.f. Denhardt & Denhardt, 2015, p. 32), we must explore how to measure homeland security enterprise outcomes. However, as budgets continue to be constrained, efficiency is just as important as effectiveness. Therefore, a more holistic approach to agency performance evaluation should adopt measures that include resource inputs, activities, and accomplishments (outputs).

Evaluating public agency resource inputs and activities helps with budgeting control and accountability. As agencies make “resource input” decisions in proposed budgets, those agencies can exercise some form of control over their programs. Control is one purpose of budgeting; it ensures tax dollars are used to accomplish budgeted objectives.⁹ Historically, “object budgeting”, or the itemization of expenditures on specific objects, served a control purpose.¹⁰ Therefore, the budgeting objective was to control line item expenditures.

Also, budgeting serves a management/efficiency approach.¹¹ After strategic priorities and objectives are determined, budgeting helps achieve efficiencies in attaining those priorities by allocating limited financial resources. Thus, understanding the outputs that certain resource inputs and activities support helps agencies manage efforts to achieve their strategic objectives more efficiently. Since budgeting also serves a planning purpose,¹² agencies must look at outcome trends to help justify out-year budgets, in support of long-term effectiveness. Existing “planning, programming, budgeting and execution” (PPBE) guidance may help agencies connect the dots between strategic agency priorities, resource needs, and resource constraints. For example, DHS’ FY2006 Congressional Budget Justification includes an overview of the goals of PPBE, which acknowledge fiscal constraints.¹³

Therefore, good fiscal management in public agency antiterrorism program administration warrants consideration of resource inputs, activities, accomplishments, and outcomes, with appropriate supporting metrics. Developing a theoretical framework integrating such considerations could be useful for agencies with prevention or deterrence-oriented missions. In that spirit, exploration of considerations for an appropriate risk-based performance measurement framework seems appropriate, so public agencies with CIKR protection responsibilities can continuously refine program execution and budgeting efforts.

Research Goals

The following research questions can be posed to help shape and inform the research in support of such a framework.

1. What is the current state of literature that might inform performance evaluation frameworks for agencies with antiterrorism mandates, specifically including protecting CIKR?
2. What are potential challenges to advancing performance evaluation frameworks, specifically with respect to incorporating risk terminology and risk theory?

Such a research effort might explore areas of the literature including risk theory, performance measurement theory, program evaluation theory, and law enforcement metrics. Additionally, such effort may benefit from a review of ideas on how to integrate concepts from risk management, particularly deterrence, risk analysis, and resilience theory, into performance evaluation frameworks. We propose ideas on how to integrate these concepts at the end of the essay, in an appendix.

Expected Research Benefits

If we believe public agencies with CIKR protection responsibilities should continuously strive to improve program execution and budgeting efforts, such agencies could benefit from conceptual frameworks to develop and refine risk-based performance metrics to help defend their budgets. Research shows that motivation for using performance metrics includes assessing effectiveness and tracking expenditure allocation.¹⁴ Additionally, academics continue to explore ways to use quantitative data to promote better agency effectiveness and contain costs.¹⁵

Literature Review

Existing Literature

Performance Measurement & Logic Model Theory.

McLaughlin and Jordan identify two purposes for measuring program performance: communicating value to others/accountability, and program improvement.¹⁶ However, what are specific ways to facilitate these purposes? Greenfield et al. discuss the theory of logic models. Logic models are conceptual frameworks to communicate visually a simplified representation of a program's activities, outputs, customers, and outcomes to internal and external audiences, and serve as planning tools.¹⁷ Therefore, logic models are one framework for managing communications and program improvement as advocated by McLaughlin and Jordan. Moreover, both McLaughlin and Jordan and Greenfield et al. offer detailed guidance to help logic model developers ensure those models are valuable. For instance, they recommend ensuring that if intermediate agency outcomes are achieved,

the end-state outcomes will reasonably follow.¹⁸ This speaks to establishing causation or correlation between elements of the logic model.

Risk & CIKR Protection – Theory.

There is much research in the theoretical and applied aspects of risk management for homeland security missions. More specifically, there is a genre of literature that deals with risk theory as applied to CIKR protection. Tauechel and colleagues summarize some of the notable work in this literature in addition to offering their own insights.¹⁹

Tauechel and colleagues offer that the intent probability component of threat can be influenced by agency activities that deter attacks by reducing vulnerability and/or consequence to attack, and such deterrence efforts can be quantified. Furthermore, they argue that CIKR vulnerabilities to exploitation by weapons of mass destruction (WMD) or illicit materiel/personnel transfer can be modeled as logic networks, with implications for how analysts assess vulnerability or more specifically “exploitation susceptibility” of such networks. Additionally, Tauechel and colleagues propose that grants might be administered to help CIKR rebuild after an attack, but distributed as a pre-attack mitigation measure, based on network analysis of supply chain resilience. Other work in the areas of deterrence theory, risk analysis, and resilience includes that of Alderson et al., Cox, Dighe et al., Kahan et al., Jenelius et al., Lebow and Stein, Lewis, Morral and Jackson, and Vugrin et al.²⁰

Incorporating risk theory into performance evaluation poses an opportunity to discuss deterrence theory and adaptive adversary considerations as possible “moderator variables” influencing the nexus between intermediate and end-state agency outcomes. Deterrence theory is multifaceted, but it can succinctly be described as the principle of “when an actor discourages aggression towards another actor, with the intended outcome that the former never has to respond to aggressive action by the latter.”²¹ Furthermore, adaptive adversaries are those that can change their behavior or characteristics in response to prevention, protection, response, or recovery efforts.²² Adaptive adversary considerations and deterrence quantification are important for CIKR risk analysis,²³ and Savitz et al. reinforce the idea of considering reactions of “other parties” in performance measurement.²⁴ Therefore, the perceived effect of changes in adversary intent upon threat reduction metrics could be a valuable component of a logic model framework to integrate risk metrics with antiterrorism program performance evaluation.

Anderson et al. claim that logic models help program managers map out “competing definitions of the determinants of a problem.”²⁵ Since there are different theories about the underlying determinants of risk, in particular the ongoing debate over “static”, probabilistic-based risk analysis vs the “dynamic” game theoretical/adaptive adversary approach espoused by the operations research community (c.f. Tauechel and Lewis, 2012, Tauechel, 2013), logic models may help visually conceptualize how both static and dynamic probabilities of attack could influence risk reduction effectiveness metrics for various antiterrorism activities.

Program theory and “complicated interventions”.

Showing causality or even correlation between prevention/deterrence-oriented homeland security activities and ultimate risk reduction outcomes may be challenging. Rogers discusses the idea of complicated vs. complex/emergent programs. Complicated programs

are those with multiple components, whereas “complex” programs represent programs with “recursive causality” and tipping points.²⁶ Therefore, logic models to describe complex programs may have inherent nonlinearities. Furthermore, Rogers mentions that the external environment, characteristics of clients, and overlapping programs could cause overconfidence in correlation estimates.²⁷

In risk parlance, resilience is the “ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.”²⁸ The definition of resilience also includes system recovery. Systems imply networks, and networks often display emergent phenomena.²⁹ Therefore, if DHS must defend networks of CIKR, and not just individual infrastructures, performance metrics that incorporate resilience or consequence reduction may need to account for network emergent phenomena such as “self-organizing criticality”, wherein systems optimize for efficiency but possibly to the detriment of resilience. This speaks to Rogers’ claim of external influence on program performance, although network emergent phenomena often result from internal, “self-organizing” aspects of network evolution. Nonetheless, this is a “complexity” consideration for program evaluation. Self-organized criticality may create a tipping point.

Applying performance measurement to programs that reduce consequence and increase resilience may be difficult. Specifically, Henstra claims that “one of the most formidable challenges facing local communities today is learning to apply the concepts and methods of performance measurement to disaster preparedness.”³⁰ Cutter et al. add to the debate over this difficulty; they claim it is difficult to measure resilience in absolute terms and proxy variables may be needed.³¹

Another consideration in the literature is that there are different types of logic models used in program theory. For example, “pipeline” logic models show a linear progression from inputs to activities to outputs, whereas “outcome chain” logic models may demonstrate outcomes where initial activities were not considered, and “realist matrix” logic models may model how interventions work differently for different groups in different situations.³² If antiterrorism missions have inherent nonlinearities, especially when it comes to risk modeling, performance evaluators may benefit from different types of logic models.

Performance metrics in law enforcement and antiterrorism.

Law enforcement metrics may inform development of counterterrorism metrics given the common “adversarial nature” of the two missions. Similarly, metric evaluation in law enforcement agencies can be challenging. For example, Braga and Bond discuss efforts to assess correlation between “hot-spot” policing activities and crime levels.³³ Deterrence is another influence upon risk metrics in law enforcement, as it is in antiterrorism. In theory, policing preemptively may deter criminal or terrorist activity. However, from a logic model perspective, Brousselle and Champagne advise that logic analysis, the evaluation of a program’s underlying theory using available scientific knowledge, needs to establish that the means correlate to the desired ends.³⁴ With deterrence theory, the notion that certain enforcement activities influenced the adversary’s “intent” can be a theoretical exercise, without direct evidence of causation. This can make logic model validation difficult.

Another takeaway from Braga and Bond's work is the importance of identifying special causal factors in a program with multiple dimensions.³⁵ Since risk reduction is theoretically achieved by threat reduction activities, vulnerability reduction activities, consequence reduction activities, or a combination of the above, a performance evaluation framework should allow "individual activity" effect isolation, as well as "simultaneously executed activity" effect analysis. Nicholson-Crotty et al. caution against excessive information aggregation; they claim multiple detailed measures of the same concept are often preferable to one aggregate measure.³⁶

However, aggregation might be valuable for different aspects of risk metrics. For instance, Ayyub claims the primary basis for evaluating resilience should include both aggregate measures of systems resilience as well as "segregated performance" of individual system components.³⁷ If program managers want to model the effects of consequence-reducing activities upon residual risk (risk remaining after those activities are performed), they might consider both segregated consequence to individual CIKR, as well as aggregate network effects-based consequences to a CIKR system such as cascading failures. Keeney and Von Winterfeldt also advocate for metric aggregatibility, particularly with respect to whether program objectives are additive or multiplicative.³⁸ For instance, the availability of a radiological detection device is one metric, and the device detection accuracy is another. The two detection program objectives in this case are multiplicative rather than additive.³⁹ Since risk analysis may be quantitative, determining whether metrics should be additive or multiplicative may be crucial.

Additional work with logic models and risk metrics in the antiterrorism world includes evaluation of the effectiveness of the Global Nuclear Detection Architecture (GNDA), a federal program to minimize radiological and nuclear terrorism risk to the U.S. This work evaluated GDNA program goals, objectives, and activities, the goals here being to minimize individual components of the risk equation: threat, vulnerability, and consequence. Each goal had subordinate objectives.⁴⁰ This study also evaluated results exclusive of costs to lower these risk equation components, instead saving those costs for cost-effectiveness analysis.⁴¹

Previous work on analyzing risk reduction metrics vs cost effectiveness also separated costs from the "utility functions" or what outcomes prospective attackers would stand to gain from successful attacks. However, like Hilliard et al., those costs were used for return on investment analysis of different government strategies to deter prospective attackers (c.f. Tauechel and Lewis, 2012; Tauechel, Hollan, and Lewis, 2015; Tauechel and Lewis, 2016). This also speaks to the concept of "metric aggregatibility" emphasized in other work; here it made sense to segregate cost from performance effectiveness metrics, but this may not always be true.

Art of the Possible?

It may be possible to address the "problem" of developing a framework for risk-based performance evaluation in antiterrorism missions that specifically involve CIKR protection. Creating a logic model that incorporates activities, accomplishments and outcomes of such missions, and supporting those logic model elements with a variety of quantitative risk metrics, might advance solutions. Furthermore, it may be possible to evaluate the appropriate use of risk metrics based on their value in helping budget for an antiterrorism

program, based on principles of line item/cost center accountability, efficiency, and/or overall program effectiveness. Moreover, such a logic model may be able to capture the effects of quantifiable deterrence and network effects upon risk metrics, as well as other considerations from this literature review.

Literature Gaps

In light of the two identified research goals, and given this snapshot of “art of the possible”, a review of the literature identifies the following gaps. With respect to the first research goal, to our knowledge the literature does not explicitly discuss a theory or model of how antiterrorism activities, outputs, and outcomes might be organized within a performance evaluation framework, with supporting quantitative risk metrics, perhaps broken down by each component of the risk equation (threat, vulnerability, consequence). Hilliard et al. (2015) specifically discussed nuclear weapon risk in what might be termed a “logic model” framework, but future work might be generalized to all CIKR risk.

With respect to the second research goal, the literature has gaps in several areas. First, despite the claims of Anderson and Savitz et al. that external influences must be accounted for and problems may have competing interpretations, to our knowledge the literature does not specifically explore how a performance evaluation framework might reconcile multiple interpretations of the threat component of the risk equation, specifically the ongoing debate over probabilistic risk analysis vs. operations research/game theory (c.f. Taquechel & Lewis, 2012).

Second, the literature does not specifically discuss the challenge of how measurable adaptive adversary influences on risk, possibly as a recursive mechanism of action, could be incorporated into a performance evaluation framework. Furthermore, Taquechel and Lewis showed how deterrence effects of certain activities could be quantified and proposed how the effects of such activities were double-counted in revised risk equations.⁴² Specifically, vulnerability reduction activities at CIKR both deter, thus reducing threat, and reduce vulnerability, therefore “doubly” reducing risk. However, to our knowledge no literature has proposed how such accounting for risk reduction might inform a performance evaluation framework.

Third, despite Henstra’s and Cutter’s efforts to explore performance metrics in the area of resilience, the literature does not specifically discuss how quantifiable network effects on system resilience could be incorporated into a performance evaluation framework for agencies with CIKR protection responsibilities. Fourth, despite the ongoing debate in the literature regarding metric aggregatibility (c.f. Ayyub, Nicholson-Crotty, Braga & Bond, Keeney & Von Winterfeldt), to our knowledge the literature does not examine how vulnerability and exploitation potential of CIKR and networks comprised thereof, both in terms of individual and aggregate vulnerability or exploitation potential, might be incorporated into performance evaluation frameworks.

Recommendations and Implications – Logic Model Framework Development

Recommendations

We recommend developing a logic model framework that maps antiterrorism activities to outputs to outcomes. Outputs may include attacks prevented/deterred, compliance achieved, and damage minimized. Outcomes may entail residual risk, or risk remaining after activities are executed and outputs (risk that was reduced) are tabulated. Furthermore, the quantitative metrics for outputs might reflect different budgeting theories, for example as discussed in Hou (2006). Additionally, such a logic model might incorporate activities and metrics that account for the nonlinear and recursive effects of adaptive adversary influence on CIKR risk, as well as the complexity of network effects upon vulnerability and consequence.

For instance, output metrics fashioned after the “responsibility center” or “line-item budgeting” approach might explore threat reduced by attacks deterred. Alternatively, metrics fashioned after the efficiency or performance-based budgeting approach might explore risk reduced, solely as a function of those threat-reducing activities, divided by time or cost spent executing those activities. As a third option, output metrics fashioned after “effectiveness-based” or “rational-comprehensive” based budgeting may explore risk reduced, as a function only of threat-reducing activities, but omitting a cost/time denominator.

Our speculation is that activity metrics should reflect number of activities performed, and that output metrics should reflect quantified risk reduced. Furthermore, we speculate that outcome metrics should be quantified residual risk after activities are performed. Greenfield et al. claim in a notional logic model for a government injury prevention program that the reduction in the incidence of sexual violence is considered an “end outcome” metric.⁴³ The end goal in this work seems to be minimized “residual violence.” More generally, they claim metrics associated with annual goals typically serve as indicators of a program’s *efforts* (our emphasis), whereas the intermediate and strategic goals (equivalent to outcomes) and their associated metrics are indicative of a program’s *effect* (our emphasis).⁴⁴ By that logic, antiterrorism activities might be considered efforts, whereas risk reduced and residual risk to CIKR might be the effects.

Implications and Constraints

Such a logic model framework would assume that antiterrorism activities can be estimated to reduce quantitatively elements of risk. In other words, certain activities might be estimated to reduce threat through deterrence; other activities might be assumed to reduce vulnerability through increasing target security and law enforcement response capabilities; and yet other activities might be assumed to reduce consequence through response and recovery efforts.

The multiplicative effects of specific activities on multiple elements of the risk equation might be accounted for in a theoretical fashion, but this could make line item budgeting difficult. However, activities that reduce multiple aspects of risk, e.g. through both deterring

(reducing threat) and protecting CIKR (e.g., reducing vulnerability), might be thought of as “robust activities.” Furthermore, agency capabilities leveraged to execute those activities might be thought of as “robust capabilities,” something that certain agencies may value even if it made activity-based or line-item budgeting difficult. One theory is that goals, requirements, and metrics should be conceived more in terms of “capability envelopes” rather than particular scenarios.⁴⁵ However, in agencies where budgeting is closely linked to capabilities (e.g. aircraft, boats, specialized tactical units), especially capabilities that perform multiple missions, a logic model approach based on activity performance and linkage to outcomes may be challenging if one objective is to inform budget development.

Fiscal Constraints

Allocation of performance requires outcome measures; whereas budgeting decisions require efficiency measures.⁴⁶ If an agency with antiterrorism mission execution responsibilities is resource-constrained, it may prefer only activity-based budgeting, here meaning budgeting for costs of executing a certain number of antiterrorism activities, without regard to output or outcome. Conversely, if an agency focuses more on performance-based budgeting, it may prefer to adjust activity execution to reduce a certain amount of risk, or leave a certain amount of estimated residual risk. A modeled optimization solution could maximize risk reduction given an upper bound constraint on resources.

Political Constraints

Some claim that outcome-based metrics are so general as to be meaningless for budgeting and accounting purposes.⁴⁷ Based on the approach proposed here, if residual risk outcome metrics are perceived as inefficacious for supporting line item or efficiency-based budgeting, the literature would suggest that not even an antiterrorism program’s effectiveness-based budgeting effort could realistically be supported by residual risk metrics.

As agencies develop and propose budgets in an environment where elected officials scrutinize agency performance metrics, it may be difficult to justify funding based on a program logic model that advocates risk reduction, even if elected officials like the principle of programs targeting quantitative risk reduction. Accountability for performance is sometime perceived as secondary compared to accountability for finances and for procedural fairness.⁴⁸ Therefore, even if a rigorous model linking activities to risk reduction metrics is developed, expenditures on capability packages or activity execution may receive more scrutiny than expenditures incurred in aggregate to achieve stated risk reduction goals.

Another consideration is that performance standards can be derived from past performance or performance of similar agencies.⁴⁹ If politicians are not familiar with the evolving technical aspects of quantitative risk analysis and management, they may benchmark agency performance off previous performance or that of similar agencies, possibly to the detriment of what an agency is truly trying to achieve.

Technological Constraints

Models that optimize performance are subject to tradeoffs between rigor and simplicity. Any modeling effort that maps specific activity execution to quantitative risk reduction

metrics, slicing and dicing amongst the theoretical elements of risk (threat, vulnerability, consequence) may increase in cost as complexity increases. Greenfield et al. encourage determining correlation or causality in logic models⁵⁰; but Savitz et al. claim that some metrics for one federal agency's antiterrorism mission might be inherently unreliable given the paucity of real-world terrorist attacks.⁵¹

Time constraints

Some agencies require models that support certain decisions to undergo a formal Verification, Validation, and Accreditation (VV&A) process. Such a process could require lots of analyst effort and financial support. Fortunately, model accreditation processes in some agencies may be tailored subject to resource constraints. Furthermore, the wicked problem approach may limit model effectiveness, absent sufficient time to develop such a model. Caudle (2005) argues that:

[t]he program logic model has one major drawback for homeland security in that it clearly targets programs, normally within an organization's control, as the unit of analysis...complex program logic models would be necessary for homeland security to reflect the interdependencies of many organizations and programs.⁵²

With this in mind, modeling the effects of Rogers' (2008) program "overlap" upon logic model activities and metrics might increase the time needed to construct a valuable risk metric-based logic model for CIKR protection missions.

Conclusions

The research here suggests that efforts to establish meaningful risk-based performance evaluation models with risk metrics for use by agencies with counterterrorism missions are in a somewhat nascent state. However, we are optimistic that by continuing to study program theory, logic models, and performance evaluation theory, as well as continuing to study how risk, deterrence, and resilience concepts are leveraged to support antiterrorism efforts, academics and practitioners might flesh out a framework for a logic model or other performance evaluation approach that integrates these concepts to help evaluate performance for agencies with a terrorism prevention/deterrence mission.

One might conjecture that an effort to build a performance evaluation framework based on quantitative risk metrics might get at the historical differentiation between performance budgeting and program budgeting. The former, derived from scientific management principles, was considered a different budgeting system from the latter, influenced by economic and systems analysis.⁵³ If program objectives are to reduce risk and minimize residual risk, and quantitative risk reduction is a metric, perhaps both performance and program-based budgeting are simultaneously attainable by one agency. One might also speculate that such a framework could integrate both the input accountability concerns and the outcome-based performance concerns that Heinrich proposes:

"[a]n important question that arises for public managers and researchers is, are outcome-based performance management systems more effective than traditional approaches to bureaucratic control?"⁵⁴

In addition to the constraints identified earlier, Caudle claims establishing cause and effect relationships to guide measurement techniques for homeland security programs is still nascent.⁵⁵ With the knowledge that perfectly quantifiable metrics may not be realistic, an agency can still move forward with studying correlation between activities and risk reduction/residual risk metrics for antiterrorism programs. Collins advocates that the public sector should not focus exclusively on “perfectly quantifiable metrics,” but should at least gather evidence of progress.⁵⁶

Risk reduction is a quantifiable metric, but correlating costs of assets to execute risk reduction activities may get at the challenge that Lewis posed in his seminal work on public budgeting. If we subscribe to the theory of evaluating budgets based on marginal utility, maximum gain for expenditures can only be obtained if those expenditures are distributed amongst different purposes such that the last dollar spent for each purpose yields the same return.⁵⁷ The concept of marginal utility entails analysis of how alternative uses of the same increment of available resources would yield different returns on investment, and prioritizing those alternative uses.⁵⁸

Some agencies with antiterrorism missions may focus on control-based budgeting and track expenditures for assets, such as boats and aircraft. If the outcomes to be achieved are risk reduction measures that can be sliced/diced in different ways, marginal utility theory may mean those agencies can link expenditures to risk reduced through threat reduction alone, through vulnerability reduction, through consequence reduction, or permutations of the above. This portfolio of options may have implications for how such agencies defend their budgets, per marginal utility theory, in an incremental budgetary environment.

Proposed Way Ahead

The next steps to continue this framework development effort might entail the following.

1. Flesh out a notional logic model that links agency antiterrorism activities, such as port patrols and vessel escorts, to agency accomplishments (possibly reduced risk), to agency outcomes (possibly residual risk).
2. Hypothesize appropriate metrics for each activity, accomplishment, and outcome. Consider direct and indirect or “proxy” metrics.
3. Assess whether those metrics might be modified to accommodate different budgeting theories (line item/responsibility center, efficiency, effectiveness).
4. Assess whether metrics can accommodate quantifiable deterrence/adaptive adversary considerations, network exploitation susceptibility and other network effects on vulnerability, and/or network effects on consequence and resilience.
5. Assess the “aggregatibility” and “severability” of various metrics. For example, with respect to adaptive adversary factors, assess whether metrics derived from the concept of attacker and defender “utility” should segregate from those metrics, or aggregate therein, costs and other agency resource inputs to execute antiterrorism activities.
6. Assess the effects of other organizations with similar missions upon the efficacy of certain metrics in evaluating logic model elements.

7. Assess whether a linear “pipeline” model, “outcome-chain”, recursive loop model, “realist” model, or other variety of logic model is most preferable.
8. Socialize various logic model formats/details with program sponsors, budget analysts, and agency overseers and revise models as appropriate.
9. Determine whether the preferred model would meet the threshold for formal agency verification, validation, and accreditation efforts, and estimate needed resources if that determination is in the affirmative.

Ongoing efforts to develop agency performance evaluation frameworks should be assessed as part of this way ahead.

Appendix

Here, we show some basic logic models that broach the recommended steps in the Proposed Way Ahead. These are not intended to be exhaustive, but instead are intended to illustrate, at a high level, how the concepts discussed in this essay might be presented for further exploration.

Threat Reduction

Logic Model Explanation

First, we show a notional activity-accomplishment-outcome logic model for deterrence activities (threat reduction). We show notional metrics, partitioned by the three budgeting theories: line item or cost center, efficiency, and effectiveness.

Purpose: Deterrence

Activity		Metric		
Stationary Target	“Zone Defense”	# Activities / time or \$ expended		
Moving Target	“Point Defense”			
Stationary Target	“Point Defense”			

Accomplishment	Metric		
Attacks Deterred	Line Item	Efficiency	Effectiveness
	$T \downarrow$	$\frac{R \downarrow _{T \downarrow}}{\$,time}$	$R \downarrow _{T \downarrow}$

Outcome	Metric		
Residual Threat	Line Item	Efficiency	Effectiveness
	T_{res}	$\frac{R_{res} _{T \downarrow}}{\$,time}$	$R_{res} _{T \downarrow}$

Figure 1. Logic model, deterrence activities (threat reduction)

Key:

$T \downarrow$ = threat reduced (as per deterrence activities)

$\frac{R \downarrow |_{T \downarrow}}{\$, time}$ = risk reduced given threat reduced, divided by resource inputs (time and/or money)

$R \downarrow |_{T \downarrow}$ = risk reduced given threat reduced, irrespective of resource inputs

T_{res} = residual threat (after deterrence activities executed)

$\frac{R_{res} |_{T \downarrow}}{\$, time}$ = residual risk given threat reduced, divided by resource inputs (time and/or money)

$R_{res} |_{T \downarrow}$ = residual risk given threat reduced, irrespective of resource inputs

In Figure 1, activities such as stationary and moving target defenses can be measured by number of activities performed, per resource input such as time or money, or both. The accomplishment of this effort is attacks deterred, with possible metrics of threat reduced (line item – tie to specific activity or asset performing activity), risk reduced as a function of threat per resource input (efficiency), or risk reduced as a function of threat (effectiveness). The outcome is residual risk, or what risk remains to the infrastructure after deterrence activities are executed.

Analysis

Here, if risk reduction is used as an efficiency or effectiveness metric, it could be isolated to the risk reduced solely as a function of threat-reducing or “deterrence” activities noted. The classic risk equation also incorporates vulnerability (V) and consequence (C) terms.

$$R = f(T, V, C)$$

Eq. 1. Basic Risk Equation

In reality, do security activities simultaneously reduce more than one element of the risk equation? This gets into aggregatibility/severability challenges, but specific to threat reduction efforts, the double counting effects of quantifiable deterrence discussed in Taquechel and Lewis (2012) may be a consideration in performance measurement.

Double Counting Threat Reduction

One can argue that change in threat, or attacker capability and intent to attack, is a function of changes in target vulnerability and/or consequence.

$$T = f(V, C)$$

Eq. 2. Threat as function of vulnerability, consequence

We also know that threat is derived from intent and capability:

$$T = f(Intent, Cap)$$

Eq. 3. Threat as function of intent, capability

Previous work⁵⁹ has proposed that intent is a function of a ratio of attacker expected utility ($U_e A$), or benefit from a successful attack, to the aggregate of all expected utilities from available attacker courses of action:

$$Intent = \frac{U_e A}{\sum U_e A}$$

Eq. 4. Intent as function of attacker expected utility

We also can surmise that attacker expected utility is a function of target vulnerability and consequence. What a target's defender stands to lose, an attacker stands to gain:

$$U_e A = f(V, C)$$

Eq. 5. Attacker expected utility as function of vulnerability, consequence

How does this lead to double counting? If target V or C decreases due to the target defender's actions, expected utility of an attack would decrease, thus decreasing intent and attacker threat. This ultimately suggests risk reduction.

$$V \downarrow, C \downarrow \rightarrow U_e A \downarrow \rightarrow Intent \downarrow \rightarrow T \downarrow \rightarrow R \downarrow$$

However, the effect of vulnerability and/or consequence reduction itself should be sufficient to argue risk is reduced:

$$V \downarrow, C \downarrow \rightarrow R \downarrow$$

Therefore, isolating the effects of threat reduction due to deterrence-oriented activities upon risk reduction becomes theoretically challenging. Did the risk reduce because an

adversary noticed the point or zone defense activities and therefore had less intent to act? If so, by that logic, risk would be mathematically reduced twice: by the lowering of threat (per Equation 3), and the lowering of vulnerability or consequence (per Equation 1). While we can argue on a theoretical level that this double-counting effect of deterrence activities seems logical, from a performance metrics standpoint, one challenge may be arguing how much risk reduction is directly attributable to activities intended to deter, or reduce threat. Zone defense security activities seem more susceptible to this challenge, if they do not focus security coverage on individual targets, but instead cast a wide net over a group of targets. The effort to reduce target vulnerability with a randomized, “zone defense” presence may be less effective than the effort to reduce attacker intent to attack, and thus reduce threat. The relationship between specific tactical activities and metrics must be explored further.

Tracking Expenditures

The nexus between agency expenditure of time and/or money obligated to execute these deterrence-oriented activities, and the execution of the activities themselves, must be clear in order to have defensible efficiency metrics. For instance, if the funding for assets executing deterrence activities is earmarked specifically for those activities, but then the asset is diverted to perform a different task, the actual expenditure of those funds may trace to multiple activities in the accounting. This may make budget planning challenging if we link strategic mission budgeting, mission operational planning, and mission execution activities.

Instead, budgeting to line item capabilities (such as aircraft or boats) that perform multiple missions within an agency’s portfolio may be easier, at least from a cost center/line-item budgeting perspective. Assets are constrained by engineering-driven costs such as fuel consumption and repair cycles, which may mean mission execution is constrained by available logistical support funding. This may reflect realities of budgetary and logistical constraints, and whether outcome-based budgeting is feasible, especially in a prevention or deterrence-oriented mission, is subject to debate. This issue is particularly relevant to deterrence-focused activities in a logic model as they may be perceived as “generalist” in nature, not protecting any specific target nor responding to specific events or actionable intelligence.

Vulnerability Reduction

Next, we show a notional activity-accomplishment-outcome logic model for Prevention/Protection-oriented activities (vulnerability reduction), with notional metrics.

Purpose: Prevent & Protect

Activity	Metric
Stationary Target "Zone Defense"	# Activities / time or \$ expended
Moving Target "Point Defense"	
Stationary Target "Point Defense"	
Compliance Inspections	

Accomplishment	Metric
Attacks Prevented	Line Item Efficiency Effectiveness
	$V \downarrow$ $\frac{R \downarrow _{V \downarrow}}{\$,time}$ $R \downarrow _{V \downarrow}$
Compliance Achieved	

Outcome	Metric
Residual Vulnerability	Line Item Efficiency Effectiveness
	V_{res} $\frac{R_{res} _{V \downarrow}}{\$,time}$ $R_{res} _{V \downarrow}$

Figure 2. Logic model, prevention/protection activities (vulnerability reduction)

Key:

$V \downarrow$ = vulnerability reduced (as per prevent/protect activities)

$\frac{R \downarrow |_{V \downarrow}}{\$,time}$ = risk reduced given vulnerability reduced, divided by resource inputs (time and/or money)

$R \downarrow |_{V \downarrow}$ = risk reduced given vulnerability reduced, irrespective of resource inputs

V_{res} = residual vulnerability (after prevent/protect activities executed)

$\frac{R_{res} |_{V \downarrow}}{\$,time}$ = residual risk given vulnerability reduced, divided by resource inputs (time and/or money)

$R_{res} |_{V \downarrow}$ = residual risk given vulnerability reduced, irrespective of resource inputs

Logic Model Explanation

The first change from Figure 1 is that a new activity is introduced: compliance inspections. These inspections may be conducted armed or unarmed, depending on the purpose, but arguably armed inspections might prevent or protect against an imminent attack more effectively.

That notwithstanding, the next change is that one accomplishment is “attacks prevented” rather than “attacks deterred.” We introduce a second objective, “compliance achieved.” Whether this is synonymous with “attacks prevented” for logic model analysis purposes may require additional examination.

Then, we see the outcome is “residual vulnerability,” or the probability of a successful attack given preventive/protective activities have been executed. The metrics for all activities, accomplishments and outcomes in this logic model have the same structure as those in Figure 1, but are modified replacing Threat with Vulnerability.

Analysis

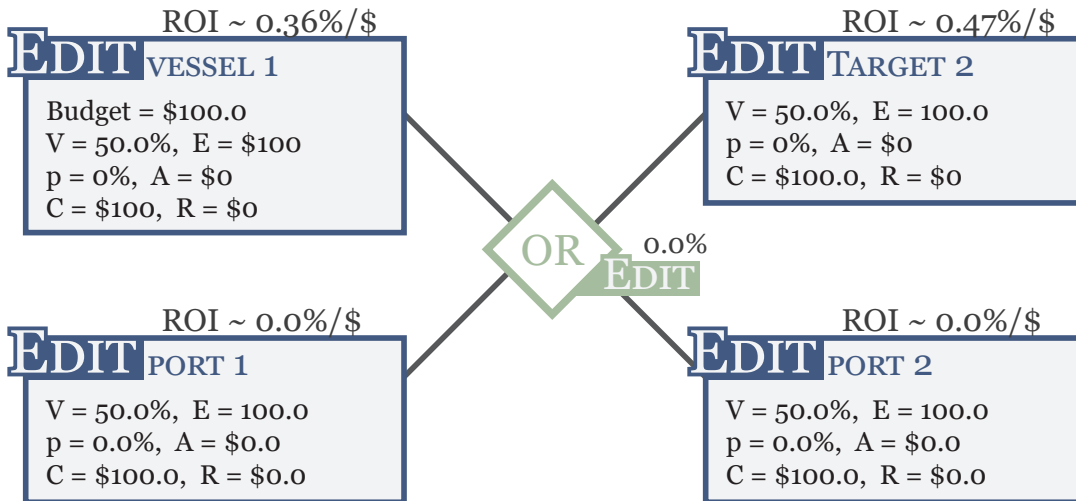
Aggregatibility/Severability

Since we are not focusing on the “double-counting” phenomenon here, aggregatibility and severability takes on a different meaning. Previous work has explored network effects in defending critical infrastructure.

Network Effects- V Reduction

We now lay the foundation for a modification to the Figure 2 logic model. This incorporates ideas from network analysis, with specific reference to the type of threat addressed. Are we protecting individual CIKR from direct attack, or from exploitation (moving illicit material through enroute to a different destination)? This analysis will assume the latter.

First, we discuss some basis concepts underpinning the “exploitation susceptibility” lens through which we will view network effects on vulnerability and performance metrics.



V = organic vulnerability of each node
 p = likelihood that fault would propagate through a node
 E = \$ that would have to be spent to reduce a node’s organic vulnerability to 5%
 A = \$ actually invested to defend a node
 ROI = return on investment

Figure 3. Logic graph rendering of a transfer network – two ports and two vessels (Taquechel, 2010, p. 31)

A transfer network is a representation of how the terrorist transfer threat, or movement of terrorists or illicit material, can propagate throughout transportation nodes.⁶⁰ If ports include CIKR that we prevent or protect against attacks, this network logic could be useful in exploring appropriate vulnerability reduction metrics for the transfer threat. Shown in expanded form, we have a notional network where an adversary might exploit foreign ports (embark), vessels, and domestic U.S. ports (debark), with the option to choose from multiple targets of attack:

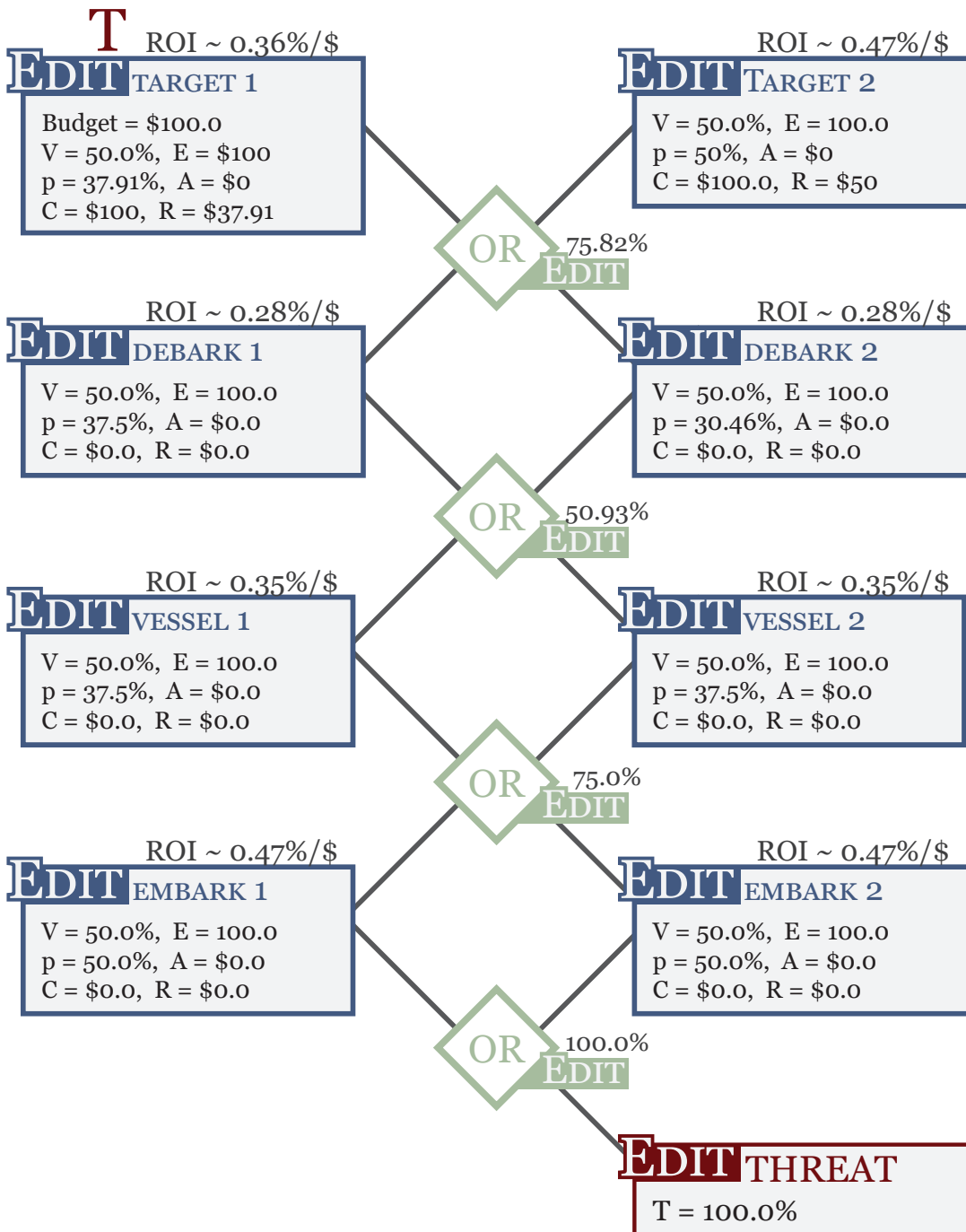


Figure 4. Logic graph rendering of an expanded transfer network (Taquechel, 2010, p. 32)

If our objective is to reduce “exploitation susceptibility,” or a specific type of vulnerability that estimates a port facility’s likelihood of exploitation due to an adversary moving illicit goods through undetected (rather than a direct attack against that facility), then our V metrics may take a different form for logic models. Previous work allows us to propose such a functional form of exploitation susceptibility:

$$V_{network} = 1 - (1 - V_{D1})(1 - V_{D2})$$

Eq. 6. Network vulnerability (exploitation susceptibility), transfer network as shown in Fig 4.

Here, this network exploitation susceptibility reflects the choices the attacker can make for target selection, and the V_{D1} / V_{D2} terms reflect a “nested” vulnerability component that accounts for the ease with which attackers can move materiel or people through this network.

This equation may yield a different value for the network’s aggregate vulnerability, or aggregate exploitation susceptibility, than if we only consider the vulnerability of individual CIKR. We can protect infrastructure in the two “ports of debarkation,” but if our objective is to defend against network exploitation, our logic model metrics now take a different form:

Purpose: Prevent & Protect – Network Exploitation

Activity		Metric
Stationary Target	“Zone Defense”	# Activities / time or \$ expended
Moving Target	“Point Defense”	
Stationary Target	“Point Defense”	
Compliance Inspections		

Accomplishment	Metric		
Exploitation Prevented	Line Item	Efficiency	Effectiveness
Compliance Achieved	$V_{network} \downarrow$	$\frac{R_{network} \downarrow}{V_{network} \downarrow}$	$R_{network} \downarrow$
		\$, time	

Outcome	Metric		
Residual Network Vulnerability (Exploitation Susceptibility)	Line Item	Efficiency	Effectiveness
	$V_{network}^{res}$	$\frac{R_{network}^{res}}{V_{network}^{res} \downarrow}$	$R_{network}^{res} \downarrow$
		\$, time	

Figure 5. Logic model, prevention/protection activities (network exploitation)

Key:

$V_{network} \downarrow$ = network exploitation susceptibility reduced (as per prevent/protect activities)

$\frac{R_{network} \downarrow |_{V_{network} \downarrow}}{\$,time}$ = network risk reduced given network exploitation susceptibility reduced, divided by resource inputs (time and/or money)

$R_{network} \downarrow |_{V_{network} \downarrow}$ = network risk reduced given network exploitation susceptibility reduced, irrespective of resource inputs

$V_{network}^{res}$ = residual network exploitation susceptibility (after prevent/protect activities executed)

$\frac{R_{network}^{res} |_{V_{network}^{res} \downarrow}}{\$,time}$ = residual network risk given network exploitation susceptibility reduced, divided by resource input (time and/or money)

$\frac{R_{network}^{res} |_{V_{network}^{res} \downarrow}}{\$,time}$ = residual network risk given network exploitation susceptibility reduced, irrespective of resource inputs

How is residual network exploitation susceptibility expressed? We add exponential terms to Equation 6 to account for modeled investments to reduce this susceptibility, expressed probabilistically.

$$V_{network}^{res} = 1 - \left(1 - V_{D1} e^{\left(\frac{-A_{D1} \lambda_{D1}}{E_{D1}} \right)} \right) \left(1 - V_{D2} e^{\left(\frac{-A_{D2} \lambda_{D2}}{E_{D2}} \right)} \right)$$

Eq. 7. Network vulnerability (exploitation susceptibility), residual after investment

Importantly – the focus of the prevention/protection activities in this logic model remains the same CIKR targets as in Figure 3 –US port infrastructure. But, there are additional influences on the vulnerability that those executing these activities “inherit” from upstream defensive efforts, such as overseas compliance inspections. These influences may be outside the scope of the logic model under consideration.

Furthermore, the compliance inspection activity holds yet another vulnerability reduction purpose when the objective is specifically to prevent or protect against exploitation via nuclear weapons shipments. This may entail inspection of weapon detection equipment and SOP compliance efforts. See Taquechel, Hollan and Lewis (2015) for more discussion.

Tracking Expenditures – Issues Specific to V-reducing Activities

One consideration for the efficiency metric denominator here is how realistic the influence of protective activities in U.S. ports is, when the issue at hand is exploitation susceptibility. The vulnerability reduction effects of overseas compliance inspections and at-sea actions may influence exploitation susceptibility, and protection activities in U.S. ports may only contribute marginally to overall network exploitation susceptibility reduction. This may be a return on investment consideration if the prevailing preference for performance metrics is driven by efficiency, or accomplishment per expenditure. This gets back to the theoretical consideration of external influences upon performance metrics as discussed in Rogers (2008).

Consequence Reduction

Next, we show a notional activity-accomplishment-outcome logic model for resilience-oriented activities (consequence reduction), with notional metrics.

Purpose: Resilience

Activity	Metric		
Port Security Grants - Resilience Investment	Grants approved per input effort/ (Time to process, \$)		

Accomplishment	Metric		
Economic Loss Reduced	Line Item $C_{\$} \downarrow$	Efficiency $\frac{R_{C_{\$}} \downarrow}{\$, time} \Big _{C_{\$} \downarrow}$	Effectiveness $R_{C_{\$}} \downarrow \Big _{C_{\$} \downarrow}$

Outcome	Metric		
Economic Productivity Retained	Line Item $C_{\res	Efficiency $\frac{R_{C_{\$}}^{res}}{\$, time} \Big _{C_{\$} \downarrow}$	Effectiveness $R_{C_{\$}}^{res} \Big _{C_{\$} \downarrow}$

Figure 6. Logic model, resilience activities (consequence reduction)

Key:

$C_{\$} \downarrow$ = economic loss theoretically avoided (by resilience activities)

$\frac{R_{C_{\$} \downarrow}}{\$,time}$ = CIKR lost productivity avoided given resilience activities, accounting for probability of attack, divided by resource inputs (time and/or money)

$R_{C_{\$} \downarrow}$ = CIKR lost productivity avoided, irrespective of resource inputs

$C_{\res = residual economic productivity (after resilience activities executed)

$\frac{R_{C_{\$}^{res}}}{\$,time}$ = residual CIKR productivity, accounting for probability of attack, divided by resource input (time and/or money)

$R_{C_{\$}^{res}}$ = residual CIKR productivity, irrespective of resource inputs

Logic Model Explanation

Here, the activity is port security grants, which per previous work were proposed to take a resilience-focused approach, providing to CIKR money specifically earmarked for capability to rebuild to facilitate some level of productivity after an incident. See Taquechel (2013) for more details.

The accomplishment is economic loss theoretically reduced or avoided by these resilience activities, as lost economic productivity can be considered a consequence. Metrics entail quantified economic loss (line item), or risk as a function of that economic consequence (network lost productivity that accounts for probability of attack), either per effort expended to administer grants (efficiency), or disregarding effort (effectiveness).

The outcome is residual economic productivity, measured by dollars (line item), or by residual network functionality per grant administration effort, or without regard to effort (efficiency vs effectiveness).

Analysis

Aggregatibility/Severability

Here, aggregatibility/severability of metrics also gets into network effects, but in terms of “cascading economic effects” on networks of infrastructure, as explored in Taquechel (2013). In other words, the aggregatibility focuses on the network effects of consequence

rather than the network effects of vulnerability or exploitation susceptibility. We can call this “failure susceptibility” in consequence terms.

Network Effects- C Reduction (Resilience)

We now show a modification to the Figure 6 logic model. This incorporates ideas from network theory, with a consequence focus. Taquechel (2013) introduced the term “inherited failure susceptibility,” proxied by CIKR network node degree, meaning the number of upstream suppliers a CIKR has in a supply chain. When considered in tandem with a CIKR’s organic failure susceptibility, e.g. lack of reserve raw product onsite to resume production after a disruption, inherited failure susceptibility may exacerbate overall network failure susceptibility.

To set context for the updated logic model, we introduce an “expected network consequence” term:

$$Con^{l(\text{exp})} = \sum_i \left(g_i Con_i^{(\text{max})} e^{\left(\frac{-A_i^{raw} \lambda_i^{raw}}{E_i^{raw}} \right)} \right)$$

Eq. 8. Expected consequence of lth supply chain network with i nodes

This term accounts for the organic failure susceptibility of all nodes in a supply chain network. The organic failure susceptibility is modeled as an exponential relationship between resilience effort actually invested and investment needed to minimize failure susceptibility. This susceptibility probabilistically modifies the maximum possible economic loss to an ith node $Con_i^{(\text{max})}$. The expected consequence to each node sums to the total expected network consequence.

If resilience activities covered in the logic model only improve resilience at some of the network nodes, they may reduce overall network failure susceptibility and economic loss, but the interdependencies between network nodes, proxied by node degree g , may increase potential loss. That said, we want to expand our depiction of network expected consequence, as a function of resilience investments at the supplier nodes, here with maximum consequence $Con_s^{(\text{max})}$.

$$Con^{l(\text{exp})} = \sum_i \left(g_s Con_s^{(\text{max})} \left[e^{\left(\frac{-A_s^{reb} \lambda_s^{reb}}{E_s^{reb}} \right)} \left(1 - e^{\left(\frac{-A_s^{raw} \lambda_s^{raw}}{E_s^{raw}} \right)} e^{\left(\frac{-A_s^{red} \lambda_s^{red}}{E_s^{red}} \right)} \right) + e^{\left(\frac{-A_s^{raw} \lambda_s^{raw}}{E_s^{raw}} \right)} e^{\left(\frac{-A_s^{red} \lambda_s^{red}}{E_s^{red}} \right)} \right] + \sum_{I_j=3} g_{I_j} Con_{I_j}^{(\text{max})} e^{\left(\frac{-A_{I_j}^{raw} \lambda_{I_j}^{raw}}{E_{I_j}^{raw}} \right)} + \sum_{C_k=6} g_{C_k} Con_{C_k}^{(\text{max})} e^{\left(\frac{-A_{C_k}^{raw} \lambda_{C_k}^{raw}}{E_{C_k}^{raw}} \right)} \right)$$

Eq. 9. Expected consequence to lth supply chain network, expanded to show supplier node failure probabilities

If we invest to increase the probability of rebuilding after a disruption, the A_s^{reb} term will increase, thus increasing economic productivity.

Next, we introduce a term for risk to a network, that factors in network expected consequence:

$$R_{cond}^l = Cap_s^l V_s^l Con^{l(\text{exp})}$$

Eq. 10. Conditional risk to lth supply chain network

The risk to a supply chain network is thus a function of network expected consequence, but also of an attacker's capability to attack supplier node s, and that node's vulnerability to attack. Therefore, an efficiency metric would be conditional network risk reduced or avoided, as a function of possible economic loss reduced, per effort to ensure such loss reduction. This term can capture the expanded form of expected consequence shown in Equation 9, to allow simulation of resilience investments that would lower conditional risk, retaining economic productivity. This retained economic productivity can be expressed as a resilience term, the difference between maximum pre-disruption economic output, and conditional risk (expected economic loss) resulting from a disruption:

$$Resilience^l = Con^{l(\text{max})} - R_{cond}^l \Big|_{Con^{l(\text{exp})} \downarrow}$$

Eq. 11. Resilience of lth supply chain, given efforts to reduce expected economic loss

Therefore, we can now show our modification to Figure 6:

Purpose: Resilience - Network

Activity	Metric
Port Security Grants - Resilience Investment	Grants approved per input effort/ (Time to process, \$)

Accomplishment	Metric									
Network Economic Loss Reduced	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center; width: 33%;">Line Item</td> <td style="text-align: center; width: 33%;">Efficiency</td> <td style="text-align: center; width: 33%;">Effectiveness</td> </tr> <tr> <td style="text-align: center;">$Con^{1(exp)} \downarrow$</td> <td style="text-align: center;">$\frac{R^l_{cond} \downarrow}{Con^{1(exp)} \downarrow}$</td> <td style="text-align: center;">$\frac{R^l_{cond} \downarrow}{Con^{1(exp)} \downarrow}$</td> </tr> <tr> <td></td> <td style="text-align: center;">$\\$, time$</td> <td></td> </tr> </table>	Line Item	Efficiency	Effectiveness	$Con^{1(exp)} \downarrow$	$\frac{R^l_{cond} \downarrow}{Con^{1(exp)} \downarrow}$	$\frac{R^l_{cond} \downarrow}{Con^{1(exp)} \downarrow}$		$\$, time$	
Line Item	Efficiency	Effectiveness								
$Con^{1(exp)} \downarrow$	$\frac{R^l_{cond} \downarrow}{Con^{1(exp)} \downarrow}$	$\frac{R^l_{cond} \downarrow}{Con^{1(exp)} \downarrow}$								
	$\$, time$									

Outcome	Metric									
Economic Productivity Retained	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center; width: 33%;">Line Item</td> <td style="text-align: center; width: 33%;">Efficiency</td> <td style="text-align: center; width: 33%;">Effectiveness</td> </tr> <tr> <td style="text-align: center;">$Con^{1(exp)}$</td> <td style="text-align: center;">$\frac{Con^{1(max)} - R^l_{cond}}{Con^{1(exp)} \downarrow}$</td> <td style="text-align: center;">$\frac{Con^{1(max)} - R^l_{cond}}{Con^{1(exp)} \downarrow}$</td> </tr> <tr> <td></td> <td style="text-align: center;">$\\$, time$</td> <td></td> </tr> </table>	Line Item	Efficiency	Effectiveness	$Con^{1(exp)}$	$\frac{Con^{1(max)} - R^l_{cond}}{Con^{1(exp)} \downarrow}$	$\frac{Con^{1(max)} - R^l_{cond}}{Con^{1(exp)} \downarrow}$		$\$, time$	
Line Item	Efficiency	Effectiveness								
$Con^{1(exp)}$	$\frac{Con^{1(max)} - R^l_{cond}}{Con^{1(exp)} \downarrow}$	$\frac{Con^{1(max)} - R^l_{cond}}{Con^{1(exp)} \downarrow}$								
	$\$, time$									

Figure 7. Logic model, resilience activities (consequence reduction) - NETWORK EFFECTS

Key:

$Con^{1(exp)} \downarrow =$ **expected supply chain** economic loss theoretically avoided (by resilience activities)

$\frac{R^l_{cond} \downarrow}{Con^{1(exp)} \downarrow} \$, time =$ **supply chain** lost productivity avoided given resilience activities, accounting for probability of attack, divided by resource inputs (time and/or money)

$R^l_{cond} \downarrow \downarrow_{Con^{1(exp)} \downarrow} =$ **supply chain** lost productivity avoided, irrespective of resource inputs

$Con^{1(exp)} =$ residual **supply chain** economic productivity (after resilience activities executed)

$\frac{Con^{l(max)} - R_{cond}^l}{\$, time} \Big|_{Con^{l(exp) \downarrow}}$ = residual **supply chain** productivity, accounting for probability of attack, divided by resource inputs (time and/or money)

$Con^{l(max)} - R_{cond}^l \Big|_{Con^{l(exp) \downarrow}}$ = residual **supply chain** productivity, irrespective of resource inputs

Tracking Expenditures – Issues Specific to C-reducing Activities

As with vulnerability reduction efforts, the inputs to achieve consequence reduction, if applied only at certain infrastructure in a network, must be considered relative to the proportional effect of those reduction efforts. More specifically, if port security grants increase resilience by lowering expected economic loss at supplier nodes (for example, in a port), but the supply chain network is composed of downstream nodes with high organic failure susceptibility, the efforts to increase port facility resilience may have a minimal effect on overall supply chain resilience. If much effort is expended to administer port security grants, that may not be an ideal return on investment. However, efficiency metrics may not be the prevailing budgetary theory preference.

About the Authors

Eric F. Taquechel is a U.S. Coast Guard officer with experience in shipboard operations, port operations, critical infrastructure risk analysis, contingency planning/force readiness, operations analysis, planning, programming, budgeting, and execution process support. He has authored and co-authored various publications on risk, resilience, and deterrence in HSAJ, the Journal of Homeland Security and Emergency Management, and IEEE. Most recently he and a coauthor published “A Right-Brained Approach to Critical Infrastructure Protection Theory in Support of Strategy and Education: Deterrence, Networks, and Antifragility”, which was selected as a Best Paper presented at the CHDS’s 2017 University-Academic Partnership Initiative’s 10th Annual Homeland Defense and Security Education Summit. Taquechel has taught courses on critical infrastructure protection and is a FEMA Master Exercise Practitioner. He holds a MPA from Old Dominion University, a master’s degree in Security Studies from the Naval Postgraduate School, and a BS from the U.S. Coast Guard Academy. Taquechel (corresponding author) may be contacted at etaqu001@odu.edu.

Dr. Marina Saitgalina is an Assistant Professor at the School of Public Service at Old Dominion University. Previously, she was an Assistant Professor at Oakland University, Michigan. Her areas of research include public administration, nonprofit management, nonprofit-government collaborations, and emergency management. She has multiple publications on such topics as nonprofit collaborations and institutional theories, and public management in emergencies in Public Management Review, Administration & Society, and Journal of Public and Nonprofit Affairs among others. She holds her MPA degree from the Academy of Public Administration in Russia, and a Ph.D. in Public Administration and Management from University of North Texas. Saitgalina may be contacted at msaitgal@odu.edu.

Acknowledgements

The authors wish to thank the referees who helped improve the quality of this work.

Disclaimer

The original opinions and recommendations in this work are those of the authors and are not intended to reflect the positions or policies of any government agency.

Notes

- 1 Carolyn J. Heinrich, "Outcomes-Based Performance Management in the Public Sector: Implications for Government Accountability and Effectiveness," *Public Administration Review* 62(2002): 712-725.
- 2 Theodore H. Poister, Obed Q. Pasha, and Lauren H. Edwards, "Does Performance Management Lead to Better Outcomes? Evidence from the U.S. Public Transit Industry," *Public Administration Review* 73(2013): 625-636.
- 3 U. S. Department of Homeland Security, *DHS Risk Lexicon* (2010), <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>, Web accessed March 26, 2018.
- 4 Ibid.
- 5 Ibid.
- 6 Theodore H. Poister, Obed Q. Pasha, and Lauren H. Edwards, "Does Performance Management Lead to Better Outcomes? Evidence from the U.S. Public Transit Industry," 625-636.
- 7 Janet V. Denhardt and Robert B. Denhardt, *The New Public Service: Serving, Not Steering* (4th ed.) (New York: Routledge, 2015).
- 8 Kathryn Newcomer and Sharon Caudle, "Public Performance Management Systems: Embedding Practices for Improved Success," *Public Performance & Management Review* 35(2011): 108-132.
- 9 Yilin Hou, "Budgeting for Fiscal Stability over the Business Cycle: A Countercyclical Fiscal Policy and the Multiyear Perspective on Budgeting," *Public Administration Review* 66(2006): 730-741.
- 10 Allen Schick, "The Road to PPB: The Stages of Budget Reform," *Public Administration Review* 26(1966): 243-258.
- 11 Yilin Hou, "Budgeting for Fiscal Stability over the Business Cycle: A Countercyclical Fiscal Policy and the Multiyear Perspective on Budgeting."
- 12 Ibid.
- 13 Department of Homeland Security. Performance Budget Overview, FY2006 Congressional Budget Justification, https://www.dhs.gov/xlibrary/assets/Budget_PBO_FY2006.pdf, Web accessed May 30, 2018.
- 14 Kathryn Newcomer and Sharon Caudle, "Public Performance Management Systems: Embedding Practices for Improved Success."
- 15 Thomas M. Rabovsky, "Using Data to Manage for Performance at Public Universities," *Public Administration Review* 74(2014): 260-272.
- 16 John A. McLaughlin and Gretchen B. Jordan, "Logic Models: A Tool for Telling your Program's Performance Story," *Evaluation and Program Planning* 22(1999): 65-72.
- 17 Victoria A. Greenfield, Valeria L. Williams, and Elisa Eiseman, "Using Logic Models for Strategic Planning and Evaluation: Application to the National Center for Injury Prevention and Control," RAND report (2006), https://www.rand.org/pubs/technical_reports/TR370.html, Web accessed March 26, 2018.
- 18 Victoria A. Greenfield, Valeria L. Williams, and Elisa Eiseman, "Using Logic Models for Strategic Planning and Evaluation: Application to the National Center for Injury Prevention and Control," RAND report (2006), https://www.rand.org/pubs/technical_reports/TR370.html, Web accessed March 26, 2018.
- 19 See: Eric F. Tauechel, "Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction," *IEEE Magazine* 24(2010): 30-35; Eric F. Tauechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8(August 2012), <https://www.hsaj.org/articles/226>. Web accessed March 26, 2018; Eric F. Tauechel, "Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program," *Journal of Homeland Security and Emergency*

Management 10(2013): 521-554; Eric F. Tauechel, Ian Hollan, and Ted G. Lewis, "Measuring the Deterrence Value of Securing Maritime Supply Chains against WMD Transfer and Measuring Subsequent WMD Risk Reduction," *Homeland Security Affairs* 11(February 2015), <https://www.hsaj.org/articles/1304>, Web accessed March 26, 2018;

Eric F. Tauechel and Ted G. Lewis, "More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases," *Homeland Security Affairs* 12(September 2016), <https://www.hsaj.org/articles/12007>, Web accessed March 26, 2018.

20 See: David L. Alderson, Gerald G. Brown, Matt Carlyle, and R. Kevin Wood, "Solving Defender-Attacker-Defender Models for Infrastructure Defense," *Proceedings of the 12th INFORMS Computing Society Conference: Research, Computing, and Homeland Defense* (2011): 28-49; Louis A. Cox, "Some Limitations of "Risk=Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks," *Risk Analysis* 28(2008): 1749-1761; Nikhil S. Dighe, Jun Zhuang, and Vicki M. Bier, "Secrecy in Defensive Allocations as a Strategy for Achieving more Cost Effective Deterrence," *International Journal of Performability Engineering* 5 (2009): 31- 43; Erik Jenelius, Jonas Westin, and Åke J. Holmgren, "Critical Infrastructure Protection under Imperfect Attacker Perception," *International Journal of Critical Infrastructure Protection* 3 (2010): 16-26; Jerome Kahan, Andrew Allen, and Justin George, "An Operational Framework for Resilience," *Journal of Homeland Security and Emergency Management* 6(2009): 1-47; Richard N. Lebow and Janet G. Stein, "Rational Deterrence Theory: I Think, Therefore I Deter," *World Politics* 41 (1989): 208–224; Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, NJ: Wiley Interscience, 2006); Ted G. Lewis, *Network Science: Theory and Applications* (Hoboken, NJ: Wiley Interscience, 2009); Andrew R. Morral and Brian A. Jackson, "Understanding the Role of Deterrence in Counterterrorism Security," RAND Occasional Paper (2009), http://www.rand.org/pubs/occasional_papers/OP281.html Web accessed March 26, 2018; Eric D. Vugrin, Drake E. Warren, Mark A. Ehlen, & R. Chris Camphouse. "A Framework for Assessing the Resilience of Infrastructure and Economic Systems," in *Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering*, eds. Kasthurirangan Gopalakrishnan and Srinivas Peeta (New York: Springer, 2010), 77–116.

21 P. Cronin and A. Cronin, *Challenging Deterrence: Strategic Stability in the Twenty-First Century*, Changing Character of War Series, (Oxford: Oxford University Press, 2007), http://ccw.modhist.ox.ac.uk/events/archives/mt06_deterrence/deterrence_report_mt2006.pdf, Web accessed March 7, 2010.

22 U. S. Department of Homeland Security, *DHS Risk Lexicon* (2010), <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>, Web accessed March 26, 2018.

23 Eric F. Tauechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8(August 2012), <https://www.hsaj.org/articles/226>, Web accessed March 26, 2018.

24 Scott Savitz, Miriam Matthews, and Sarah Weiland, *Assessing Impact to Inform Decisions: A Toolkit on Measures for Policymakers*. RAND report (2017), <https://www.rand.org/pubs/tools/TL263.html>, Web accessed March 26, 2018.

25 Laurie M. Anderson et al., "Using Logic Models to Capture Complexity in Systematic Reviews," *Research Synthesis Methods* 2(2011): 33-42.

26 Patricia J. Rogers, "Using Programme Theory to Evaluate Complicated and Complex Aspects of Interventions," *Evaluation* 14(2008): 29-48.

27 Ibid.

28 U. S. Department of Homeland Security, *DHS Risk Lexicon* (2010), <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>, Web accessed March 26, 2018.

29 Ted G. Lewis, *Network Science: Theory and Applications*.

30 Daniel Henstra, "Evaluating Local Government Emergency Management Programs: What Framework Should Public Managers Adopt?" *Public Administration Review* 70(2010): 236-246.

31 Susan Cutter, Christopher Burton, Christopher Emrich, "Disaster Resilience Indicators for Benchmarking Baseline Conditions," *Journal of Homeland Security and Emergency Management* 7(2010): 1-22.

- 32** Sue C. Funnell and Patricia J. Rogers, *Purposeful Program Theory: Effective Use of Theories of Change and Logic Models* (San Francisco: Jossey-Bass, 2011).
- 33** Anthony A. Braga and Brenda J. Bond, "Policing Crime and Disorder Hot Spots: A Randomized Controlled Trial," *Criminology* 46(2008): 577-607.
- 34** Astrid Brousselle and Francois Champagne, "Program Theory Evaluation: Logic Analysis," *Evaluation and Program Planning* 34(2011): 69-78.
- 35** Anthony A. Braga and Brenda J. Bond, "Policing Crime and Disorder Hot Spots: A Randomized Controlled Trial," *Criminology* 46(2008): 577-607.
- 36** Sean Nicholson-Crotty, Nick A. Theobald, Jill Nicholson-Crotty, "Disparate Measures: Public Managers and Performance-Measurement Strategies," *Public Administration Review* 66(2006): 101-113.
- 37** Bilal M. Ayyub, "Systems Resilience for Multihazard Environments: Definition, Metrics and Valuation for Decision Making," *Risk Analysis* 34(2014): 340-355.
- 38** Ralph L. Keeney and Detlof Von Winterfeldt, "A Value Model for Evaluating Homeland Security Decisions," *Risk Analysis* 31(2011): 1470-1487.
- 39** Ibid.
- 40** Holly Hilliard, Gregory S. Parnell, and Edward A. Pohl, "Evaluating the Effectiveness of the GNDA using Multi-Objective Decision Analysis," *Systems Engineering* 18(2015): 441-452.
- 41** Ibid.
- 42** Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk."
- 43** Victoria A. Greenfield, Valeria L. Williams, and Elisa Eiseman, "Using Logic Models for Strategic Planning and Evaluation: Application to the National Center for Injury Prevention and Control."
- 44** Ibid.
- 45** Sharon Caudle, "Homeland Security: Approaches to Results Management," *Public Performance & Management Review* 28(2005): 352-375.
- 46** Sean Nicholson-Crotty, Nick A. Theobald, Jill Nicholson-Crotty, "Disparate Measures: Public Managers and Performance-Measurement Strategies."
- 47** Suresh Cuganesan and David Lacey, "Developments in Public Sector Performance Measurement: A Project on Producing Return on Investment Metrics for Law Enforcement," *Financial Accountability & Management* 27(2011): 458-479.
- 48** Robert D. Behn, "Why Measure Performance? Different Purposes Require Different Measures," *Public Administration Review* 63(2003): 586-606.
- 49** Ibid.
- 50** Victoria A. Greenfield, Valeria L. Williams, and Elisa Eiseman, "Using Logic Models for Strategic Planning and Evaluation: Application to the National Center for Injury Prevention and Control."
- 51** Scott Savitz, et al., *Enhancing U.S. Coast Guard Metrics*, RAND report, 2015), https://www.rand.org/pubs/research_reports/RR1173.readonline.html, Web accessed March 26, 2018.
- 52** Sharon Caudle, "Homeland Security: Approaches to Results Management," *Public Performance & Management Review* 28(2005): 352-375.
- 53** Allen Schick, "The Road to PPB: The Stages of Budget Reform."
- 54** Carolyn J. Heinrich, "Outcomes-Based Performance Management in the Public Sector: Implications for Government Accountability and Effectiveness," *Public Administration Review* 62(2002): 712-725.

- 55** Sharon Caudle, "Homeland Security: Approaches to Results Management."
- 56** James C. Collins, *Good to Great and the Social Sectors: A Monograph to Accompany Good to Great*. (Harper: New York, 2005).
- 57** Verne B. Lewis, "Toward a Theory of Budgeting," *Public Administration Review* 12(1952): 42-54.
- 58** Ibid.
- 59** Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk."
- 60** Eric F. Taquechel, "Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction."

Copyright © 2018 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

The background of the cover is a dramatic painting. The upper portion shows a dark, stormy sky with a blueish-grey hue. Below, a large, multi-masted sailing ship is engulfed in intense orange and yellow flames, with thick black smoke billowing upwards. In the foreground, a small, dark wooden rowing boat is filled with several figures, some appearing to be in a state of panic or distress. The water is dark and turbulent, reflecting the fire and the dark sky. The overall mood is one of chaos and tragedy.

Causes & Explanations of Suicide Terrorism: A Systematic Review

By Vanessa Harmon, Edin Mujkic, Catherine Kaukinen, & Henriikka Weir

Abstract

The frequency of suicide terrorist attacks has increased dramatically since the year 2000, creating a renewed interest in this area of study, as well as an increase in the importance of understanding individual and organizational motivations behind engagement in suicide terrorism. The following is a systematic review of current research in the field of causes and explanations of suicide terrorism, limited to research articles in peer-reviewed journals and grey literature, excluding published books by single authors. This essay provides a brief background into the issues surrounding suicide terrorism and the evidence currently available concerning causes and motivations. It describes the strengths and limitations of currently available academic research and the conclusions that this literature presents both in terms of policy and future research efforts.

Suggested Citation

Harmon, Vanessa, Edin Mujkic, Catherine Kaukinen, and Henriikka Weir. "Causes and Explanations of Suicide Terrorism: A Systematic Review." *Homeland Security Affairs* 14, Article 9 (December 2018). <https://www.hsaj.org/articles/14749>

Introduction

The terrorist attacks of September 11, 2001 were not the first time a terrorist organization used suicide terrorism to achieve their objectives. Instances of suicide tactics are evident throughout history. As early as 400 B.C.E., Greek sailors set ships on fire and steered them into enemy forces, a tactic that has become so common throughout history that it inspired the coining of the term 'fireship.'¹ Another example includes suicide attacks executed by the Islamic Order of Assassins during the early Christian Crusades.² Modern history has been no less influenced by the use of suicide tactics, the most well-known example being the Japanese Kamikaze pilots of World War II. Despite the wide variety of tactics each individual suicide attacker employed, one notable similarity can be discerned: suicide tactics tend to be used when a weaker force believes that less drastic measures will be ineffective against a materialistically superior opponent.³ The origins of modern suicide terrorism can also be linked to this asymmetry between opposing forces. It was not until the 1980s that the world experienced suicide terrorism in its modern form. The first major contemporary suicide terrorist attacks were the 1981 bombing of the Iraqi embassy in Beirut, and Hezbollah's attack on the American Marine barracks in Lebanon.⁴ The apparent success of suicide tactics, especially against a force of significantly superior numbers, provides the basis for the strategic argument as explanation of suicide terrorism's evolution. The strategic approach, however, is only one of the many proposed causal explanations that researchers have considered.

This article explores research on the various explanations and causes for suicide terrorism that have been proposed in recent academic literature. Although modern suicide terrorism has been a threat since the 1980s, there was limited research conducted prior to 2000 that differentiated suicide terrorism from terrorism in general.⁵ The study of suicide terrorism specifically has been concentrated primarily in the years following 2000.

The purpose of this study is to conduct a comprehensive systematic review of current research on the causes and explanations of suicide terrorism. This systematic review will contribute to the progression of future research and the development of effective policy. The adoption of counterterrorism policy based on perceived causes can have limited impact if research has not substantiated those perceptions. Understanding the intricate interactions between different causal factors and determining promising research directions will prompt renewed focus in areas that can have the greatest impact on policy development and identification of potential courses of action to limit the risk of future attacks. This review will contribute to the field of suicide terrorism research by providing a comprehensive overview of current literature and the way ahead.

Background

Terrorist violence is employed to convey a message to whichever target audience has been identified by the organization responsible. The violence and randomness of the act instills fear even in those not directly affected and directs attention to the cause.⁶ Often perpetrated against unarmed civilians, suicide terrorism creates a sense of horror and fragility throughout the affected society. The dawn of contemporary suicide terrorism was not that long ago. However, the prevalence, tactics, and perceptions of terrorists and terrorism have changed and evolved continually. Since the beginning of modern suicide terrorism in the 1980s, counterterrorism analysts have anticipated gradual adaptation and an increase in events as terrorists become more familiar and more comfortable with these tactics. Contrary to this expectation, suicide terrorism has not undergone a gradual increase in popularity among terrorist strategists. There were more suicide attacks worldwide from 2003 to 2005 than there were in the entire preceding quarter century.⁷ Both researchers and policy makers alike have noticed this spike in the use of suicide attacks by terrorists worldwide. The Chicago Project's Suicide Attack Database has shown this striking observation, demonstrating the astounding shift in frequency of attacks beginning after 2001.

The systematic analysis of attacks from 2001 to 2014 illuminates the continued increase in the use of suicide attacks throughout the world. The progressive increase emphasizes the importance of understanding motivations behind suicide tactics. The slight decrease after 2007 could potentially be interpreted as progress in counterterrorism, but it is important to note that even in 2011, the low point in the last ten years, there were 254 attacks in one year, more than the 220 attacks over the 20 year stretch from 1982-2001.

History and Examples

The birth of the modern age of suicide terrorism in the 1980s marked a turning point from a fairly steady rate of suicide attacks as military tactics throughout history. Prior to the 1980s, suicide tactics had been integrated into military operations to create an advantage over an enemy of superior material strength. Whether through crashing a vessel into another ship to counter a rival's greater numbers or using suicide pilots in a surprise attack on enemy forces, some sacrifices create advantages for other allied combatants. Beginning in the 1980s, adaptive use of suicide-terrorist tactics and strategies allowed small, non-state and pseudo-state actors to achieve their objectives against larger, more formidable opponents, thus creating a perceived strategic advantage for suicide terrorism. The 1983 Marine Barracks Bombing in Beirut demonstrates the effect that a few willing to give their

lives can have against many. In this case only two truck bombs killed almost 300 American and French servicemen and injured many more; the sacrifice of only a few lives enabled the attackers to ensure the death of hundreds of their targets. In the next decades leading up to the turn of the century, suicide tactics were adopted and adapted by nationalist and extremist groups around the world.

The Chicago Project⁸ identifies more than 40 organizations that conducted suicide attacks between 1982 and 2013 as part of 25 separate campaigns.⁹ Between 1982 and 2000, the Liberation Tigers of Tamil Eelam (LTTE) were responsible for more suicide attacks than any other individual organization. They conducted 72 suicide terror attacks in their separatist campaign against Sri Lanka and India, resulting in more than 1000 deaths and 2500 injuries.¹⁰ Although members of the LTTE were among the most prolific suicide attackers of the time, they were not the only group to use the tactic. The Chicago Project identifies 174 suicide attacks and 2702 deaths that occurred during the 1980s and 1990s.¹¹ The majority of attacks were directed at security targets with only 17.2% of targets being civilian and 14.9% political. Often cited as the first terrorist organization to use suicide terrorism, Hezbollah launched a campaign against Israeli forces in Lebanon that is second only to the LTTE in terms of the number of suicide attacks initiated. Other Palestinian, Chechen, and Islamic militant groups also engaged in suicide terror as part of 10 separate campaigns during this time. The car bomb, first used by Hezbollah in the 1981 Iraqi Embassy bombing in Beirut, and the belt bomb, invented and perfected by the LTTE, monopolized suicide terror tactics as the weapon of choice until 2001.¹²

The turn of the century saw an even greater increase than that observed in the 1980s and the use of suicide terrorist attacks spiked. There were more suicide attacks between 2001 and 2005 than in the thirty years prior. Analysts have largely attributed this spike to the Palestinian-Israeli conflict and the de-Baathification of the Iraqi government in conjunction with the disbanding of the Iraqi security forces in 2003. Between 2000 and 2014, Iraq was first in the number of suicide attacks by location, with Israel coming in fifth.¹³ Sissons and Al-Saiedi noted that de-Baathification largely contributed to the creation of the insurgency and the increase in violence that resulted. The disbanding of the Iraqi military left more than 700,000 armed and trained Iraqi security force members unemployed, disenfranchised and hostile towards the United States, now seen as occupiers in Iraq.¹⁴ Consequently, there was an increase in suicide-terror attacks beginning in Iraq in 2003. Although seven of the 35 attacks in 2003 occurred from February to April of that year, 80 percent occurred after the official de-Baathification orders were issued.¹⁵ Despite the fact that United States military leadership had intended to employ the Iraqi security forces to help restore security and order in post-war Iraq, the reality of the de-Baathification orders left disbanded security forces with the perception of broken promises and betrayal by the U.S. forces.¹⁶ Given these sentiments, it was not surprising to see increased hostilities and the development of the insurgency within Iraq.

The phrase 'one person's terrorist is another person's freedom fighter' epitomizes many of the explanations for this spike in suicide terror. Several explanations for suicide tactics that focus on the fact that a suicide attack can be an effective asymmetrical tactic against hardened targets provide some insight into why those who see themselves as freedom fighters may engage in these activities. The attacks on the World Trade Center and the Pentagon in 2001 demonstrated the potential effectiveness of these tactics to prospective future attackers.

The attacks of September 11, 2001 prompted not only an increase in the use of suicide attacks as a terrorist tactic but also a greater international impact for this approach. In the aftermath of September 11, the NATO Alliance invoked, for the first time, Article Five of the Washington Treaty, which states that an armed attack against one of its members is an attack against them all.¹⁷ Not only is the international response more elaborate now than in the 20th century, but travel, media, and technology have changed the attacks themselves, beginning a new phenomenon that some researchers call the “globalization of martyrdom.”¹⁸ Islamic extremist suicide attacks have reached countries all over the world, establishing the perception that suicide terror is a predominantly Islamic activity, and giving many the impression that religion is a causal factor in the activity itself. Even in Muslim countries, this perception seems to be verified. During the wars in Iraq and Afghanistan there was an average of one suicide attack per day.¹⁹ Although Western governments will argue justifiably that Islamic militant groups are a principal threat in today’s security environment, it is important to recognize that it is only recently that Islamic militant groups have surpassed other terrorist organizations as the leading perpetrator of suicide terror and that they are not the only terrorists to engage in suicide attacks.

Between 2001 to 2014, 3,802 attacks occurred resulting in 37,562 deaths and 96,644 injuries.²⁰ The largest number of attacks in a single year occurred in 2007 and while the majority of targets remain security-oriented, a greater percentage of civilian targets have been selected.²¹ As was the case during the previous 20 years, car-bombs and belt-bombs monopolize the weapon selection. However, September 11, 2001 established the hijacked airplane as the deadliest suicide-attack weapon. Although these statistics are somewhat staggering and the various definitions used by individual researchers show slight variations in reported numbers, the trends remain the same and the notable spike in attacks after 2001 is universally acknowledged among subject matter-experts.²² It is also important to recognize that, although suicide attacks make up a small percentage of terrorist attacks around the world, the importance of understanding their impact cannot be underestimated. Suicide attacks make up only three percent of terrorist attacks, but are responsible for 48 percent of the fatalities as a result of terrorism.²³ This statistic proves that although suicide terrorist attacks account for only a small percentage of all terrorism, this tactic has some of the most detrimental and fatal effects. Therefore the influence and power of suicide terrorism need to be considered in order to better understand terrorist motivations and to progress toward effective preventative programs.

This essay provides a systematic review of academic peer-reviewed research in the area of causes of suicide terrorism. Several researchers have conducted literature reviews in the area of suicide terrorism. Martha Crenshaw analyzed 13 different books on the subject written by current leading experts in the field, comparing theories, perspectives, and policy suggestions.²⁴ Grimland, Apter, and Kerkhof conducted a review of currently available research to build on our understanding of psychological perspectives and their importance.²⁵ For the most part, previous reviews, critiques, and studies have focused on a single causal theory, a single work, or on validating a model of interconnectivity among theories.²⁶ This paper uses a systematic review to compile existing research in a comprehensive and straightforward manner to demonstrate where modern research stands and the potential for developing more effective counter-terrorism approaches.

Method

Progress is made continually in a variety of disciplines of academic research. More than two million articles are published in academic journals every year.²⁷ Even with an extremely narrow focus, it is difficult to stay apprised of all the developments in the literature over time. A systematic review is designed to help organize and assess current research in a specific area in order to address limitations associated with current literature. It is an in-depth literature review that locates, appraises and synthesizes available research relating to an explicit research area.²⁸ A systematic review should provide evidence-based answers that help to change practices or improve policies. By following a systematic methodological process and by explicitly explaining this process, the review can provide a comprehensive examination of research associated with the topic area and be reproducible by others in the future, providing the greatest advantage to the field of research.²⁹ Systematic reviews cover both published academic journal articles and 'grey literature'. Grey literature encompasses unpublished studies or studies with limited distribution including research reports from government agencies, reports from scientific research groups, working papers, doctoral dissertations, and conference proceedings, to help avoid publication bias.³⁰ Articles and research were collected from a variety of sources in order to amass the most representative sample of current literature available. Research was drawn from search engines such as Google Scholar, Air University Library's Index to Military Periodicals, Bielefeld Academic Search Engine, Directory of Open Access Journals, JSTOR, and PubPsych. This essay is supported by credible sources in combination with varied perspectives and media, through which information was gathered to develop an objective, well-researched systematic review.

Key words in research included: "causes of suicide terrorism," "religion and suicide terrorism," "social influence in suicide terrorism," "psychology and suicide terrorism," "suicide terror," "logic of suicide terrorism," and "strategy and suicide terrorism." Accommodating for different terminology, similar keywords were researched replacing "suicide terror" with "martyrdom." Articles were found through the previously-mentioned search engines as well as the reference sections of applicable articles, and were reviewed to ensure that the greatest amount of applicable information was analyzed. It should be noted that only articles written in English were considered for this systematic review.

Selection Criteria

To be included, research was required to differentiate between suicide and non-suicide terrorism. It was required to address root causes of suicide terrorism and/or explanations of suicide-terrorist activities. This may have been done through a description of preventative or responsive programs on the condition that they address a specific element believed by the author(s) to contribute to suicide terrorism. Research was limited to peer-reviewed articles and grey literature. Books written by subject-matter experts were also considered for information that was presented throughout the paper, but not in the analysis tables.

Resources Excluded

The research included peer-reviewed journal articles and grey literature (there is a dissertation included for example). It does not include reviews of published books on

the causes of suicide terrorism. An exception to this is made for chapters of edited books written by multiple authors. There are several experts in this field who have published books on the topic, and further investigation into this material would benefit future reviews of this nature. Many researchers also included newspaper and magazine articles written by subject-matter experts among their sources. This research excluded these articles due to the type of publication. However, given the popularity of the subject matter in recent years, a significant number of articles fall in to this category. Because of the subject-matter expertise of their authors, these articles, although not peer-reviewed, can provide more information on the state of research in this field and potentially significant details that could be useful in subsequent research.

Throughout the course of research, several books by subject-matter experts were found that went into great detail about the potential causes of suicide terrorism. As this systematic review focused on peer-reviewed articles, these books were excluded from the systematic review. We also found some articles that critiqued and compared the aforementioned books. Some of these articles were also excluded from the systematic review as they did not present a potential cause for suicide terrorism, but instead discussed the strengths and weaknesses of previous research. The arguments of these articles are extremely useful to the development of future research but were outside the scope of this review. Finally, any articles that did not distinguish in their research between suicide terrorism and terrorism in general were excluded. It remains a topic of debate as to whether suicide terrorism should be considered a separate form of terrorism, but for the purposes of this review, suicide terrorism was assumed to be a unique form of terrorism deserving of independent research.

The authors compiled the list of articles that were included in this systematic review. The table is organized by year to highlight the growing interest that researchers took in determining the causes of suicide terrorism after 2000. This may have been a direct result of increased interest and visibility of the new threat of suicide bombers after the attacks of September 11, 2001 or a reflection of the financial support provided to research in this field following a realization of the vulnerability of powerful governments to the tactic. A total of 47 articles were found that analyzed the causes and motivations of suicide terrorism and ranged in focus from individual-level motivations to social forces to organizational strategies. The table that describes research articles that were found during the course of the data collection process but were excluded from the review is included in this essay as Appendix A. It explains briefly the purpose of each article and why it was not applicable to this systematic review. For reasons outlined above, books written by a single author are not described.

Results

After noting the spike in suicide terrorism incidents, it is not difficult to explain the corresponding increase in the interest that researchers have paid to suicide terrorism research. Much of the research available concerning modern day suicide terrorism has been published since 2001 with a significant amount of focus on Islamic Jihadists and religious extremism. This may be a result of the world's current perception of Islamic terrorist groups as a significant threat to Western societies and subsequent funding increases or it may simply be due to the recent increase in Islamic extremist violence, providing significantly more data to be analyzed in this area. Many researchers recognize this as a limiting factor to

the understanding of suicide terrorism. Some researchers continue to focus on the rise of Islamism as a contributory factor behind the increase in incidents. In contrast, others take varying approaches to determine the root causes of suicide terrorism in order to explain the use of suicide tactics by Jihadist and non-Jihadist movements alike. Studies in this area are difficult as suicide terrorism represents a relatively small portion of global terrorist attacks, an estimated 2.16%, and therefore most research does not differentiate between causes of non-suicide and suicide terrorism.³¹ Despite restrictions, researchers have made continual efforts towards understanding terrorism in general, and furthermore, understanding suicide terrorism as a distinct practice.

Theorized Causes of Suicide Terrorism

One cannot deny that suicide terrorism is often perceived as successful in achieving the immediate objectives of the terrorist organization. Following the Marine Barracks Bombing in Lebanon in 1983, President Reagan ordered the withdrawal of American troops within four months.³² This is one of many examples of the perceived success of suicide attacks that support the strategic argument for suicide terrorism. Considering the ratio of terrorists killed to their enemy victims often associated with suicide terrorism, the justification for this tactic against a superior combatant force is clear. Pape notes a correlation in his research between foreign military occupation and an increase in suicide terrorist activity that lends itself to this school of thought.³³ This approach is closely related to the theory that organizational and institutional motivations are the most contributory elements to suicide terrorism. Where the former approach argues that the strategic effects of suicide terrorism justify these actions, the latter relies on the views of those within the organization or institution to agree with this argument. Atran goes so far as to suggest that changing the institutionally-held morals and values of terrorist cells is essential to changing the prevalence of the practice itself.³⁴

Propaganda that draws people to the group begins with the morals and values of the individual citizens within a society. Convincing the population of the moral logic of martyrdom is the first step to recruiting new members and justifying the actions of the group to their civilian supporters. Conversely, changing this perception could very well be the first and most important step away from suicide terrorism and terrorism in general.³⁵ The influence of society is, therefore, essential to not only the success of a suicide attack, but also to the initial perpetration of that attack. One popular theory suggests that the government regime will influence whether a nation falls victim to perpetrators of a suicide attack; however, several researchers have found that government type is irrelevant in this scenario.³⁶ Additionally, Piazza does suggest that regime type was related to the perpetration of suicide attacks.³⁷ Other societal elements such as economy, education, religion and culture have also been included in theories about the causes of suicide terrorism.³⁸ While environmental and societal influences would provide a more manageable explanation in terms of preventative and responsive programs, there is also the possibility that individual factors are more important to suicide terrorism than these more convenient elements. Even if they are not among the most significant causal factors, understanding psychological aspects of those who perpetrate suicide attacks can help society to counter them. Post, Ali, Henderson, Shanfield, Victoroff, and Weine suggest that psychological aspects of individual terrorists will make them more or less likely to engage in suicide terrorism with emphasis on collective identity and social psychology.³⁹ This perspective, even if it concerns an individual, once again relates back to societal influences.

It is important to note this interconnectivity of causes. As is the case in the study of the causes of crime, there are many potentially influential causal factors related to suicide terrorism. A better understanding of all contributing factors, as well as the relationships among the factors, governments, and law enforcement, will enable the global community to address properly the rising phenomenon of suicidal terrorism.

The articles analyzed are used to identify the root causes of suicide terrorism specified in the literature. The data are grouped by the theorized cause that an individual author proposes. Although each theory varies slightly from others in the same group, theorized causes can be broadly limited to four categories: individual-level motivations, organizational-level motivations, theories of societal influence, and some combination of those three approaches. Tables that contain summaries of reviewed articles by theory are provided in Appendices B, C, and D of this essay.

Individual-Level Motivations

The desire to understand why and how individuals can decide to sacrifice themselves to kill others is natural. For many this mentality is unfathomable. Whether one has been personally influenced by an attack or one has witnessed the effects of suicide terrorism from afar, it is difficult for observers to comprehend how someone can be so dedicated to violence against others that they are willing to make that ultimate sacrifice. Individual-level theories stem from an effort to understand the individuals that engage in suicide missions. Many of the early theories employed to explain the motivations of suicide terrorists focused on the individual level, including nine of the articles analyzed in this systematic review. It is now generally acknowledged that there is not necessarily a psychological profile of those who are willing to commit what many people, cultures and religions consider to be a grave sin. The Committee of the Psychological Roots of Terrorism for the Madrid Summit on Terrorism, Security and Democracy in 2005 explicitly stated that individual-level theories that suggest a psychological abnormality of the attacker are incapable of explaining the phenomenon.⁴⁰ This perception has not hindered research in the area of individual-level motivations, although many theories now incorporate various levels, as will be discussed in a later section.

A common question among researchers is whether suicide terrorists can be categorized as suicidal.⁴¹ Pedahzur, Perliger, and Weinberg acknowledge what others have noticed as well, that suicide terrorists do not exhibit common characteristics of individuals bent on suicide.⁴² They suggest instead that suicide terrorists fall into a new category of suicide typology, that of fatalistic-altruistic suicides and define this typology as individuals who fit into both Durkheim's altruistic and fatalistic typologies of suicide behavior. In this case the individual sees their suicide as a duty to the group (altruistic) and has suffered from long-term political and economic oppression and has no hope for their future (fatalistic). Kimhi and Even take a slightly different approach, arguing that there is not one single profile, but that suicide bombers can be grouped into four typologies: religious, exploited, retribution for suffering, and social/nationalist, where each is attributed different prerequisite and supporting factors.⁴³ This theory suggests that every case of suicide terrorism required a motivated individual, the technical system to carry out the attack, and a condoning political leader. Beyond these similarities, the different prerequisite factors and supporting factors associated with each typology range from religious interpretations encouraging terror to political awareness and belief that armed struggle and suicide missions are vital to national

liberation. Similarly, Orbach refers to prerequisite and supporting factors as ‘facilitators of suicide’ and suggests that these facilitators, combined with a sociological typology of the altruistic suicide, are at the root of suicide terrorism.⁴⁴

One thing is obvious: suicide terrorists do not exist in a vacuum but are consistently impacted by the world around them. Each of the individual-level theories acknowledge that events within society, family, and an individual’s life contribute to the ultimate decision to engage in suicide missions. The debate concerning what is the most influential factor remains undecided. Whether suicide terrorists are completely altruistic, sacrificing themselves for the benefit of future generations, whether they experienced some trauma earlier in life that led them on this course, or they are making a rational, tactical choice under a belief that they will succeed against a hardened target for the benefit of their organization, understanding each individual’s motivation is difficult. When one simply considers cultural and religious differences, it is easy to see where determining a single profile for the suicide terrorist may be impossible.⁴⁵ Jacques and Taylor examined suicide-terror attacks perpetrated by groups in the Middle East and Chechnya as well as Al Qaeda and the LTTE in an effort to determine common factors concerning suicide terror in general and found differences in motivations between men and women.⁴⁶ For women, motivations were often based on personal events, and recruitment was done through peer influence, exploitation and self-promotion. For men, motivations were based on religious and nationalistic ideologies and recruitment was done through peer influence, exploitation, self-promotion and religious persuasion.

The difficulty in determining a single individual profile brings us to theories that focus on organizational-level motivations.

Organizational-Level Motivations

Theories focusing solely on organizational-level motivations are far more rare than other level theories encompassing only five of the articles analyzed in this paper. The obvious influence that society and the individual’s organization have on the decisions of the individual lends credence to theories that stress combinations of influential factors. The idea that suicide terrorism is used as a tactic against a militarily-superior enemy has been discussed previously in various sections of this review and is an integral part of combination theories discussed in the next sections, but it has an especially important place in organizational-level theories. In her 1987 article, “Theories of Terrorism,” Crenshaw proposed that terrorism could be analyzed on two different levels, both of which are centered on the organizational level and remain applicable to theories of suicide terror. From one perspective, violence is employed by an organization to affect political change, and from the other, the purpose of the organization’s actions is simply to sustain the organization. Ayers suggests that suicide terrorism is used strategically by an organization to gain tactical advantage over the enemy and to aid in recruitment efforts.⁴⁷ Although both these strategic and promotional goals coincide with Crenshaw’s framework, the concept that suicide terrorism is nothing more than a rational, strategic weapon and cannot be attributed to any irrational influence is a difficult one to accept.⁴⁸ If emotion and personal choice play no part in the decision to engage in suicide missions, then efforts to create policy to counter suicide attacks become inconsequential. As long as there is strategic benefit to the attacks, this theory suggests that they will continue to be used. Pape agrees, suggesting that terrorism is employed for one of two reasons: to force government to change policy and/or to mobilize additional recruits and financial aid for the organization.⁴⁹ Suicide terrorism is the coercive instrument

of choice for terrorist groups simply because it is perceived that it works. Ergil conducted a study focusing on The Worker's Party of Kurdistan (PKK) and determined a somewhat more palatable organizational theory.⁵⁰ He suggests that group dynamics and the influence of an 'omnipotent' leader contribute to the use of suicide tactics by an organization and require a significant amount of coercion and force from leadership. This suggests at least that the removal of a fanatical leader can help to eliminate the possibility of suicide attacks from a particular organization.

Societal-Level Theories

In addition to organizational-level forces influencing the engagement of a particular group in suicide missions, many scholars have noted that while some groups are willing to use suicide tactics, other groups with similar ideologies and characteristics will refrain. Many analysts attribute this in large part to societal-level factors, and six of the articles analyzed below examine these societal influences. From conditioning and education to community support, theorists have been drawn to societal influences to explain both individual and group actions with respect to suicide terrorism. Upon analyzing the education system for Palestinian children between 1980 and 2000, Burdman found that literature, media, and educational faculty contributed to a conditioning campaign that infused children with the idea of becoming martyrs.⁵¹ An authoritarian society, religious and nationalist learning, educational techniques, group processes, programming and conditioning, indoctrination, and emotion all had significant and negative effects on the individual mental health of the children exposed to these influences. Learning from the earliest ages to see suicide terrorism as an honorable endeavor solidifies the notion for the rest of one's life, making it a cultural mentality and especially difficult to change. Although Burdman's study was limited to the Palestinian-Israeli conflict, this trend in societal and cultural marketing and belief can be seen in other areas as well.⁵² Post suggests that even second and third generation emigrants that are now joining the global Salafi jihad experience the feelings of loss and deprivation commonly attributed to causal theories of suicide terrorism.⁵³ In the case of the LTTE, suicide terrorism was framed in a light such that it was marketed as heroism. Ramasubramanian suggests that the fear of death, on a societal level, can motivate people to heroism.⁵⁴ With cultural beliefs that adhere to the martyrdom-equals-heroism concept, it is easier to understand how individuals would be influenced to engage in suicide-terror attacks.

The LTTE's fear of death, as Ramasubramanian refers to it, can be related to a cultural frustration that is noted by several researchers within the Palestinian population.⁵⁵ Khashan suggests that a combination of Palestinian collective frustration, Political Islam, and extreme poverty leads to the use of suicide terror as a tactic.⁵⁶ Although poverty has been disqualified as a causal factor in the number of suicide terror attacks, researchers have not disqualified the influence of poverty on individual and community stressors.⁵⁷ Benmelech, Berrebi, and Klor suggest that poor economic conditions, especially high unemployment, allow terrorist organizations to recruit better educated, more mature suicide terrorists to their cause and improve the quality of potential targets.⁵⁸

The current targeting of Western democratic countries by terrorist organizations, often originating from non-democratic nations, has led some researchers to analyze the question of whether regime type effects the likelihood of being targeted for suicide terrorism as well as the likelihood of producing suicide terrorists. Jackson, Wade and Reiter hypothesized

that democracies and especially mixed regimes would be more likely to experience suicide terrorism.⁵⁹ This hypothesis was not supported by their research. However, they did find nation size, Islam, and national and global experience with suicide terrorism to be correlated to suicide terrorism. The study found that regime type is uncorrelated with suicide terrorism but was marginally correlated to the number of religious minorities at risk within the nation. The society we live in and the culture that we grow up a part of have an astounding impact on our lives and how we interact with the rest of the world. These societal-level theories consider these impacts to be the root causes of suicide terrorism, however even more theories have emerged that consider them to be a significant part of the cause while maintaining the importance of individual and organizational influences to the process as well.

Combination Theories

The vast majority of theories in the last decade, along with some of the earliest studies, have suggested a combination of factors at the individual, organizational, and societal levels. In fact, 25 of the 45 articles take this combination approach. Often listed as one of the three pre-eminent studies of suicide terrorism causal theories, Merari's "The Readiness to Kill and Die: Suicidal Terrorism in the Middle East" posits that four distinct groups of factors influence an individual's decision to participate in a suicide terror attack: "cultural factors, indoctrination, situational factors, and personality factors."⁶⁰ He suggests that if the person is suicidal, the organization simply provides the excuse necessary to commit suicide. Although the idea that suicide terrorists are suicidal has been refuted by more recent research, the combination of individual, organizational, and societal-level forces to explain suicide terrorism is a lasting concept.⁶¹ Atran suggested that suicide terrorism was used as a weapon of psychological warfare against the greater population while putting strong emphasis on organizational and institutional roles in motivations.⁶² At the individual level, a combination of psychological and cultural elements makes individuals more susceptible to recruitment. Atran later argued that analyzing the individual terrorists and attempting to develop a profile of the suicide terrorist is inconsequential.⁶³ The focus should be placed on society's perception of global Jihad and the organizational and group dynamics of the greater terrorist networks but specifically of the cells involved in suicide terrorism. Similarly, Pape argues that a combination of strategic, social, and individual logic supports suicide terrorism as an effective form of terrorism; however, the strategic element unifies the others and ultimately enables the terrorists' agenda.⁶⁴

Berman and Laitin's theory of hardened targets coincides with the idea that strategic advantage is at the forefront of the motivation.⁶⁵ They argue that suicide terrorism is a rational decision; it incorporates an assessment that a successful attack on a hard, well-protected target that could withstand a conventional insurgency attack outweighs the cost of losing one member. Moghadam also agrees, arguing that a combination of individual and organizational-level motivations contributes to the use of suicide terror as a tactic.⁶⁶ At the individual level, several factors influence the potential suicide bomber, but they are not always the same combination of factors. At the organizational level, organizational goals and strategies are integrated in recruitment, training, and indoctrination to support the use of suicide terror as a tactic.

While some researchers place the greatest part of the motivation squarely with organizational strategy, others consider it to be only one element of the motivation behind a suicide attack.

Brym and Araj argue that often revenge and retaliation are among the most important elements at both an individual level and an organizational level.⁶⁷ Gill places emphasis on political and social psychology and group dynamics as the root causes of suicide terror.⁶⁸ Post, Ali, Henderson, Shanfield, Victoroff, and Weine argue that from a psychological perspective, collective identity and normality have the greatest bearing, but that economics, history, politics and anthropology contribute as well.⁶⁹ Pedahzur considers the organizational-level motivations and individual-level motivations to be of equal importance and developed a three-stage model for explaining suicide terrorism involving organizational leadership decision-making, individual motivations, and organizational recruitment, socialization, and employment.⁷⁰

Regardless of which level of motivation is considered most important to a specific researcher, the number of articles that follow this combination model demonstrates a new trend towards acknowledging the complicated and unique motivations for suicide terror.

Research Methods

Current research focused on explaining suicide terrorism has been largely conducted using three distinct methods: review and critique of other theories and research; psychological autopsies using interviews and open source data; and empirical analysis of data compiled on various suicide attacks. Table 1, located below, shows how many of the documents analyzed as part of this systematic review used each method. Most of the articles on the topic fall into the first category and take on a narrative form discussing the merits or limitations of other research.⁷¹ Commonly included in these narratives are models presented by Robert Pape, Mia Bloom, and David Laitin and Eli Berman.⁷² The second method, although far less common than the first, has significantly more potential to be able to analyze individual-level motivations. Psychological autopsies are interviews conducted with close family and friends and, for perpetrators of successful suicide missions, they are the closest thing to first-hand accounts that are available to researchers.⁷³ Although not without limitations, this method provides a unique approach to data collection. Some researchers took a different approach to the psychological autopsy, collecting their data from literature published about various attacks, attackers and the groups to which they belong.⁷⁴

The third method is characterized by researchers using various databases of suicide attacks to conduct empirical analysis on different aspects of each attack.⁷⁵ The variety of databases included Lexis Nexis' online database of world news media, Freedom House and Polity data, Israeli Security Agency's reports on Palestinian suicide terrorists that attacked or attempted to attack in Israel, the West Bank and the Gaza Strip, and the online database of the International Policy Institute for Counter-Terrorism (ITC) in Herzliya, Israel, among others.

In a few cases, the methods used did not fit neatly into any of the three aforementioned categories of methods. For instance, Azam uses literature on economics in conflict and economics of terrorism as well as other microeconomic theories in order to show changes to individual investment in suicide bombing as it relates to increased wealth and education.⁷⁶ Moghadam created a framework of analysis that examined the process of the suicide attack from initial motivation to execution at both the individual and organizational level and applied it to various theories of motivation for the bomber and aspects of the organization.⁷⁷ Gill used examples of various suicide attacks and the actions of suicide bombers to describe a common progression through the life of a suicide bomber in an effort to establish the

contributions of individual, group and societal factors to suicide terrorism.⁷⁸ Burdman reviewed 31 educational textbooks published prior to 2000 and used by the Palestinian Authority's Ministry of Education as well as various media programs and publications in order to analyze the conditioning of children in Palestine.⁷⁹ Each of these studies helped to improve the quality of research and the understanding that we have of the field of suicide terrorism in their own way.

Table 1: Types of Research Methods Used

Research Method	Number of Articles Using this Method
Review and Critique of other theories and research	21
Psychological Autopsies	2
Empirical analysis	14
Other (Including combinations of the above methods)	8

Limitations

Suicide terrorism is not a topic that is easily studied. Fortunately, suicide attacks constitute a very small percentage of terror attacks and insurgency efforts worldwide. The nature of suicide terrorism elicits limitations, especially concerning the current preoccupation with Islamic Jihadists and in developing adequate research methods.

Religious Extremist Focus

The focus on Islamic Jihadists in today's media and Western defense structure is a result of not only the recent increase in the use of suicide tactics by these groups but also the sheer magnitude of destruction resulting from the attacks of 9/11. Unfortunately, this preoccupation has been reflected unavoidably in academic research. Some would argue that this pre-occupation with Islamic Jihadist attacks is justified by the prevalence of such attacks in current statistics. In addition to Islamic jihadist attacks on Iraq and Afghanistan, individual articles also focus on the Palestinian-Israeli conflict, the LTTE and Chechen terrorists, as well as attacks that take place within oppressive regimes throughout the world.⁸⁰ Several articles focus specifically on Islamic militant groups and Middle Eastern suicide terrorism.⁸¹ The majority of research considers all suicide attacks in one dataset. While this seems the most effective way to diminish any potential bias towards the influence of religious extremism, the statistical difference between the number of attacks perpetrated by groups with no religious motivation and those with extreme religious views skews the available data. Researchers that have used global suicide terrorism within their dataset unfortunately have significantly more data for these groups. Interestingly, this may be a limitation, but few have indicated that religion is a cause for suicide terrorism. Many suggest that religion is helpful to an organization to recruit suicide terrorists and to justify their involvement in suicide attacks, but that religion is not significant as a causal factor.

The very nature of suicide terrorism does not lend itself to academic research. Researchers are limited in their potential methods by the success of a suicide attack. Some authors attempt to overcome this by conducting psychological autopsies as their primary data collection

method. However, the psychological autopsy is dependent on the memories, opinions and openness of the families and friends of the bombers. Others rely on statistical data surrounding the suicide attacks themselves, but this approach has the potential to ignore important individual-level elements. Interviewing failed bombers discounts the differences between these individuals and those that succeeded in carrying out their attack. Every individual research method has its limitations, but in the case of suicide terrorism, these limitations have so far hindered the academic community from establishing an accepted causal theory. The recent trend towards theories that suggest a combination of individual, organizational and societal influences has begun to incorporate the evidence presented by prior research suggesting that combining several different research methods may be a way to diminish the limitations of a single method and incorporate the combined evidence of the past.

Discussion

Academic research to explain the foundation of suicide terrorism has, in recent years, greatly expanded. Since the attacks of September 11, 2001, suicide terrorism has been at the forefront of both media attention and security concern all around the world. During development of any security policy, defense and government officials understand the need to address the root causes of the issue in order to develop effective and lasting response programs. Unfortunately, in the early days of modern suicide terrorism when causal research was limited, without accurate research, policy was developed based on perceived elements that have since proven to be less impactful than originally anticipated. Recent research has begun to improve our understanding of the root causes of suicide terrorism, but with the growing popularity of suicide terrorism as a terrorist-organizational tactic, there remains a need to continue expanding our knowledge in the area.

This systematic review revealed several important characteristics of current research. First, the vast majority of research in this subject consists of literature reviews and theories based on previous research, either research on suicide terrorism or research on related subjects such as suicide or terrorism in general. Causes of suicide terrorism are difficult to study by their very nature. The success of a mission requires the death of the attacker and leaves researchers with limited options for collecting data. They are restricted to after-the-fact data collection by the target state or interviews with attackers who failed or abandoned their mission, would be attackers, or family and friends, all of which may limit the applicability of their findings when applying them to successful attackers. Despite the difficulty that arises from the lack of available primary sources, there have been empirical studies conducted that make use of the data available. This type of research demonstrates the ability to conduct more robust and verifiable studies, which could benefit greatly our knowledge of causal factors.

Secondly, although earlier research considered individual elements of suicide terrorism as main contributing factors, more recent research has acknowledged the need for a multidimensional approach to both research and policy development. Both academics and policy makers have begun to see suicide terror as resulting from interacting factors at the individual, organizational, and societal levels. There may be one factor that has the greatest impact for an individual or an organization to engage in suicide terrorism, however, it is unlikely that this factor is the same in every situation. The most effective reactive and

preventative policies will address suicide terrorism from multiple directions in order to ensure the greatest level of applicability to the situation. This does not limit the value of understanding individual aspects of specific groups and societies. For instance, policies that attempt to address poverty, collective humiliation, religious fanaticism, and community support may be an effective combination of efforts within the Palestinian-Israeli conflict. In comparison, those that address exploitation, coerced participation and reciprocal violence may be more effective in situations similar to the LTTE's struggle against the Sri Lankan government.

Finally, several researchers have focused not on root causes but on the spread of suicide terrorism.⁸² This new global phenomenon has significantly increased the number of attacks as well as the number of states directly affected, whether as targets or as perpetrators. Developing effective policy will depend on addressing the root causes of suicide terrorism using a multidimensional approach, the spread of suicide terrorism on a national and international level, and the influence of the media in both of these areas. The power of media and propaganda in today's society is overwhelming and highly prominent in both of these areas. Without effective policy that addresses the media, other efforts have the potential to be significantly less effectual. Cooperative efforts to acquire a stronger understanding of the causes and characteristics of suicide-terrorist practices, as well as researchers' increased willingness to respond to progressive research using a multidimensional approach, will help develop further preventative programs to limit the risk of future attacks.

Limitations of Current Research

Given the inherent difficulty in studying suicide terrorism, it is not surprising to see the limitations of current research. However, researchers have been making progress in minimizing these limitations. Although suicide attacks constitute a very small percentage of terror attacks and insurgency efforts worldwide, their increasing frequency and their lethality are generating greater interest among academics, governments, and the civilian population. It is important not to let the current preoccupation with Islamic Jihadists create tunnel vision and a subsequent void in research that is generalizable to other groups. It is also essential to remember that current evidence suggests that while religion may be helpful to an organization to recruit suicide terrorists and justify their involvement in suicide attacks, it is not significant as a causal factor and we should keep that in mind. Researchers have also begun to counter the limitations that have arisen from the difficulty in developing research methods that can account for the death of the attacker. By diversifying the research methods used and beginning to move away from narrative critiques of older works, we begin to get a bigger, more complete picture that has led us to see the importance of several different levels of motivation.

Future Research

This field can continue to be enriched by further empirical research. Diversifying the research methods will help to counter unavoidable limitations of other studies, as those studies will help to fill in gaps in future efforts. Areas that require greater consideration range from the difference between individual motivations of men and women, as well as organizational differences in employing men and women, to comparing suicide tactics to non-suicide tactics.⁸³ In our current age of technology and global media, the influence of

information sharing cannot be ignored, Although some authors have acknowledged its importance, this is a concept that has largely been left out of causal research. The role of media as an amplifier of global and individual reactions should be examined in far greater detail.⁸⁴ Strong research methods and frameworks need to be employed to take into account interactions among people, groups, and society as a whole while considering individual, social, and organizational factors.⁸⁵

Finally, Crenshaw notes that greater distinction should be made between types of suicide attacks and between the expected outcomes of the attack.⁸⁶ The difficulty with fulfilling this improvement to future research is that suicide attacks are, relatively speaking, few in number. Although a distinction should be made, this may create further limitations by diminishing the sample size.

Policy Implications

The attacks of September 11, 2001 launched renewed interest in counterterrorism around the world. The limited research that had been performed concerning the subject of causes for suicide terrorism unfortunately restricted new policies to address either identified causes of terrorism and insurgency in general or speculated causes of suicide terrorism. Research in the field has progressed substantially, and we now acknowledge the complex relationship of factors that lead to suicide-terror attacks. Although there is not a single agreed-upon cause, several elements have repeatedly been shown to have an effect and policy can now address these issues more effectively.

Societal influences have been acknowledged by many of the leading experts in this field and it is, therefore, not surprising that many suggest policy reforms that act at a societal and community level. Intelligent aid services are emphasized as the first step to combating suicide terrorism.⁸⁷ Improving and strengthening local organizations to be able to provide better social services and education will give the people somewhere to look for aid other than terrorist groups, reducing their importance to the community.⁸⁸ Creating alternative options for potential suicide terrorists can help to reduce their participation and allegiance to extremist religious terror organizations.⁸⁹ Additionally, addressing religious and gender inequality in areas of frequent terrorist and suicide terrorist attacks is important to both human rights efforts and counterterrorism.⁹⁰ Although some research has disqualified the impact of the economy on the quantity of suicide terrorism, 'the war on poverty' approach to counterterrorism can be effective provided that it follows an evidence-based approach to the actual impact of the economy on terrorism and societies that produce terrorists.⁹¹

Individually-targeted counterterrorism efforts are much more difficult to identify than those on the societal level, however, policies that prevent individuals from beginning down a pathway to suicide terrorism are essential in the long run. In the short term, focusing on the organizational level has the potential for more immediate results but also for subsequent impact at the individual level later on.⁹² Organizationally-targeted policy that focuses on dissension within the group, facilitated exit from the group, and delegitimizing the leaders will help to reduce suicide terrorism.⁹³ Policy responses need to incorporate and address interactions among people, groups, and society as a whole, taking into account the individual, social, and organizational factors that contribute to the phenomenon.⁹⁴

About the Authors

Vanessa Harmon has been a member of the Canadian Armed Forces since 2003. She has a BSc in physics and space sciences from the Royal Military College of Canada and a Master's of Criminal Justice from the University of Colorado, Colorado Springs. She is currently working in Ottawa as an Aerospace Engineer in the Royal Canadian Air Force holding the rank of Major. She may be reached at vanessa.harmon@forces.gc.ca.

Edin Mujkic, Ph.D., is an Assistant Professor in the School of Public Affairs at the University of Colorado, Colorado Springs. His work is focused on professional military education, national security and U.S. foreign policy, homeland security and emergency management, as well as the general field of public administration. His research has appeared in *Public Administration Quarterly*, *Public Integrity*, and *Democracy & Security*, among other outlets. He may be reached at emujkic@uccs.edu.

Catherine Kaukinen, Ph.D., is a Professor and Chair in the Department of Criminal Justice at the University of Central Florida. Kaukinen's research interests include intimate partner violence, risk and protective factors for violent victimization, the history of Title IX and Federal initiatives to address violence against college women, and the evaluation of campus-based violence against women prevention and intervention programs. Her research has appeared in *Criminology*, *Journal of Marriage and Family*, *Journal of Research in Crime & Delinquency*, *Journal of Interpersonal Violence*, and *Trauma, Violence, and Abuse*, among other outlets. She may be reached at Catherine.Kaukinen@ucf.edu.

Henriikka Weir, Ph.D., is an Assistant Professor in the School of Public Affairs at the University of Colorado, Colorado Springs. Dr. Weir is also a former police officer. Her research interests revolve mainly around the intersection of childhood maltreatment, intimate partner violence, trauma, substance abuse, violence, and delinquency / adult offending. She also studies the causes, correlates, and effects of trauma among police officers. Dr. Weir's research has been published in *Journal of Criminal Justice and Behavior*, *Journal of Criminal Justice*, *Journal of Criminal Justice Education*, *Youth Violence and Juvenile Justice*, *Criminal Justice Studies*, and *Violence and Crime in the Family* among others. She may be reached at Hweir@uccs.edu.

Appendix A

Articles Excluded from the Review

Karin Andriolo, “Murder by Suicide: Episodes from Muslim History,” *American Anthropologist* 104, no. 3 (2002): 736-742.

Reason for Exclusion: This article analyzes three different cases of ‘murder by suicide’ from history to determine historical symbolic strategies to reconcile the potential killer with his or her death, not to explain the cause or motivation to engage in suicide terrorism.

Scott Ashworth, Joshua D. Clinton, Adam Meirowitz and Kristopher Ramsay, “Design, Inference, and the Strategic Logic of Suicide Terrorism,” *The American Political Science Review* 102, no. 2 (2008): 269-273.

Reason for Exclusion: This article focuses on critiquing Robert Pape’s 2003 book “The Strategic Logic of Suicide Terrorism.” The authors suggest that Pape’s research design cannot be used adequately to reveal “relevant statistical associations between the use of suicide terror and its possible correlates.” (p. 269) Although critiques of research design are important for improving knowledge of a specific field, the article will not be used in the review .

Efraim Benmelech and Claude Berrebi, “Human Capital and the Productivity of Suicide Bombers,” *The Journal of Economic Perspectives* 21, no. 3 (2007): 223-238.

Reason for Exclusion: This article analyzes the relationship between human capital (education, experience) and suicide bombing, finding that older, more experienced attackers are assigned to more important targets and are less likely to fail.

Clara Beyler, “Messengers of Death: Female Suicide Bombers,” *Institute for Counter-Terrorism*, 2003.

Accessed September 3, 2014. <http://www.ict.org.il/Article/854/Messengers%20of%20Death%20-%20Female%20Suicide%20Bombers>.

Reason for Exclusion: Although this article alludes to some of the motivations of female suicide bombers around the world, the focus is on describing the history and impact of women in this role, especially the differences in use and exploitation by different groups.

Matthew B. Capell and Emile Sahliyah, "Suicide Terrorism: Is Religion the Critical Factor?" *Security Journal* 20 (2007): 267-283.

Reason for Exclusion: Rather than discuss explanations of suicide terrorism specifically, this article focuses on religion and suicide terrorism as explanations for the increased lethality of modern terrorism in general. It is interesting and helpful to consider suicide terrorism as a cause and not just an outcome; however, this is outside the scope of this essay.

D. Suba Chandran, "Suicide Terrorism in South Asia: From Promised Land to Presumed Land," *Institute of Peace and Conflict Studies*, (2003).

Accessed September 4 2014. <http://www.ipcs.org/article/pakistan/suicide-terrorism-in-south-asia-from-promised-land-to-presumed-1085.html> .

Reason for Exclusion: The focus of this article is to highlight the dissimilarities between suicide attacks perpetrated in Sri Lanka, India, and Pakistan. Although the author briefly touches on nationalistic motivations versus religious motivations, the purpose is not to discuss causes of suicide terrorism.

Martha Crenshaw, "Suicide Terrorism in Comparative Perspective," in *Countering Suicide Terrorism*, by Boaz Ganor, (Herzliya, Israel: The International Policy Institute for Counter-Terrorism, 2002).

Reason for Exclusion: In this article, although the author briefly outlines theorized causes of suicide terrorism at the individual, organizational and cultural levels, the focus is on relating suicide terrorism to terrorism in general, as well as outlining similarities to self-immolation and hunger strikes.

Stephen F. Dale, "Religious Suicide in Islamic Asia: Anticolonial Terrorism in India, Indonesia and the Philippines," *Journal of Conflict Resolution* 32, no. 1 (1988): 37-59.

Reason for Exclusion: This article stresses the importance of understanding the historical use of suicide attacks throughout the history of Middle Eastern religious conflict in order to better comprehend modern suicide terror. The author alludes to this historical use as an influence in creating a culture that supports suicide attacks, but does not specifically discuss causes of suicide terrorism.

Adam Dolnik, “Die and Let Die: Exploring Links Between Suicide Terrorism and Terrorist Use of Chemical, Biological, Radiological, and Nuclear Weapons,” *Studies in Conflict and Terrorism* 26, no. 1 (2003): 17-35.

Reason for Exclusion: This article considers the nuances of contemporary suicide terrorism and how they are not indicative of an increased likelihood to use mass-casualty attacks with WMDs.

Linda Butler, “Suicide Bombers: Dignity, Despair, and the Need for Hope: An Interview with Eyad El Sarraj,” *Journal of Palestine Studies* 31, no. 4 (2002): 71-76.

Reason for Exclusion: Although this article goes into some detail about the psychological-level motivations of Palestinian suicide bombers, the article is not included in the review because it does not include reproducible research. The dialogue between Butler and El Sarraj is included in the discussion.

Roxanne L. Euben, “Killing (for) Politics: Jihad, Martyrdom, and Political Action,” *Political Theory* 30, no. 1 (2002): 4-35.

Reason for Exclusion: The focus of this article is on defining and clarifying *Jihad* and explaining the role of *Jihad* in the political sense. It does not detail a theory of suicide terrorism causes.

Jeremy Ginges, Ian Hansen, and Ara Norenzayan, “Religion and Support for Suicide Attacks,” *Psychological Science* 20, no. 2 (2009): 224-230.

Reason for Exclusion: The authors focus on relating religion to popular support for suicide terrorism. Although there is evidence within their study showing that religion influences the willingness to participate in martyrdom, overall popular support is the intended dependent variable.

Harvey Gordon, “The ‘Suicide’ Bomber: Is it a Psychiatric Phenomenon?” *Psychiatric Bulletin* 26, no. 8 (2002): 285-287.

Reason for Exclusion: The author discusses whether suicide bombing can be described in psychiatric terms similar to those of ‘suicide’. Although he comes to the conclusion that suicide bombings are mostly political and there is not currently sufficient psychiatric understanding of the phenomenon, he does not get into the deeper causes of suicide terrorism.

Rohan Gunaratna, "The Post-Madrid Face of Al Qaeda," *The Washington Quarterly* 27, no. 3 (2004): 91-100.

Reason for Exclusion: This article focuses on the changes to terrorist ideologies after 2001 and the effects that Al Qaeda, Iraq, and Afghanistan have had on terrorism as a security threat in recent years. The author looks at the changing security environment and how counterterrorism needs to adapt to this environment.

Simon Haddad, "A Comparative Study of Lebanese and Palestinian Perceptions of Suicide Bombings: The Role of Militant Islam and Socio-Economic Status," *International Journal of Comparative Sociology* 45, (2004): 337-363.

Reason for Exclusion: This article examines the difference between Palestinian and Lebanese support for suicide attacks as a tactic. The author found that political Islam was the most important determinant of support and more prevalent among Palestinians than Lebanese even though approval was stronger among Lebanese.

Mohammed M. Hafez, "Dying to Be Martyrs: The Symbolic Dimension of Suicide Bombers," in *Root Causes of Suicide Terrorism: The Globalization of Martyrdom*, by Ami Pedahzur, (New York, NY: Routledge, 2006).

Reason for Exclusion: The author considers the individual-level motivations for suicide tactics and suggests that the symbolism surrounding 'martyrdom', largely framed by the organization and society, gives individuals the justification for their own personal motivation. The focus of this narrative is not to present a theory of individual motivations but rather to present a test that can help to evaluate rational models of explaining suicide terrorism at the individual level and to show the way ahead for researchers to understand the symbolism and social meaning of the acts themselves to the bombers (p. 56).

Mohammed M. Hafez, "Martyrdom Mythology in Iraq: How Jihadists Frame Suicide Terrorism in Videos and Biographies," *Terrorism and Political Violence* 19, no. 1 (2007): 95-115.

Reason for Exclusion: As the author explicitly states, the focus of the article is to show how specific groups frame their actions to achieve communication goals by manipulating their narratives. The study does not address the motivations of individual suicide attackers and is not included in the Systematic Review.

Michael C. Horowitz, “Nonstate Actors and the Diffusion of Innovations: The Case of Suicide Terrorism,” *International Organization* 64, no. 1 (2010): 33–64.

Reason for Exclusion: The author focuses on the spread of suicide terrorism between groups and the potential to be able to identify which groups may be open to adopting suicide terrorism as a tactic. As the focus is not on identifying the root cause of suicide terrorism, the article is not included in the Systematic Review.

Mark Juergensmeyer, “Religion as a Cause of Terrorism,” in *The Roots of Terrorism (Democracy and Terrorism)*, by Louise Richardson (New York, NY: Taylor & Francis Group, LLC, 2006).

Reason for Exclusion: Although this article relies heavily on studies of suicide terrorism, specifically Robert Pape’s 2005 book *Dying to Win: The Strategic Logic of Suicide Terrorism*, the focus is on discussing religious violence and religion as a cause for terrorism generally.

Martin Kramer, “The Moral Logic of Hizballah,” in *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, by Walter Reich, (Washington D.C.: The Woodrow Wilson Center Press, 1990).

Reason for Exclusion: Although other researchers in the field (Piazza, 2008; Pape, 2003) have cited this article as one of the few pre-2000 research documents on the subject of suicide terrorism, the article describes the moral justification that Hizballah used to sanction suicide terrorism as a tactic after the fact as opposed to the root causes of the act itself. The article was used within this research but was excluded from the comparison table.

Alan B. Krueger and Jitka Malečková, “Education, Poverty and Terrorism: Is There a Causal Connection?” *Journal of Economic Perspectives* 17, no. 4 (2003): 119–144.

Reason for Exclusion: Although the authors present a brief description of the economic conditions of various suicide bombers (pp. 135-137) in order to dispel the idea that poverty and education are driving factors in many forms of terrorism, the focus of the article is on terrorism in general. For this reason, the article was not included in the systematic review.

Andrew H. Kydd and Barbara F. Walter, “The Strategies of Terrorism,” *International Security* 31, no. 1 (2006): 49–80.

Reason for Exclusion: This article discusses motivations for terrorism in general and not motivations for suicide tactics specifically.

Assaf Moghadam, “The Roots of Suicide Terrorism: A Multi-Causal Approach,” in *Root Causes of Suicide Terrorism: The Globalization of Martyrdom*, by Ami Pedahzur, (New York, NY: Routledge, 2006).

Reason for Exclusion: The purpose of this article is not to describe or debate causes, but to build a framework of analysis that can be used for future research. In addition, it highlights the importance of studying suicide terrorism on multiple levels acknowledging the interactions between them.

Assaf Moghadam, “Suicide Terrorism, Occupation and the Globalization of Martyrdom: A Critique of Dying to Win,” *Studies in Conflict and Terrorism* 29, no. 8 (2006): 707–729.

Reason for Exclusion: The article does not present a suggested cause but argues that Pape’s conclusions in his 2001 book *Dying to Win* may have been wrongly made due to several shortcomings of the research design. Due to the focus of the article, it was not included in the review below.

Assaf Moghadam, “Motives for Martyrdom: Al-Qaida, Salafi Jihad, and the Spread of Suicide Attacks,” *International Security* 33, no. 3 (2008): 46–78.

Reason for Exclusion: The author focuses on the spread of suicide terrorism as a result of the increasing appeal of Taqfiri Salafism (the guiding ideology of al-Qaeda and its associates) and the evolution of al-Qaeda as a global network.

Jerrold M. Post, “Terrorist Psycho-Logic: Terrorist Behavior as a Product of Psychological Forces,” in *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, by Walter Reich, (New York, NY: Cambridge University Press, 1990).

Reason for Exclusion: Although other researchers in the field (Piazza, 2008; Pape, 2003) have cited this article as one of the few pre-2000 research documents on the subject of

suicide terrorism, the article refers to terrorism in general and does not specifically address causes of suicide terrorism, but does suggest a psychological cause for the extreme actions of terrorism as a tactic. The article was used within this essay, but was excluded from the comparison tables.

Joseph Pugliese, “Biotypologies of Terrorism,” *Cultural Studies Review* 14, no. 2 (2008): 49–66.

Reason for Exclusion: In this article, the author strives to impress upon the reader the potential negative impacts of using biometrics within the military and law enforcement to target individuals by corporeal features. Individuals who embody certain biotypologies are subjected to the fear and mistrust of the population as a result of this corporeal targeting. Although this is an important issue in terms of limiting panic and developing accurate ways of identifying terrorists, this is outside the scope of this article.

Allison G. Smith, “The Implicit Motives of Terrorist Groups: How the Needs for Affiliation and Power Translate into Death and Destruction,” *Political Psychology* 29, no. 1 (2008): 55–75.

Reason for Exclusion: In this article, the author shows that group dynamics, specifically affiliation and power motives, were especially significant to terrorist organizations. In-group and out-group affiliation was shown to be more impactful than power motives in a group’s tendency towards terrorism. This research is focused on terrorism in general and does not specifically analyze suicide tactics. Although many of the groups that were considered engaged in suicide tactics, due to the focus of the article it is not included in the systematic review.

Domenico Tosini, “Al-Qaeda’s Strategic Gamble: The Sociology of Suicide Bombings in Iraq,” *Canadian Journal of Sociology* 35, no. 2 (2010): 271–308.

Reason for Exclusion: The author focuses not on causes of suicide terrorism but on why some organizations targeted Iraqi Shi’ite civilians instead of targeting occupying military forces.

Ellen Townsend, “Suicide Terrorists: Are They Suicidal?” *Suicide and Life-Threatening Behavior* 37, no. 1 (2007): 35–49.

Reason for Exclusion: This article describes how empirical studies show that suicide terrorists are not suicidal but suggests that psychological autopsies will help improve our understanding of suicide terror.

Jeff Victoroff, “The Mind of the Terrorist: A Review and Critique of Psychological Approaches,” *Journal of Conflict Resolution* 49, no. 1 (2005): 3-42.

This article considers various theories of crime and personality to describe the psychology of the terrorist, but does not specifically address suicide terrorism and was, therefore, excluded from the systematic review.

Appendix B

Summary of Reviewed Articles that Discuss Individual-level Motivations for Suicide Bombers

Pedahzur, Ami, Arie Perliger and Leonard Weinberg. "Altruism and Fatalism: The Characteristics of Palestinian Suicide Terrorists." *Deviant Behavior* 24, no. 4 (2003): 405-423.

Terrorist Organization Focus: Palestinian suicide terrorists from 1993-2002.

Research Method: Using a database that includes both suicide and non-suicide Palestinian terrorist attacks against Israel from 1993 to 2002, the authors identified suicide (or attempted suicide) terrorists and compiled characteristics of each in order to compare them to non-suicide terrorists in the same area in an effort to determine the root cause of their suicide activities. The authors built their research framework similarly to relative-deprivation theories of collective political violence.

Supporting Arguments: Altruistic suicide occurs when an individual is entrenched in an organization and feels a duty to commit suicide. The individual sees himself or herself as secondary to the whole. Acute altruistic suicide specifically relates to martyrdom. The acute altruistic suicide perpetrator believes in a fantastic life after death but sees life as worthless.

Fatalistic suicide is a product of hopelessness that is often the result of continued and persistent political and economic oppression.

Conclusions: At an individual level, suicide terrorists fall into a new category of suicide typology, that of fatalistic altruistic suicides.

The authors' research showed that a combination of altruistic and fatalistic characteristics define the Palestinian suicide bombers. The altruistic characteristics were prominent at the organizational level and the fatalistic characteristics were prevalent at the individual level, thus addressing both levels will be key to policy development.

Lester, David, Bijou Yang and Mark Lindsay. "Suicide Bombers: Are Psychological Profiles Possible?" *Studies in Conflict & Terrorism* 27, no. 4 (2004): 283-295.

Terrorist Organization Focus: All (for review of previous research) but the authors used Michel and Herbeck (2001) specifically for an in-depth biography of Timothy McVeigh as a case study.

Research Method: Review of existing literature to determine current data and speculation about the profile of a suicide bomber, followed by the examination of cases that are similar to suicide bombers (but are not).

Supporting Arguments: In the case of Timothy McVeigh, the in-depth biography allowed scholars to profile him and categorize his behaviors into a specific type. Although McVeigh was not a suicide bomber, his plan included the possibility that he would be required to die in order to be successful. This suggests that other suicide bombers may be able to be profiled in a similar way.

Conclusions: The authors suggest a psychological cause, particularly a combination of individual-level factors such as conventionalism, authoritarian submission, authoritarian aggression, power, toughness, anti-intracception, and projection (pp. 290-291).

Profiles of suicide bombers could potentially be developed should researchers conduct in-depth analyses of individual bomber's personal histories. They do not suggest that a single profile is possible but that there may be a selection of profiles that can be applied.

Kimhi, Shaul and Shemuel Even. "Who are the Palestinian Suicide Bombers?" *Terrorism and Political Violence* 16, no. 4 (2004): 815-840.

Terrorist Organization Focus: Palestinian Suicide Bombers

Research Method: Content analysis focuses on identifying patterns in the history of each bomber. The authors used a convenient sample using "details that have been published in the literature describing suicide terrorists." (p. 815) They analyzed 60 cases that they categorized into four groups: religious, exploited, retribution for suffering, and social/nationalist.

Supporting Arguments: The authors suggested that every case of suicide terrorism required a motivated individual, the technical system to carry out the attack, and a condoning political leader. Beyond these similarities, each typology had different prerequisite factors (PF) and supporting factors (SF).

Religious: PF: religious interpretations encouraging terror and a charismatic leader; SF: sympathetic community, groupthink, and family support for the bomber after the attack.

Exploited: PF: individuals that cannot refuse the organization and personal or family problems resulting in depression; SF: Sympathetic community and the redemption of sins upon death.

Retribution for Suffering: PF: death or serious injury to someone close, trauma related to the Israeli occupation, and continuous difficulty related to the Israeli occupation; SF: sympathetic community, and family support for the bomber after the attack.

Social/Nationalist: PF: political awareness and belief that armed struggle and suicide missions are vital to liberation; SF: organizational participation in suicide missions, sympathetic community, and international media attention.

Conclusions: The authors present four typologies of suicide bombers and attribute different prerequisite factors and supporting factors for each typology.

In addition to the four typologies of the Palestinian suicide terrorist that emerged from the authors' research, they also noticed some overlap and suggested that suicide terrorism is the result of both multiple factors and multiple trajectories of the terrorist. They indicate that this research examines personal psychological motivations of the suicide bomber and it is important that political and social approaches be integrated into the solution.

Orbach, Israel. "Terror Suicide: How is it Possible?" *Archives of Suicide Research* 8, no. 1 (2004): 115-130.

Terrorist Organization Focus: Although the author does not indicate a specific group focus, he maintains concentration on the Palestinian-Israeli conflict.

Research Method: Analysis of research and open-source media information on various suicide attacks.

Supporting Arguments: The author argues that cultural values contribute to the willingness of suicide attackers to act but only in conjunction with certain facilitators, including an "enthusiastic determination to achieve a goal, ideological rage, glorification of the post-self, heavenly rewards, materialistic benefits for families, induced dissociative processes, and linguistic mediation." (p. 115) Through his observation of the preparation phase of a suicide bomber's training, many of the elements he describes are made evident.

Conclusions: A combination of what the author refers to as 'facilitators of suicide' and a sociological typology of altruistic suicide is suggested as the root cause of suicide terrorism.

The author suggests a preliminary profile of the suicide bomber as possessing several characteristics: religiosity, tendency for identification, self-collectivistic perception, suggestibility, imagination, naiveté, magical thinking, and aspirations for personal fame.

Azam, Jean-Paul. "Suicide Bombing as Inter-Generational Investment." *Public Choice* 122, no. 1-2 (2005): 177-198.

Terrorist Organization Focus: Hezbollah

Research Method: The author uses literature on economics in conflict and economics of terrorism as well as other microeconomic theories in order to show changes to individual investment in suicide bombing as it relates to increased wealth and education.

Supporting Arguments: The author builds an economic model that analyzes the relationship between the belief of individual bombers that their actions will benefit future generations by providing some public good and the bombers' intergenerational altruism. He argues that education and wealth provide a better understanding of the importance of investment in the future and subsequently increase intergenerational altruism.

Conclusions: The author proposes a theory similar to those in economics suggesting that the act of suicide bombing benefits, not the current generation, but future generations

within the family, especially when applied to wealthy and well- educated suicide bombers in Lebanon.

The author suggests that in order to reduce suicide bombings either the average income in at-risk populations should be reduced (although he acknowledges that this is not an acceptable form of aid), or the cost of performing the attacks must increase (although this is difficult to influence p. 193), and further suggests that an intelligent aid policy can influence the incidence of suicide terrorism.

Speckhard, Anne and Khapta Ahkmedova. "The Making of a Martyr: Chechen Suicide Terrorism," *Studies in Conflict and Terrorism* 29, no. 5 (2006): 429-492

Terrorist Organization Focus: Chechen nationalist groups targeting Russian interests

Research Method: Semi-structured empirical psychological autopsies (interviews with close family and friends) of 34 (of a possible 112) suicide terrorists who participated in Chechen suicide attacks from 2000-2005 augmented by interviews with surviving hostages of the Dubrovka Theatre takeover. The research distinguishes between gender, types of attacks, targets, and type of target. It also includes suicide attacks where the attacker survived and notes the changing trend in target type from Russian military bases in Chechnya to civilian targets in Russia.

Supporting Arguments: Throughout the course of their interviews, the authors noted that each of the perpetrators of suicide terrorist attacks had experienced a significant trauma. All in the sample had experienced the death or torture of a close family member or friend and seen societal-wide trauma. The only two exceptions were those who did not carry out their suicide mission. Following this trauma, interviewees noticed a significant change in behavior, especially with regard to religion and the justification of martyrdom.

Conclusions: In this research sample, trauma "appears to be the strongest catalyst to deep psychological and behavioral changes that ultimately led to the choice of suicide terrorism." (p. 455)

Similar to other research, the authors found that a combination of organizational, societal, and individual factors influenced suicide terrorists towards martyrdom. However the overarching and strongest element was the presence of a significant trauma. This potential cause should be examined in other organizations to determine if it is common to suicide terrorism in general, nationalist groups in general, or solely Chechen suicide terrorists.

Berman, Eli and David D. Laitin. "Religion, Terrorism, and Public Goods: Testing the Club Model." *Journal of Public Economics* 92 (2008): 1942-1967.

Terrorist Organization Focus: Taliban, Hamas, and Hezbollah were the primary focus of the discussion although some other Palestinian organizations were included in the analysis.

Research Method: The authors analyzed radical religious rebel groups in order to explain why these groups are more likely to use suicide terror than other insurgency organizations. They used a club-good model to relate the provision of public goods and the associated self-sacrifice of members to the effective recruitment and dispatch of suicide bombers.

Supporting Arguments: Upon analyzing several radical religious rebel groups, the authors noted a variety of elements that supported their hypothesis: the organizations often provided public services to their communities, enforced prohibitions, and required sacrifices of their members. The authors also compared the tactical-level decisions of insurgency and suicide attacks.

Conclusions: The authors suggest a tactical, rational, motivation by individual terrorists to be used against hardened targets as a root cause.

The findings of the study suggest that policy changes in counterterrorism that address constructive incentives can combat suicide terror. Creating alternative options for potential suicide terrorists can help to reduce their participation and allegiance to extremist religious terror organizations.

Jacques, Karen and Paul J. Taylor. "Male and Female Suicide Bombers: Different Sexes, Different Reasons?" *Studies in Conflict & Terrorism* 31, no. 4 (2008): 304-326.

Terrorist Organization Focus: Terrorist groups from the Middle East, Chechnya, Al Qaeda, and the LTTE were examined for a broad analysis of suicide terrorists in general.

Research Method: A log-linear analysis of 30 female and 30 male suicide terrorists differentiating between method of recruitment, motivation for attack, and outcome of attack (p. 304).

Supporting Arguments: The authors deconstruct current literature concerning the motivations and recruitment of women to extremist terrorism organizations as compared to this thesis, developing individual hypotheses for variation between men and women in each aspect.

After testing their hypotheses, the only hypothesis not supported by their data showed that women were more motivated by revenge and women were equally likely to be proactive in their recruitment.

Conclusions: The authors found slight differences in motivations for men and women.

For women: motivations are based on personal events and recruitment through peer influence, exploitation, and self-promotion.

For men: motivations are based on religious and nationalistic ideologies and recruitment through peer influence, exploitation, self-promotion, and religious persuasion.

The authors suggest that this research brought to light previously unexplored theories of female involvement in suicide terrorism. Further exploration and analysis is vital to future explanatory models and typologies of suicide terror.

Kruglanski, Arie, Xiaoyan Chen, Mark Dechesne, Shira Fishman and Edward Orehek. "Fully Committed: Suicide Bombers' Motivation and the Quest for Personal Significance." *Political Psychology* 30, no. 3 (2009): 331-357.

Terrorist Organization Focus: All, however the media clips that they analyzed focused on the Palestinian bombers and other Islamic extremist and Middle Eastern terrorist organizations.

Research Method: The authors base their theory on established psychological research both in the area of suicide terrorism and general human behavior. They analyzed interviews and media clips of successful suicide attackers' statements to determine individual motivations.

Supporting Arguments: "The quest for personal significance has been hailed by psychological theorists as a major motivational force in human behavior." (p. 335)

The reminder of personal mortality enforces commitment and ideology of the group. This commitment may help to diminish the fear of death for individual bombers, especially if there is a belief in immortality in the afterlife.

The possibility of loss of significance can have a similar effect to the quest for significance.

Conclusions: The combination of personal trauma, frustration, ideology and social pressure has been determined to contribute to a decision to engage in suicide terrorism. The authors suggest that a quest for personal significance can tie these individual motivations together into one overarching framework.

They suggest that policies should address the significance that is attributed to the act of suicide terrorism as well as the sense of significance-loss that volunteers feel (p. 353).

Appendix C

Summary of Reviewed Articles that Discuss Organizational-Level Causes of Suicide Terrorism

Ergil, Doğu. "Suicide Terrorism in Turkey." *Civil War* 3, no. 1 (2000): 37-54.

Terrorist Organization Focus: The Worker's Party of Kurdistan (PKK)

Research Method: The author examined Turkish-language accounts about the PKK's suicide attacks as well as the culture of the organization itself.

Supporting Arguments: Examination of the suicide attacks conducted by the PKK demonstrated that the organization expressly ordered each individual attack. The hierarchical, leader-oriented group employed charismatic leaders in a culture that allows for suicide attacks in the service of a higher cause. This enabled the organization to justify the attacks and influence its members. The author argues that situational factors in the years leading up to 1995, including the arrest of the leader, influenced the organization to progress into suicide attacks.

Conclusions: The author suggests group dynamics and the influence of an 'omnipotent' leader in addition to a significant amount of coercion and force from leadership as causal factors. The importance of ethnic "difference" to the development of armed rebellion in the area provides a focus for future policy development. Addressing religious and gender inequality in areas of frequent terrorist and suicide-terrorist attacks could be an effective counterterrorism measure.

Pape, Robert. "The Strategic Logic of Suicide Terrorism." *American Political Science Review* 97, no. 3 (2003): 28-39.

Terrorist Organization Focus: The study considers 188 suicide attacks from around the world from 1980-2001 conducted by various terrorist groups from around the world.

Research Method: Using the Lexis Nexis online database of world news media, Pape identified all suicide attacks from 1980-2001 and analyzed each incident for similarities, differences, level of success, motivations, and target properties.

Supporting Arguments: The author suggests that every group that uses suicide-terror tactics began with less drastic methods and progressed to suicide tactics when their efforts failed to get them what they wanted (p. 350). Data analysis found three consistent properties between the attacks: timing, nationalist goals, and target selection (p. 347).

Conclusions: Pape suggests that terrorism is perpetrated for one of two reasons: to force government to change policy and/or to mobilize additional recruits and financial aid for the

organization. Suicide terrorism is simply the coercive instrument of choice for terrorist groups because it works. The author suggests that counterterrorism should focus on homeland security rather than offensive military action in order to be the most effective. Pape came to five conclusions: suicide terrorism is strategic in nature, is specifically designed to coerce modern democracies into concessions, has been increasing in frequency because terrorists have found it to be an effective tool, produces diminishing returns, and can most effectively be countered by reducing terrorists' confidence in their ability to succeed in their attack.

Gambetta, Diego. *Can We Make Sense of Suicide Missions?* (New York, NY: Oxford University Press, 2005).

Terrorist Organization Focus: All groups, organizations, and governments that have used suicide missions of any kind in recent history.

Research Method: This narrative discusses similarities on an organizational level between groups who engage in suicide missions.

Supporting Arguments: Gambetta identified several generalizations about suicide missions (SMs):

1. All suicide missions are organized and supported by an organization.
2. Various types of armed organizations use SMs including legitimate governments.
3. All organizations that use SMs also use conventional tactics.
4. All organizations that use SMs are either not rooted in a community or they have the support of their constituency.
5. The weaker side in a conflict carries out all SMs.

Conclusions: The author suggests that at the individual level, there are too many differences and unique characteristics to be able to identify a single individual-level motivation but that the generalizations at the organizational level help to characterize and identify those who may engage in SMs. He highlights the similarities between how governments and people will treat their war heroes and how these organizations treat martyrs, emphasizing the idea that one person's terrorist is another's freedom fighter.

Gupta, Dipak and Kusum Mundra. "Suicide Bombing as a Strategic Weapon: An Empirical Investigation of Hamas and Islamic Jihad." *Terrorism and Political Violence* 17, no. 4 (2005): 573-598.

Terrorist Organization Focus: Hamas and Islamic Jihad within the Palestinian-Israeli conflict.

Research Method: The authors perform empirical analysis of twice-yearly data collected on suicide attacks by Hamas and Islamic Jihad between 1991 and 2003. They determined

significant coefficients using a Quasi-Maximum Likelihood Ratio and checked their results using a Seemingly Unrelated Regression.

Supporting Arguments: The results of the empirical analysis demonstrate a reciprocal relationship between suicide bombing and Israeli operations. A reciprocal relationship between suicide bombings and violence against Palestinians by Israeli forces demonstrates the strategic, political, and physical provocation of both sides. The actions themselves and the fallout from both the suicide attacks and the Israeli operations eliminate the possibility of compromise for either side. Further analysis explained that the decision to use suicide bombing over any other method was dependent on the perceived success and the magnitude of destruction that would result (p. 589).

Conclusions: The reciprocal actions between Israelis and Palestinians further mistrust, hatred, and denial of potential compromise by either side (p. 509). Rational-choice theories and analysis based on game theory are not applicable to suicide terrorism due to the complexity of motivations and the presence of multiple goals. In-depth case studies and the regression that the authors conducted are better able to capture these intricacies.

Ayers, Nick. "Ghost Martyrs in Iraq: An Assessment of the Applicability of Rationalist Models to Explain Suicide Attacks in Iraq." *Studies in Conflict & Terrorism* 31, no. 9 (2008): 856–882.

Terrorist Organization Focus: Although there is no single organizational focus, the author restricts his analysis to attacks that occurred in Iraq.

Research Method: The author considers four different rationalist models that hypothesize potential strategic causes of suicide terrorism: "(1) Robert Pape's model of strategic signaling and coercive bargaining, (2) Mia Bloom's model of organizational outbidding, (3) a model of internal recruiting, and (4) David Laitin and Eli Berman's model of hardened targets." (pp. 857-858) Dividing the research conducted on the 4 models into three categories (group characteristics and goals, group claims, and characteristics of the targets) the author analyzes the applicability of the findings for Iraq specifically.

Supporting Arguments: Ayers' research shows support for the final two theories but not the first two. For strategic signaling, the percentage of attacks against military vs. non-military targets counters the theory that the end-goal is for the withdrawal of foreign occupiers. In terms of the organizational outbidding model, the percentage of unclaimed attacks suggests that the support of the local population is not garnered by suicide terror. In terms of recruitment, the number of Iraqi nationals engaged in suicide attacks suggest some small amount of support for global jihad. The study showed the most support, however, for the tactical tool theory.

Conclusions: Suicide Terrorism is used strategically by an organization to gain tactical advantage over the enemy and aid in recruitment efforts (p. 856). The author suggests that suicide attacks can generally fit into any overall terrorist strategy. It is, therefore, essential to understand the tactical-level motivations and implications for these attacks in order for military strategists to accurately determine terrorist strategies and develop effective policies and procedures.

Appendix D

Summary of Reviewed Articles that Discuss Societal-Level Causes of Suicide Terrorism

Burdman, Daphne. "Education, Indoctrination and Incitement: Palestinian Children on Their Way to Martyrdom." *Terrorism and Political Violence* 15, no. 1 (2003): 96-123.

Terrorist Organization Focus: A study based on Palestinian educational culture.

Research Method: Review of 31 educational textbooks published prior to 2000 and used by the Palestinian Authority's Ministry of Education as well as various media programs and publications (p. 98).

Supporting Arguments: The author notes several instances of incitement to martyrdom from educational texts for Palestinian children in grades 5, 6, 7, 8, and 10 as well as in *Contemporary History of the Arabs and the World* (p. 101). Teachers' guides and television campaigns also showed instances of incitement. The authors evaluated the success of this educational campaign by highlighting the suicide attacks and martyrdom resulting from insurgency actions by children under the age of 18 (pp. 105-106).

Conclusions: The author summarized the influences of this educational campaign by outlining the effects that authoritarian society, religious and nationalist learning, educational techniques, group processes, programming and conditioning, indoctrination, and emotion have on individual mental health. Correcting the effects of this educational campaign will require "termination of incitement, re-education and de-conditioning" (p. 118) and is the responsibility of both the international community and the Palestinian people.

Khashan, Hilal. "Collective Palestinian Frustrations and Suicide Bombings." *Third World Quarterly* 24, no. 6 (2003): 1049-1067.

Terrorist Organization Focus: Palestinian refugees of the Palestine-Israel conflict.

Research Method: Using a simple random sample of 342 Palestinian refugees in southern Lebanon, interviews were conducted to perform an empirical analysis to answer whether suicide terrorists can be profiled in terms of education, economics, and personality; whether militant Islamist ideology is pervasive in their philosophy; and whether they make up a significant percentage of the refugees.

Supporting Arguments: The author found that the majority of the interviewees believed that suicide missions would successfully force Israel to submit to the demands of the

Palestinian people (p. 1061). There was also a significant proportion of the respondents that were willing to act as suicide bombers against Israeli civilians (p. 1061).

Conclusions: The author suggests that a combination of Palestinian collective frustration, Political Islam, and extreme poverty lead to the use of suicide terror as a tactic. The author found that the Palestinian refugee camps were essentially a breeding ground for potential suicide bombers. The closed society, extreme poverty, and collective societal humiliation allowed for pervasive militant religious extremism to justify and promote both support to the suicide attacks of others and for the willingness to participate.

Ramasubramanian, R. "Suicide Terrorism in Sri Lanka." (Institute of Peace and Conflict Studies, New Delhi, India, 2004).

Terrorist Organization Focus: Terrorist groups in Sri Lanka, specifically the LTTE and their suicide contingent, the Black Tigers.

Research Method: Descriptive, research-based article that describes the state of suicide terrorism in Sri Lanka (differentiating between suicide and suicidal terrorism). The author describes the threat scenario, suicide terrorism in Sri Lanka, the LTTE, the motivations of the Black Tigers, the role of women in the suicide cadre, and the psychological and nationalistic framework of suicide terrorism.

Supporting Arguments: The author cites societal and community activities that paint the Black Tigers as heroic martyrs for the Tamil people to demonstrate the motivation that some will have in the face of death. He describes the support to families of suicide bombers after their missions, the commemoration of the martyrs' deaths (not the celebration of their lives) and the upbringing of individuals to believe that they can and should choose the cause over their lives.

Conclusions: The fear of death, on a societal level, can motivate people to heroism. In the case of the Tamils, suicide terrorism has been framed in a light such that it is marketed as heroism (p. 15). The author suggests that counterterrorism and modern technology cannot eliminate suicide bombings, but that there are steps that can end suicide terrorism in Sri Lanka: understand the aim, history and the people; teach both sides that they are part of the problem and the solution; show that it does not matter who started the war as both sides sustain it; demonstrate that the standards of 'winning' are different than in a non-asymmetric war; have each side take proposals of peace talks seriously; address the societal mindset towards suicide bombing; and address the leadership that supports the use of suicide bombing as a tactic.

Jackson, Sara Wade and Dan Reiter. "Does Democracy Matter?: Regime Type and Suicide Terrorism." *The Journal of Conflict Resolution* 51, no. 2 (2007): 329–348. .

Terrorist Organization Focus: Focus on all suicide attacks from the Freedom House and Polity data combining Pape (2003) and Pedahzur's (2005) datasets.

Research Method: Using Freedom House and Polity data, the authors conducted quantitative tests on the relationship between regime type and suicide terrorism from 1980- 2005. The article builds on Pape's assertion that suicide attacks are almost exclusively perpetrated against democracies that are perceived to be occupiers.

Supporting Arguments: The results of the tests showed mixed results for the relationship between economic development and suicide terrorism. There was a positive correlation between larger states and an increase in suicide terrorism as well as a significant positive correlation between Muslim states and being victims of suicide terrorism. There was also a limited statistical correlation between democracies and being victims of suicide terrorism.

Conclusions: The authors hypothesized that democracies and especially mixed regimes would be more likely to experience suicide terrorism. This hypothesis was not supported by their research. However they did find nation size, Islam, and national and global experience with suicide terrorism to be correlated to suicide terrorism. The study found that regime type is uncorrelated with suicide terrorism but was marginally correlated to the number of religious minorities at risk within the nation. The authors suggest that further research on the relationship between suicide terrorism and non-suicide terrorism will help to improve the direction of causal research.

Gibson, Kyle Richard. "The Roles of Operational Sex Ratio and Young-Old Ratio in Producing Suicide Attackers." (Ph.D. dissertation, University of Utah, 2011).

Terrorist Organization Focus: All

Research Method: The author collected information on individual suicide attackers using data from three studies conducted prior to this one for 1208 suicide attackers from attacks that took place from 1981 to 2007. The data were analyzed to determine if there was a correlation between age, gender, and marriage demographics in a given country and the likelihood of that country producing suicide bombers.

Supporting Arguments: The author found that higher ratios of marriageable men to women, higher polygyny rates, percentages of Muslims, and larger populations were correlated to greater production of suicide bombers. Also, countries with a greater ratio of young men to old were less likely to produce suicide bombers.

Conclusions: The author suggests a multifaceted approach to counter suicide terrorism due to the influence of individual, social, and strategic elements of motivation. Limiting the appeal of suicide attacks to groups and individuals while addressing societal feelings of oppression and humiliation can be used in the counterterrorism effort. This research suggests that

decreasing operational sex ratios, decreasing the young-old ratio, and decreasing polygyny may decrease suicide attacks.

Benmelech, Efraim, Claud Berrebi, and Esteban F. Klor. "Economic Conditions and the Quality of Suicide Terrorism." *The Journal of Politics* 74, no. 1 (2012).

Terrorist Organization Focus: Palestinian suicide terrorists acting against Israeli targets from 2000 to 2006.

Research Method: The dataset used for this research consisted of 157 suicide terrorists gathered from the Israeli Security Agency's reports on Palestinian suicide terrorists that attacked or attempted to attack in Israel, the West bank and the Gaza Strip from September 2000 to December 2006. The data cover terrorist age, education, previous terror activity, target, the economics and demographics of the target area, and security measures in place.

Supporting Arguments: Other research suggests a similar relationship to the one that the authors propose: that when unemployment is low, there are desirable mainstream jobs for potential suicide attackers and only low-ability attackers that cannot find jobs can be recruited. The authors' research indicates that higher unemployment is correlated with more educated, mature and experienced suicide attackers that carry out attacks on more important targets closer to the area from which they originate. The correlation between the economy and the outcome of attacks is more indirect. The research indicated that higher quality suicide attackers are less likely to be stopped and more likely to cause more fatalities (p. 122).

Conclusions: Although the authors acknowledge previous research that disqualifies poverty as a causal factor in the quantity of terror attacks, they suggest that poor economic conditions, especially high unemployment, allow terrorist organizations to recruit better educated, more mature suicide terrorists to their cause and improve the quality of potential targets.

Previous research has begun to disqualify the impact of the economy on the quantity of suicide terrorism, leading some to argue against maintaining 'the war on poverty' approach to counterterrorism. This, and other research that demonstrates the importance of the economy of terrorism can help to focus counterterrorism policy in a manner that will be more efficient.

Appendix E

Summary of Reviewed Articles that Suggest Suicide Terrorism is Caused by a Combination of Individual, Organizational and/or Societal-Level Factors

Merari, Ariel. "The Readiness to Kill and Die: Suicidal Terrorism in the Middle East." in *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, by Walter Reich and Walter Laqueur, (Washington D.C.: The Woodrow Wilson Center Press, 1990).

Terrorist Organization Focus: Terrorists in the Middle East active in suicide car bombings between 1983 and 1986.

Research Method: The author examined the facts collected on 31 cases of suicide terrorism by car bomb in the Middle East from 1983-1986 (p. 203).

Supporting Arguments: Suicide terrorists often engage in two levels of indoctrination: the first is at the cultural level throughout their upbringing; and the second is mission oriented (p. 199). Situational factors, including group pressures, can be seen in other suicide situations throughout history, for example mass suicides, chain suicides, and suicides for an audience. The only personality factor that the author noted with any level of certainty, due to the difficulty in profiling and analyzing psychological elements of suicide terrorists, is the common element of a broken home.

Conclusions: The author argues that four distinct groups of factors influence an individual's decision: "cultural factors, indoctrination, situational factors, and personality factors." (p. 196) The person is suicidal while the organization simply provides the excuse. The author suggests that the individual suicide terrorists wish to die for personal reasons and the terrorist organizations provide them with an excuse to act. Terrorist groups legitimize the violent act that would normally be unacceptable (p. 206). For this reason, terrorism should be addressed separately at the group level while suicide needs to be addressed at the individual level.

Atran, Scott. "Genesis of Suicide Terrorism." *Science* 299 (2003): 1534-1435.

Terrorist Organization Focus: All

Research Method: Narrative describing the evolution of suicide terrorism throughout history and some of the more common theories of causes.

Supporting Arguments: Institutional factor: the relationship between peers and the loyalty to cohorts is especially important in determining suicide-terrorism behavior. Often this relationship between members of the group, known as fictive kin, is built and strengthened by the organization through religion.

Conclusions: The author argues that suicide terrorism is used as a weapon of psychological warfare against the greater population by an organization. On an individual level, a combination of psychological and cultural elements make individuals susceptible to recruitment. Preventing bombers from reaching their target is likely an ineffective strategy due to high cost and low likelihood of success. Strategies aimed at literacy, poverty, and reducing military occupation have the potential to be slow, ineffective, or counterproductive. Institutional-level programs have the most promising outlook on counterterrorism (p. 1537).

Moghadam, Assaf. "Palestinian Suicide Terrorism in the Second Intifada: Motivations and Organizational Aspects." *Studies in Conflict and Terrorism* 26, no. 2 (2003): 707-729.

Terrorist Organization Focus: Palestinian suicide bombers that attacked in the first 21 months of the Second Intifada.

Research Method: The author creates a framework of analysis that examines the process of the suicide attack from initial motivation to execution at both the individual and organizational level and proceeds to apply it to various theories of motivation for the bomber and aspects of the organization.

Supporting Arguments: Several researchers have supported the idea that suicide terrorism is rooted in an interconnected relationship between the individual, the organization and the society. Interviews with attackers, families, and friends as well as evidence from many different suicide attacks show support for the many different individual motivations that the author proposes, with varying degrees of influence for each motivation depending on the individual. Support for the strategic and tactical benefits to the organizations, as well as the consistent presence of the orientation phase of training and preparation support the organizational level of the author's proposal.

Conclusions: The author argues that a combination of individual and organizational level motivations contribute to the use of suicide terror as a tactic. At the individual level, several factors influence the potential suicide bomber but they are not always the same combination of factors. At the organizational level, organizational goals and strategies are integrated in recruitment, training and indoctrination to support the use of suicide terror as a tactic. It is unlikely that a single factor, either at the individual or organizational level, is solely responsible for a suicide attack. The author's framework of analysis is designed to analyze both levels of

influence and can be applied on a larger scale. Policy and prevention strategies should also be developed along these lines, integrating individual-level programs and organizationally-targeted response. However, in the short term, organizationally-targeted policy may be more effective due to the difficulty in addressing individual motivations.

Ariel Merari. "The Readiness to Kill and Die: Suicidal Terrorism in the Middle East." in *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences* by Andrew Silke (West Sussex, England: John Wiley & Sons, 2003).

Terrorist Organization Focus: The focus is on Islamic terrorist groups although at the group level the author presents factors applicable to other groups as well.

Research Method: This article is a narrative that uses examples to show that the suicide terrorist is not suffering from any pathological disorders or mental illness and that religion is not a motivating factor in the way that is sometimes perceived in the Western world when considering Islam. He also describes group-level factors that are similar across groups. Although this seems to suggest a group-level motivational theory, with the incorporation of societal factors in the group discussion, it can be seen as a combination theory.

Supporting Arguments: There is no evidence that suicide bombers suffer from mental illness or psychopathology. In one instance (the PKK) there is evidence that members were coerced into becoming suicide bombers, but otherwise, bombers are generally volunteers and believe in their goal. Understanding of Islam demonstrates that many of the perceptions in the Western world about motivations for martyrdom and after-death expectations are false. There are several group-level factors that are seen across groups, including the support of the bombers' families, desperation of the group in conflict, cultural precedent for self-sacrifice, and indoctrination of the bomber.

Conclusions: The strategic advantage of suicide bombing over hardened targets means that the tactic will always be attractive to terrorists. The author argues though, based on previous evidence, that no group remains committed to suicide terrorism for an extended amount of time and concludes that the groups involved in suicide terrorism now will graduate to less drastic tactics in the near future.

Atran, Scott. "Mishandling Suicide Terrorism." *The Washington Quarterly* 27, no. 4 (2004): 67-90.

Terrorist Organization Focus: Al-Qaeda and its affiliates.

Research Method: The author focuses on demonstrating by example how modern counterterrorism, although focused on current theories, is ineffective due to the invalidity of these individual theories to be applied in a blanket manner. He suggests that a layered approach that addresses various contributory factors will be more successful in countering suicide attacks (p. 72).

Supporting Arguments: correlation between a lack of civil liberties and terrorism. Suicide terrorists exhibit no socially dysfunctional attributes or suicidal symptoms. There is correlation between U.S. involvement in international situations and terrorist attacks against U.S. targets (p. 74). Many suicide terrorists are educated, able-bodied, and committed to the cause, possibly because this type of person makes a more reliable recruit. Small cells within the organizational network allow for the development of 'fictive kin' and a strengthening of the bond between individuals – the theory of banality of evil (p. 80).

Conclusions: The author suggests that suicide terrorism is the result of the cumulative effect of multiple variables but puts strong emphasis on organizational and institutional role in motivations. Effective counterterrorism will be the result of a coordinated, integrated strategy with multiple layers to address a variety of contributing factors. These layers include: defense of critical infrastructure and emergency response; intelligence collection; and political, social and economic programs addressing root causes of suicide terrorism aimed at reducing potential recruits' receptivity to terrorist recruitment.

Hisham H. Ahmed. "Palestinian Resistance and 'Suicide Bombing': Causes and Consequences." in *Root Causes of Terrorism: Myths, Reality and Ways Forward* by Tore Bjørgo. (New York, NY: Routledge, 2005).

Terrorist Organization Focus: Palestinian-Israeli conflict.

Research Method: The author presents a narrative describing events throughout the Palestine-Israel conflict that seem to have instigated changes in suicide bombing frequency. Testimony from lawyers and would-be bombers is used to describe the difference between suicide and martyrdom. A study conducted by Shafiq Masalha on Palestinian children age 10-11 is also used within the research to demonstrate the state of the psychology of the Palestinian population.

Supporting Arguments: Peaceful protest prior to 1987 Intifada was ineffectual. Testimony suggests belief in the equivalence of suicide bombing to the tactics of Israeli troops (p. 93). The testimony of a would-be bomber suggests that Israeli occupation and repression has scarred the psyche of the Palestinian people. 15% of Palestinian children involved in Masalha's study had dreams about becoming martyrs. When military operations by Israeli forces increase, suicide operations do as well.

Conclusions: The author suggests a combination of conceptual, military, psychological, social, religious, and political motivations for suicide bombings. The solution is political in nature and will require action on both sides as the two act in retaliation to the actions of the other and the 'chicken before the egg' argument cannot be solved without compromise and political action.

Berman, Eli and David D. Laitin. "Rational Martyrs vs. Hard Targets: Evidence on the Tactical Use of Suicide Attacks." in *Suicide Bombing from an Interdisciplinary Perspective* by Eva Mayerson Milgrom, (Princeton: Princeton University Press, 2004). and Berman, Eli and David D. Laitin. "Hard Targets: Theory and Evidence on Suicide Attacks." (Working Paper, National Bureau of Economic Research, Cambridge, MA, 2005).

Terrorist Organization Focus: The data the authors use are limited to the Palestinian-Israeli conflict and they note that the LTTE specifically do not fit into their model. They suggest extensions to the model to make it more applicable to other suicide terrorists.

Research Method: The authors build a framework that fits suicide terrorists and the organizations that support them into a rational-choice model by combining data on suicide attacks and club theory.

Supporting Arguments: Within this model, it is necessary that the martyrs be 'rational', which the authors argue is easily achieved given a belief in the cause and either a belief in reward for their actions in the afterlife or a sense of altruism towards those who will survive and a belief that their lives will be bettered. Radical religious groups both demand sacrifice of their members and provide social interaction. Coreligionists are generally softer targets and can be attacked using conventional tactics if desired. "The stronger the social service provision function of the club, the greater the proportion of its attacks will be suicide attacks... [and] the more damage it will do per suicide attack." (p. 24)

Conclusions: The authors argue that suicide terrorism is a rational decision that incorporates an assessment that a successful attack on a hard, well-protected target that will withstand a conventional insurgency attack outweighs the cost of losing one member and that radical religious organizations are well suited to organize such attacks. The authors acknowledge that terrorist groups out of Sri Lanka, Chechnya and Kurdistan likely do not fit into this model but suggest an extension that incorporates the threat to outside members as part of the club model. The authors suggest that their model has demonstrated that "weakening the benign activities of clubs reduces their ability to carry out attacks" (p. 28) which can be achieved directly or indirectly by strengthening competitor activities.

Elster, Jon. "Motivations and Beliefs in Suicide Missions." in *Making Sense of Suicide Missions* by Diego Gambetta. (Oxford, England: Oxford University Press, 2005).

Terrorist Organization Focus: Palestine, 9/11, Lebanon, Kamikaze, LTTE, PKK, Teenage Martyrs in Iraq-Iran War, Chechnya, Kashmir, Iraq.

Research Method: The author divides suicide missions into two levels of actors: individual attackers and the organizations that incite and enable the attacks. It is important to note that the definition that the author uses for suicide missions encompasses much more than suicide terrorism, as many other researchers consider it and may present different results.

Supporting Arguments: The author suggests that peer pressure, attachment to a cause larger than the self, indoctrination, revenge, and benefit to family/friends/society/future generations all contribute to an individual's motivations. Religion is not a motivating factor, although it may act to disinhibit the attacker. Previously considered individual causes that have been discounted in recent years, such as poverty and education, may still contribute at the population level. At the organizational level, motivations can be viewed in terms of goals, which are territorial (i.e. recovery of homeland, defense of homeland or expulsion of occupiers), religious (defense of holy sites or destruction of infidels), or both.

Conclusions: In the Middle East and Sri Lanka especially, the author suggests that feelings of inferiority and resentment have a significant impact. For Palestinian attackers, the belief that suicide missions are effective and that Israel is evil has a significant impact.

Merari, Ariel. "Social, Organizational and Psychological Factors in Suicide Terrorism." in *Root Causes of Terrorism: Myths, Reality and Ways Forward* by Tore Bjørgo. (New York, NY: Routledge, 2005).

Terrorist Organization Focus: Bombers involved in the Palestinian-Israeli conflict.

Research Method: The author conducted interviews with family and friends of suicide attackers, failed attackers, and trainers of attackers and consulted media reports to analyze individual and organizational-level motivations for suicide terrorism.

Supporting Arguments: Although the author examines individual factors and psychological causes, he rules them out. Theories that consider suicide to be acts of aggression or depression cannot explain suicide terrorism. The closest explanation of this type is Durkheim's concept of Optional Altruistic Suicide, however the author does not think that suicide terrorists fit this model either. Public support will influence a group's willingness to use suicide terror as a tactic as will the number of volunteers. No case is known of an individual carrying out a suicide attack on their own without an organization supporting them.

Conclusions: The author suggests that perceived necessity plays a more important role in an organization's decision to use suicide attacks than culture and ideology. Given his conclusions, the author suggests that counterterrorism should focus on physical defensive measures, deterring the organization, and influencing the opinion of the terrorists' constituency.

Atran, Scott. "The Moral Logic and Growth of Suicide Terrorism." *The Washington Quarterly* 29, no. 2 (2006): 127-147.

Terrorist Organization Focus: Islamic extremist groups with some mention of political and revolutionary groups.

Research Method: This article focuses on countering the premises of Robert Pape's "Dying to Win: The Strategic Logic of Suicide Terrorism," arguing that Pape's data apply to a recently outdated form of suicide terrorism and are no longer applicable. Using examples that contradict data and conclusions made in "Dying to Win," the author argues for a different root

cause of suicide terrorism. The author also conducted individual interviews with displaced youth about their perception of martyrdom.

Supporting Arguments: Throughout his interviews, the author found that many of the youth with whom he interacted professed support for global jihadi movements (p. 128). Suicide terrorists are “frequently middle-class, secularly well educated, but often ‘born-again’ radical Islamists... embrac[ing] apocalyptic visions for humanity’s violent salvation.” (p. 128) Pape’s data analysis consisted of suicide attacks from 1980-2001, however, more suicide attacks were conducted between 2001-2005 than in this period.

Conclusions: The author suggests that analyzing the individual terrorists and attempting to develop a profile of the suicide terrorist is inconsequential. The focus should be placed on society’s perception of global jihad and the organizational and group dynamics of the greater terrorist networks but specifically of the cells involved in suicide terrorism.

Hafez, Mohammed M. “Rationality, Culture and Structure in the Making of Suicide Bombers: A Preliminary Theoretical Synthesis and Illustrative Case Study.” *Studies in Conflict & Terrorism* 29, no. 2 (2006): 165-185.

Terrorist Organization Focus: Palestinian Suicide Bombers for the case study, however, the author notes several other groups that employ suicide attacks.

Research Method: The author employs a case study of Palestinian suicide bombers in order to illustrate the validity of an analytical method that incorporates rationalist, cultural, and structural approaches to explaining suicide terrorism.

Supporting Arguments: Organizational leaders on the Palestinian side of the Palestine-Israel conflict have stated their principle reason for employing suicide bombing as its relative effectiveness in comparison to conventional terrorism (p. 173). At the individual level, the author suggests that bombers use a redemptive logic to justify their actions, arguing, “martyrdom operations” are necessary to fulfill one’s commitment to God.” (p. 175) At the societal level, the ethnic conflict between Palestine and Israel combined with a recent (since the 1970s) resurgence of Islamic activism and religion can help to explain the cultural acceptance of suicide tactics.

Conclusions: Similarly to the assertions of some of the other researchers included in this work, the author argues that the three levels of motivation: individual, organizational and social, are interrelated to one another (p. 181). Religious interpretation that promotes martyrdom is essential to the individual decision (p. 180). At the organizational level, strategic decisions in relation to asymmetric conflict promote the use of suicide bombers. At the societal level, support of these operations requires three conditions: cultural norms, legitimate authorities condoning the tactics, and feelings of victimization at the community level (p. 181).

Pape, Robert. "Dying to Win: The Strategic Logic of Suicide Terrorism." *The Australian Army Journal* 3, no. 3 (2006): 25-37.

Terrorist Organization Focus: Although a large portion of the article addresses al-Qaeda specifically, it also considers other Islamic, Palestinian, and Sri Lankan groups.

Research Method: The article uses data from the Chicago Project on Suicide Terrorism. The data used in the Chicago Project are collated from open-source data in Arabic, Hebrew, Tamil, Russian, and English. The author presents some of the findings of this project.

Supporting Arguments: "Every suicide campaign since 1980 has been waged by terrorist groups whose principal goal has been to establish self-determination." (p. 28) 301 of 315 attacks since 1980 were part of a larger terrorist campaign designed for political or secular gain (p. 28). Individual suicide terrorists tend to come from countries with foreign (American) combat presence (p. 30).

Conclusions: The author suggests a combination of strategic, social, and individual logic supports suicide terrorism as an effective form of terrorism. However, the strategic element unifies the others and ultimately enables the terrorists' agenda. The author suggests that each of the influencing factors in suicide terrorism combine to produce a strategically logical explanation for suicide terrorism. Combination approaches like this incorporate a variety of observations that individual theories may overlook.

Bloom, Mia. "Dying to Kill: Motivations for Suicide Terrorism." in *Root Causes of Suicide Terrorism: The Globalization of Martyrdom* by Ami Pedahzur. (New York, NY: Routledge, 2006).

Terrorist Organization Focus: General discussion of groups that use suicide tactics.

Research Method: Narrative incorporating previous research conducted by the author and other subject matter experts.

Supporting Arguments: The author breaks down the discussion of motivations into two levels: individuals and organizations. At each level the author presents interview excerpts that suggest the basis for using suicide attacks as a tactic. At the individual level, perpetrators have incentives from various aspects of their lives including religious, material, social, and cultural elements (p. 35). At the organizational level, the strategic advantage against a materialistically superior enemy along with the cultural and societal perception and influence are of significance to the organization. The author especially focuses on group competition and outbidding and its impact on the use of suicide attacks as a tactic.

Conclusions: The author suggests that a combination of individual-level motivations and organizational motivations contribute to the perpetration of a suicide attack. The author suggests that countering this 'outbidding' can be done as part of counterterrorism policy by employing a concept of 'outbidding the outbidder' or by emphasizing elements of policy that the terrorist group is incapable of delivering (p. 46), although this will be more easily accomplished for nationalistic groups than for religious ones. Financially-targeted counterterrorism efforts may be the key to beginning this outbidding process.

Brym, Robert J. and Bader Araj. "Suicide Bombing as Strategy and Interaction: The Case of the Second Intifada." *Social Forces* 84, no. 4 (2006): 1969–1986.

Terrorist Organization Focus: Insurgent and state violence in Israel, the West Bank, and Gaza from Oct 26 2000 to July 12 2005.

Research Method: Review and analysis of data collected from "the online database of the International Policy Institute for Counter-Terrorism (ITC) in Herzliya, Israel; the website of Israel's Ministry of Foreign Affairs; the East Coast evening edition of the New York Times; and two authoritative Arabic newspapers – al-Quds, published in Jerusalem, and al-Quds al 'Arabi, published in London." (p. 1974) The collected information was analyzed on 128 variables.

Supporting Arguments: The authors were able to confirm their data by comparing Israeli-published reports with Arabic publications. Their model found statistical significance between assassinations and suicide bombings, other intifada-related deaths and suicide bombings, and a reciprocal relationship between suicide bombings and Palestinian prisoners (p. 1983).

Conclusions: The authors suggest that the motivations behind suicide bombings are mixed and complex. Organizational strategy is only one element of the motivation behind a suicide attack and often revenge and retaliation are important elements at both an individual level and an organizational level. Specifically they found 5 types of personal motives for the attacks ranging from a desire for personal revenge to a desire to achieve a religious goal. They also found 5 organizational rationales and 5 precipitant elements.

Grimland, Meytal, Alan Apter, and Ad Kerkhof. "The Phenomenon of Suicide Bombing: A Review of Psychological and Non-psychological Factors." *Crisis* 27, no. 3 (2006): 107–118.

Terrorist Organization Focus: All

Research Method: The authors evaluated research and theories from a variety of contributors to the field and provided evidence that supports the importance of many diverse factors to the cause of suicide terrorism.

Supporting Arguments: Common elements throughout the process of becoming a suicide bomber support the theory of a multidimensional approach. The authors saw evidence that cultural, religious, and societal influences, including from the media and other technologies, contributed to the process, as did individual-level factors, the indoctrination period, and organizational and strategic forces.

Conclusions: The authors suggest a complex interaction between many contributory forces as the root cause of suicide terrorism. The counterterrorism way ahead is first and foremost through efforts to change the media's glorification of suicide attacks followed closely by similar efforts to de-glorify acts of suicide terror in education and the community. They also highlight the importance of preventing the humiliation, oppression, and abuse of subdivisions of the civilian population.

Isaac, Jeffrey C., Karen Rasler, Eli Berman, David Laitin, Roxanne Euben, Ian Shapiro and Gilles Kepel, "Review Symposium: Understanding Suicide Terror." *Perspectives on Politics* 5, no. 1 (2007). 117-140.

Terrorist Organization Focus: All

Research Method: A review symposium that reviewed three books: Pape's 2005 *Dying to Win: The Strategic Logic of Suicide Terrorism*, Gambetta's 2005 *Making Sense of Suicide Missions*, and Bloom's 2005 *Dying to Kill: The Allure of Suicide Terror*. Each of the authors presents a unique perspective on the strengths and weaknesses of the books and suggests potential issues or theories that were not addressed in the books under study.

Supporting Arguments: Suicide terrorists are not mentally unstable or psychotic but are suggested to be 'altruistic communitarians'. At the tactical level, suicide attacks are useful within asymmetric warfare when conditions in the area are not conducive to conventional insurgency and there is a desire to compel a state to change. Societal constraints including support and organizational constraints such as defection influence the decisions of a terrorist organization. Collective societal humiliation may be an essential contributor to community support (p. 136). Although Islam is not causal to suicide terrorism, the role of religion is undeniable (p. 126) as it presents a potential meaning that can be adopted by attackers and used as a selective interpretive frame for their views (p. 130).

Conclusions: Berman and Laitin suggest an ecological theory of rebellion to better examine suicide missions in a more dynamic light than these three books have. Following from this theory, a stronger foundation for policy would be developed. They suggest strengthening local organizations' (other than the terrorist organizations) ability to provide social services and education in competition with those terrorist groups that provide these services now and devoting more resources to eliminating current and future tactics of asymmetric warfare. Rasler argues that the policy recommendations concerning counterterrorism efforts that strive to minimize negative impacts to local populations are essential and policies that distinguish between moderate and radical groups will be the most effective (p. 121). The books under review suggest alternative perspectives to rational choice theories which, in this case, seem incapable of adequately explaining suicide terrorism (Shapiro).

Crenshaw, Martha. "Explaining Suicide Terrorism: A Review Essay." *Security Studies* 16, no. 1 (2007): 133-162.

Terrorist Organization Focus: This article compares various elements of 13 different books published on suicide terrorism since 2002 and therefore considers a variety of terrorist organizations.

Research Method: Qualitative comparison of 13 different books using three main questions: why sponsoring organizations would see suicide attacks as effective, why a community would support them, and why individuals would engage in suicide missions. The author then compares the various policy recommendations.

Supporting Arguments: Even among these published books there is no consensus about causes of suicide terrorism. However, the research seems to demonstrate a multi-dimensional integration of social, psychological, and political interactions.

Conclusions: The author suggests that the interaction between individual, organizational and societal factors results in the use of suicide tactics. She notes that many of the authors included in her review consider individual emotions, religious influences, community support, and organizational strategy among the many elements that eventually lead to the use of suicide tactics. The author noted areas for improvement in research including: comparing suicide and non-suicide attacks by the same group, considering the role of media as an amplifier of global and individual reactions, distinguishing between types of suicide attacks, and distinguishing between the expected outcomes of the attack while refraining from lumping all attacks together simply given the expected death of the perpetrator.

Gill, Paul. "A Multi-Dimensional Approach to Suicide Bombing." *Journal of Conflict and Violence* 1, no. 2 (2007): 142-159.

Terrorist Organization Focus: All including some organizations that have not engaged in suicide-terror attacks as comparison groups.

Research Method: The author synthesizes empirically-based, one-dimensional research by other authors into a multidimensional concept. He analyzes theories from three different dimensions to build a model that takes into account interconnected influencing factors (individual, organizational, and community dimensions).

Supporting Arguments: Various studies have been conducted in order to explain suicide terrorism and multiple theories have been explored including individual-level theories such as pathological disposition to violence and rational choice, and others such as organizational-level theories, for instance, strategic motives and public support, and societal-level theories such as political freedom and poverty (pp. 144-145). Noting the interconnectivity between each of the elements presented by other researchers supports the author's model.

Conclusions: The author suggests a complex combination of factors from the individual, organizational, and community levels with emphasis on political and social psychology and group dynamics as the root causes of suicide terror. Further research is needed to refine the model. If confirmed, the theory suggests that a wide variety of policies at the various levels can be employed to counter suicide terrorism.

Gill, Paul. "Suicide Bomber Pathways among Islamic Militants." *Policing* 2, no. 4 (2008): 412-422.

Terrorist Organization Focus: Suicide bombers that have acted outside of a conflict area or outside of their own state as well as Palestinian, Tamil, Chechen, and Lebanese suicide bombers.

Research Method: The author uses examples of various suicide attacks and the actions of suicide bombers to describe a common progression through the life of a suicide bomber in order to establish the contributions of individual, group, and societal factors to suicide terrorism.

Supporting Arguments: In the initial phase, the author describes the importance of community support, media attention, and legitimization of suicide bombings. The second phase, the catalyst, can take many forms and can be religious, political, or personal, from religious radicalization to personal loss. The third phase, pre-existing ties, sets the stage for greater opportunity to join a terrorist organization. The final phase prior to the attack, in-group radicalization, includes solidifying ideologies, declarations of intent, and preparations for the act itself.

Conclusions: The author outlines a process or pathway from socialization, to the catalyst, to social bond, to the internalization of relevant group norms that solidifies the path of the suicide bomber. The author highlights that although he outlined one pathway to suicide terrorism, it is important to note that the elements may occur in a different order and that individuals can experience different catalysts, but he argues that each phase is essential to the process.

Kruglanski, Arie W., Xiaoyan Chen and Agnieszka Golec. "Individual Motivations, The Group Process and Organizational Strategies in Suicide Terrorism." *Journal of Policing, Intelligence and Counterterrorism* 1, no. 3 (2008): 70-84.

Terrorist Organization Focus: Islamic extremist focus.

Research Method: The article is a narrative incorporating the research of several authors into a theory that incorporates individual motivations, group and peer influence, and organizational strategy.

Supporting Arguments: The average suicide bomber is male between the ages of 18 and 27 (p. 71). At this age, higher levels of testosterone and greater susceptibility to social influence as well as likelihood to experiment with social roles contribute to individual motivations. At the group level, indoctrination of the individual in their new role as living martyr solidifies their path (p. 75). Solidifying the ideology of the group and the influence of an authority figure is also essential. At the organizational level, strategic considerations and the influence that the group has over the individual work together and lead to the bombing activity.

Conclusions: The authors consider the process of becoming a suicide bomber to be a combination of individual motivations, group pressure, and organizational strategy. Given that training of the bombers must take place somewhere, the authors argue that organizational cooperation with a host state is essential. Addressing state sponsorship is a critical element to counterterrorism. The authors also argue that negotiation with terrorists is inevitable and deterrence needs to be incorporated into counterterrorism efforts.

Piazza, James A. "A Supply-Side View of Suicide Terrorism: A Cross-National Study." *The Journal of Politics* 70, no. 1 (2008): 28-39.

Terrorist Organization Focus: Various groups involved in suicide and non-suicide terrorism from 1998-2005.

Research Method: The author used empirical tests to analyze common theories and correct for perceived selection bias in other studies. Using data from 4660 suicide and non-suicide terrorist attacks from 1998-2005 and a logistical regression, the author tested 4 hypotheses.

Supporting Arguments: The study found that terrorists who are nationals of non-democratic states are more likely to engage in suicide attacks (p. 28). The authors tested strategic theories and democracy theories of suicide terrorism but found no empirical evidence to support them. They did, however, find statistical correlation between suicide terrorism and foreign occupation, religious diversity, and group typology.

Conclusions: "Suicide terrorism is a product of political and organizational features of the terrorists themselves." (p. 28) There was no evidence of correlation between suicide terrorism and occupation by regime type. Democracies were determined to be less likely to produce suicide terrorists. Groups with universal or abstract political goals were more likely than groups with domestic political goals to engage in suicide terrorism.

Post, Jerrold M., Farhana Ali, Schuyler Henderson, Steven Shanfield, Jeff Victoroff and Steven Weine. "The Psychology of Suicide Terrorism." *Psychiatry* 72, no. 1 (2009): 13-31.

Terrorist Organization Focus: Terrorism is discussed broadly but the main emphasis is on militant Islam.

Research Method: Review of current literature on the psychology of suicide terrorism with the intention of informing mental health professionals to help improve understanding of the phenomenon of suicide terror.

Supporting Arguments: Social and cultural elements of the life course shape the collective identity. Socialization begins long before entering into a terrorist group, for instance, the authors provide an example of pro-suicide terrorism propaganda in a kindergarten class in Gaza City (p. 19). Adolescent psychology can be used to help explain the predominance of adolescent males as the core group of suicide terrorists (p. 20) focusing on the stage of experimentation, identity, and group influence. The authors explain the social process model, moral disengagement, intergroup relations theory, leader-follower relationships, and 'deindividuation' to describe group influence in the suicide terrorism process.

Conclusions: Collective identity and normality form a psychological perspective, although economics, history, politics, and anthropology contribute as well. The authors argue that "suicide terrorism is the result of a complex psychological pathway," (p. 27) and in order to limit suicide terrorists and prevent future attacks, policies should address the issue in a way that does not allow individuals to enter onto this path in the first place. They also suggest that dissension within the group, facilitated exit from the group, and delegitimizing the leaders will help to reduce suicide terrorism.

Pedahzur, Ami. "Toward an Analytical Model of Suicide Terrorism – A Comment." *Terrorism and Political Violence* 16, no. 4 (2010): 841–844.

Terrorist Organization Focus: The author's focus is on societies and communities that suffered from repression and were involved in a long-lasting struggle (which excludes some of Al-Qaeda's suicide terrorists).

Research Method: This article is a comment on a previous article. The author proposes an alternative model to the argument of the previous article as a result of prior research and knowledge on the subject. The author states that the amount of time allowed for a response did not afford the ability to describe in great detail or present the arguments with sufficient supporting facts.

Supporting Arguments: The author noticed trends in the suicide bombing process that support this three-stage model. The first stage includes a strategic decision by the organization and requires a permissible social environment. The second stage includes recruitment based on a personal experience or loyalty to the group and once again requires a social environment where suicide terrorism is permissible. The final stage is at the organizational level and includes training and confirmation of the bomber's commitment.

Conclusions: The author presents a three-stage model for explaining suicide terrorism: Stage 1) Organizational leadership decision-making; Stage 2) Individual motivations; Stage 3) Organizational recruitment, socialization and employment process (where stages 1 and 2 will likely co-occur). The author suggests continuing research along the lines of the proposed three-stage model. Although a more defined model than many others, it follows the same multidimensional approach of other researchers.

Karademir, Kutluer. "Suicide Terrorism as a Multidimensional Process: A Complex Relational Approach." *International Journal of Security and Terrorism* 4, no. 2 (2013).

Terrorist Organization Focus: 17 different organizations that were active from 1981 to 2006 and are included in Gambetta and Tzvetkova's (2006) dataset (listed by group on p. 28) (as cited in Karademir, 2013).

Research Method: Using a database compiled by Gambetta and Tzvetkova in 2006 (as cited in Karademir, 2013), the author applies a theoretical framework of analysis devised by Stacey (2001) to examine the interactive elements of suicide terrorism and show that these complex relationships between factors are the root causes of suicide terrorism.

Supporting Arguments: The author's focus is to present Stacey's (2001) theoretical framework as a potentially useful tool for future research, and to demonstrate the applicability of the framework, he provides examples of its application. He highlights arguments of cultural humiliation and betrayal and their influence on suicide terrorism and describes the procedure of becoming a suicide terrorist in the context of captured Al Qaeda militants from the 2003 suicide mission in Istanbul.

Conclusions: The author suggests a complex relationship between individual, social, and organizational factors. Policy responses need to incorporate and address interactions among people, groups, and society as a whole, taking into account the individual, social, and organizational factors that contribute to the phenomenon. The author suggests that future research should apply this framework in order to gain the greatest understanding of the phenomenon and find the most applicable policy responses.

Notes

- 1 Merriam-Webster, "Fireship," 2014, <http://www.merriam-webster.com/dictionary/fireship> (accessed May 19, 2018).
- 2 Scott Atran, "Genesis of Suicide Terrorism," *Science* 299 (2003): 1534-1435.
- 3 Ibid.
- 4 Ibid.
- 5 Robert A. Pape, "The Strategic Logic of Suicide Terrorism," *American Political Science Review* 97, no. 3 (2003): 343-361; James A. Piazza, "A Supply-Side View of Suicide Terrorism: A Cross-National Study," *The Journal of Politics* 70, no. 1 (2008): 28-39.
- 6 Jerrold M. Post, *The Mind of the Terrorist: The Psychology of Terrorism from the IRA to al-Qaeda* (New York, NY: Palgrave MacMillan, 2007).
- 7 Scott Atran, "The Moral Logic and Growth of Suicide Terrorism," *The Washington Quarterly* 29, no. 2 (2006): 127-147.
- 8 The Chicago Project does not distinguish between suicide terrorist attacks and other forms of suicide attack.
- 9 The University of Chicago, "Chicago Project on Security and Terrorism: Suicide Attack Database," 2014. http://cpostdata.uchicago.edu/search_new.php (accessed April 18, 2014).
- 10 Ibid.
- 11 Ibid.
- 12 Ibid.
- 13 Ibid.
- 14 Miranda Sissons and Abdulrazzaq Al-Saiedi, "A Bitter Legacy: Lessons of De-Baathification in Iraq," 2013, <http://www.ictj.org/sites/default/files/ICTJ-Report-Iraq-De-Baathification-2013-ENG.pdf> (accessed May 20, 2018); James P. Pfiffner, "US Blunders in Iraq: De-Baathification and Disbanding the Army," *Intelligence and National Security* 25, no. 1 (2010): 80.
- 15 The University of Chicago (2014).
- 16 Pfiffner, "US Blunders in Iraq: De-Baathification and Disbanding the Army," (2010).
- 17 NATO Public Diplomacy Division, "NATO Briefing: Countering Terrorism," 2011, http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2011_09/20110905_NATO_Briefing_Countering_Terrorism_EN.pdf (accessed May 20, 2018).
- 18 Assaf Moghadam, "Suicide Terrorism, Occupation and the Globalization of Martyrdom: A Critique of Dying to Win," *Studies in Conflict and Terrorism* 29, no. 8 (2006): 707-729.
- 19 Anne Speckhard and Khapta Ahkmedova, "The Making of a Martyr: Chechen Suicide Terrorism," *Studies in Conflict and Terrorism* 29, no. 5 (2006): 429-492.
- 20 The University of Chicago (2014).
- 21 Ibid.
- 22 Scott Atran, "Mishandling Suicide Terrorism," *The Washington Quarterly* 27, no. 4 (2004): 67-90; Sara Wade Jackson and Dan Reiter, "Does Democracy Matter?: Regime Type and Suicide Terrorism," *The Journal of Conflict Resolution* 51, no. 2 (2007): 329-348; Ami Pedahzur, "Toward an Analytical Model of Suicide Terrorism – A

Comment," *Terrorism and Political Violence* 16, no. 4 (2010): 841-844; Pape, "The Strategic Logic of Suicide Terrorism," (2003).

23 Paul Gill, "A Multi-Dimensional Approach to Suicide Bombing," *International Journal of Conflict and Violence* 1, no. 2 (2007): 142-159.

24 Martha Crenshaw, "Explaining Suicide Terrorism: A Review Essay," *Security Studies* 16, no. 1 (2007): 133-162.

25 Meytal Grimland, Alan Apter and Ad Kerkhof, "The Phenomenon of Suicide Bombing: A Review of Psychological and Nonpsychological Factors," *Crisis* 27, no. 3 (2006): 107-118.

26 Alan B. Krueger and Jitka Maleckova, "Education, Poverty and Terrorism: Is There a Causal Connection?" *Journal of Economic Perspectives* 17, no. 4 (2003): 119-144; Jeff Victoroff, "The Mind of the Terrorist: A Review and Critique of Psychological Approaches," *Journal of Conflict Resolution* 49, no. 1 (2005): 3-42; David Lester, Bijou Yang and Mark Lindsay, "Suicide Bombers: Are Psychological Profiles Possible?" *Studies in Conflict & Terrorism* 27, no. 4 (2004): 283-295; Scott Ashworth, Joshua D. Clinton, Adam Meirowitz and Kristopher W. Ramsey, "Design, Inference, and the Strategic Logic of Suicide Terrorism," *American Political Science Review* 102, no. 2 (2008): 269-273; Gill, "A Multi-Dimensional Approach to Suicide Bombing," (2007); Pedahzur, "Toward an Analytical Model of Suicide Terrorism – A Comment," (2010).

27 Mark Ware and Michael Mabe, *The STM Report: An Overview of Scientific and Scholarly Journal Publishing*, Overview, The Hague: International Association of Scientific, Technical and Medical Publishers, 2015, <http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1008&context=scholcom> (accessed December 17, 2018).

28 Angela Boland, Gemma Cherry and Rumona Dickson, *Doing a Systematic Review: A Student's Guide* (London: SAGE Publications Limited, 2013).

29 Arlene G. Fink, *Conducting Research Literature Reviews: From the Internet to Paper* (Thousand Oaks, CA: Sage Publications, 2005).

30 José Luis R. Martin, Victor Pérez, Montse Sacristán and Enric Álvarez, "Is Grey Literature Essential for a Better Control of Publication Bias in Psychiatry?: An Example From Three Meta-analyses of Schizophrenia," *European Psychiatry* 20, no. 8 (2005): 550-553; Laura McAuley, Ba Pham, Peter Tugwell and David Moher, "Does the Inclusion of Grey Literature Influence Estimates of Intervention Effectiveness Reported in Meta-Analyses?" *The Lancet* 356, no. 9237 (2000): 1228-1231; Annette Boaz, Deborah Ashby and Ken Young, *Systematic Reviews: What Have They Got to Offer? Evidence-based Policy and Practice*, (2002) <https://www.kcl.ac.uk/sspp/departments/politiceconomy/research/cep/pubs/papers/assets/wp2.pdf> (accessed December 17, 2018).

31 Piazza, "A Supply-Side View of Suicide Terrorism: A Cross-National Study," (2008).

32 Mark Ensalaco, *Middle Eastern Terrorism* (Philadelphia, PA: University of Pennsylvania Press, 2008).

33 Robert Pape, "Dying to Win: The Strategic Logic of Suicide Terrorism," *The Australian Army Journal* 3, no. 3 (2006): 25-37; Pape, "The Strategic Logic of Suicide Terrorism," (2003).

34 Atran, "Mishandling Suicide Terrorism," (2004).

35 Atran, "The Moral Logic and Growth of Suicide Terrorism," (2006).

36 Jackson and Reiter, "Does Democracy Matter?: Regime Type and Suicide Terrorism," (2007); Piazza, "A Supply-Side View of Suicide Terrorism: A Cross-National Study," (2008).

37 Piazza, "A Supply-Side View of Suicide Terrorism: A Cross-National Study," (2008).

38 Rohan Gunaratna, "The Post-Madrid Face of Al Qaeda," *The Washington Quarterly* 27, no. 3 (2004): 91-100; Hilal Khashan, "Collective Palestinian Frustrations and Suicide Bombings," *Third World Quarterly* 24, no. 6 (2003): 1049-1067; Crenshaw, "Explaining Suicide Terrorism: A Review Essay," (2007).

39 Jerrold M. Post, Farhana Ali, Schuyler W. Henderson, Steven Shanfield, Jeff Victoroff and Stevan Weine, "The Psychology of Suicide Terrorism," *Psychiatry* 72, no. 1 (2009): 13-31.

40 Post, *The Mind of the Terrorist: The Psychology of Terrorism from the IRA to al-Qaeda*, (2007).

- 41 Ellen Townsend, "Suicide Terrorists: Are they Suicidal?" *Suicide and Life Threatening Behavior* 37, no. 1 (2007): 35-49.
- 42 Ami Pedahzur, Arie Perliger and Leonard Weinberg, "Altruism and Fatalism: The Characteristics of Palestinian Suicide Terrorists," *Deviant Behavior* 24, no. 4 (2003): 405-423.
- 43 Shaul Kimhi and Shemuel Even, "Who are the Palestinian Suicide Bombers?" *Terrorism and Political Violence* 16, no. 4 (2004): 815-840.
- 44 Israel Orbach, "Terror Suicide: How is it Possible?" *Archives of Suicide Research* 8, no. 1 (2004): 115-130.
- 45 Jean-Paul Azam, "Suicide Bombing as Inter-generational Investment," *Public Choice* 122, no. 1/2 (2005): 177-198; Eli Berman and David D. Laitin, "Religion, Terrorism, and Public Goods: Testing the Club Model," *Journal of Public Economics* 92 (2008): 1942-1967; Speckhard and Ahkmedova, "The Making of a Martyr: Chechen Suicide Terrorism," (2006).
- 46 Karen Jacques and Paul J. Taylor, "Male and Female Suicide Bombers: Different Sexes, Different Reasons?" *Studies in Conflict & Terrorism* 31, no. 4 (2008): 304-326.
- 47 Nick Ayers, "Ghost Martyrs in Iraq: An Assessment of the Applicability of Rationalist Models to Explain Suicide Attacks in Iraq," *Studies in Conflict and Terrorism* 31, no. 9 (2008): 856-882.
- 48 Martha Crenshaw, "Theories of Terrorism: Instrumental and Organizational Approaches," *The Journal of Strategic Studies* 10, no. 4 (1987): 13-31.
- 49 Pape, "The Strategic Logic of Suicide Terrorism," (2003).
- 50 Doğu Ergil, "Suicide Terrorism in Turkey," *Civil Wars* 3, no. 1 (2000): 37-54.
- 51 Daphne Burdman, "Education, Indoctrination and Incitement: Palestinian Children on Their Way to Martyrdom," *Terrorism and Political Violence* 15, no. 1 (2003): 96-123.
- 52 Ibid.
- 53 Post, *The Mind of the Terrorist: The Psychology of Terrorism from the IRA to al-Qaeda* (2007).
- 54 R. Ramasubramanian, "Suicide Terrorism in Sri Lanka," (Institute of Peace and Conflict Studies, New Delhi, India, 2004).
- 55 Ibid.
- 56 Khashan, "Collective Palestinian Frustrations and Suicide Bombings," (2003).
- 57 Efraim Benmelech, Claud Berrebi and Esteban F. Klor, "Economic Conditions and the Quality of Suicide Terrorism," *The Journal of Politics* 74, no. 1 (2012): 113-128.
- 58 Ibid.
- 59 Jackson and Reiter, "Does Democracy Matter?: Regime Type and Suicide Terrorism," (2007).
- 60 Ariel Merari, "The Readiness to Kill and Die: Suicidal Terrorism in the Middle East," in *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, by Walter Reich and Walter Laqueur, (Washington D.C.: The Woodrow Wilson Center Press, 1990), 196.
- 61 Pedahzur, Perliger and Weinberg, "Altruism and Fatalism: The Characteristics of Palestinian Suicide Terrorists," (2003).
- 62 Atran, "Genesis of Suicide Terrorism," (2003); Atran, "Mishandling Suicide Terrorism," (2004).
- 63 Atran, "The Moral Logic and Growth of Suicide Terrorism," (2006).
- 64 Pape, "Dying to Win: The Strategic Logic of Suicide Terrorism," (2006).

- 65** Eli Berman and David D. Laitin, "Review Symposium: Understanding Suicide Terror," *Perspective on Politics* 5, no. 1 (2007): 122-129.
- 66** Assaf Moghadam, "Palestinian Suicide Terrorism in the Second Intifada: Motivations and Organizational Aspects," *Studies in Conflict and Terrorism* 26, no. 2 (2003): 65-92.
- 67** Robert J. Brym and Bader Araj, "Suicide Bombing as Strategy and Interaction: The Case of the Second Intifada," *Social Forces* 84, no. 4 (2006): 1969-1986.
- 68** Gill, "A Multi-Dimensional Approach to Suicide Bombing," (2007).
- 69** Post et al., "The Psychology of Suicide Terrorism," (2009).
- 70** Pedahzur, "Toward an Analytical Model of Suicide Terrorism – A Comment," (2010).
- 71** Mia Bloom, "Dying to Kill: Motivations for Suicide Terrorism," In *Root Causes of Suicide Terrorism: The Globalization of Martyrdom*, by Ami Pedahzur, (New York, NY: Routledge, 2006); Atran, "Genesis of Suicide Terrorism," (2003); Ayers, "Ghost Martyrs in Iraq: An Assessment of the Applicability of Rationalist Models to Explain Suicide Attacks in Iraq," (2008); Berman and Laitin, "Review Symposium: Understanding Suicide Terror," (2007); Crenshaw, "Explaining Suicide Terrorism: A Review Essay," (2007); Gill, "A Multi-Dimensional Approach to Suicide Bombing," (2007); Grimland, Apter and Kerkhof, "The Phenomenon of Suicide Bombing: A Review of Psychological and Nonpsychological Factors," (2006); Post et al., "The Psychology of Suicide Terrorism," (2009); Pedahzur, "Toward an Analytical Model of Suicide Terrorism – A Comment," (2010); Ramasubramanian, "Suicide Terrorism in Sri Lanka" (2004).
- 72** Eli Berman and David D. Laitin, "Hard Targets: Theory and Evidence on Suicide Attacks," November 2005, <http://www.nber.org/papers/w11740.pdf> (accessed May 19, 2018); Eli Berman and David D. Laitin, "Rational Martyrs vs. Hard Targets: Evidence on the Tactical Use of Suicide Attacks," In *Suicide Bombing from an Interdisciplinary Perspective*, by Eva Meyersson Milgrom, (Princeton: Princeton University Press, 2004), 1-38; Berman and Laitin, "Review Symposium: Understanding Suicide Terror," (2007); Berman and Laitin, "Religion, Terrorism, and Public Goods: Testing the Club Model," (2008); Pape, "Dying to Win: The Strategic Logic of Suicide Terrorism," (2006); Bloom, "Dying to Kill: Motivations for Suicide Terrorism," (2006).
- 73** Speckhard and Akhmedova, "The Making of a Martyr: Chechen Suicide Terrorism," (2006).
- 74** David Lester, Bijou Yang and Mark Lindsay, "Suicide Bombers: Are Psychological Profiles Possible?" *Studies in Conflict & Terrorism* 27, no. 4 (2004): 283-295; Ergil, "Suicide Terrorism in Turkey," (2000); Kimhi and Even, "Who are the Palestinian Suicide Bombers?" (2004); Orbach, "Terror Suicide: How is it Possible?" (2004).
- 75** Kutluer Karademir, "Suicide Terrorism as a Multidimensional Process: A Complex Relational Approach," *International Journal of Security and Terrorism* 4, no. 2 (2013): 15-30; Benmelech, Berrebi and Klor, "Economic Conditions and the Quality of Suicide Terrorism," (2012); Brym and Araj, "Suicide Bombing as Strategy and Interaction: The Case of the Second Intifada," (2006); Jackson and Reiter, "Does Democracy Matter?: Regime Type and Suicide Terrorism," (2007); Jacques and Taylor, "Male and Female Suicide Bombers: Different Sexes, Different Reasons?" (2008); Merari, "The Readiness to Kill and Die: Suicidal Terrorism in the Middle East," (1990); Pape, "The Strategic Logic of Suicide Terrorism," (2003); Pedahzur, Perliger and Weinberg, "Altruism and Fatalism: The Characteristics of Palestinian Suicide Terrorists," (2003).
- 76** Azam, "Suicide Bombing as Inter-generational Investment," (2005).
- 77** Moghadam, "Palestinian Suicide Terrorism in the Second Intifada: Motivations and Organizational Aspects," (2003).
- 78** Paul Gill, "Suicide Bomber Pathways among Islamic Militants," *Policing* 2, no. 4 (2008): 412-422.
- 79** Burdman, "Education, Indoctrination and Incitement: Palestinian Children on Their Way to Martyrdom," (2003).
- 80** The University of Chicago, "Chicago Project on Security and Terrorism: Suicide Attack Database," (2014); Kimhi and Even, "Who are the Palestinian Suicide Bombers?" (2004); Pedahzur, Perliger and Weinberg, "Altruism and Fatalism: The Characteristics of Palestinian Suicide Terrorists," (2003); Ramasubramanian, "Suicide Terrorism in Sri Lanka," (2004); Speckhard and Akhmedova, "The Making of a Martyr: Chechen

Suicide Terrorism," (2006); Ayres, "Ghost Martyrs in Iraq: An Assessment of the Applicability of Rationalist Models to Explain Suicide Attacks in Iraq," (2008).

81 Berman and Laitin, "Hard Targets: Theory and Evidence on Suicide Attacks," (2008); Jacques and Taylor, "Male and Female Suicide Bombers: Different Sexes, Different Reasons?" (2008).

82 Michael C. Horowitz, "Nonstate Actors and the Diffusion of Innovations: The Case of Suicide Terrorism," *International Organization* 64 (2010): 33-64; Assaf Moghadam, "Motives for Martyrdom: Al-Qaida, Salafi Jihad, and the Spread of Suicide Attacks," *International Security* 33, no. 3 (2008): 46-78.

83 Crenshaw, "Explaining Suicide Terrorism: A Review Essay," (2007).

84 Ibid.

85 Karademir, "Suicide Terrorism as a Multidimensional Process: A Complex Relational Approach," (2013).

86 Crenshaw, "Explaining Suicide Terrorism: A Review Essay," (2007).

87 Azam, "Suicide Bombing as Inter-generational Investment," (2005).

88 Berman and Laitin, "Review Symposium: Understanding Suicide Terror," (2007).

89 Berman and Laitin, "Religion, Terrorism, and Public Goods: Testing the Club Model," (2008).

90 Ergil, "Suicide Terrorism in Turkey," (2000).

91 Benmelech, Berrebi and Klor, "Economic Conditions and the Quality of Suicide Terrorism," (2012); Bloom, "Dying to Kill: Motivations for Suicide Terrorism," (2006).

92 Moghadam, "Palestinian Suicide Terrorism in the Second Intifada: Motivations and Organizational Aspects," (2003).

93 Post et al., "The Psychology of Suicide Terrorism," (2009).

94 Karademir, "Suicide Terrorism as a Multidimensional Process: A Complex Relational Approach," (2013).

Copyright © 2018 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).



Defending Cities Against Nuclear Terrorism: Analysis of A Radiation Detector Network for Ground Based Traffic

By Edward Cazalas

Abstract

This article describes a specific, promising concept for a traffic-based radiation detector network concept deployed on roads/highways/stoptlights/etc. The detector network concept is intended to help defend urban areas against nuclear attack by adversaries. The network has two potential functions: to detect and localize the covert transport of nuclear materials or weapons (specifically plutonium-based), and to monitor nuclear fallout in post-attack scenarios. This work analyzes the basic technical feasibility of the network, including detector hardware, deployment, and detection statistics. It will provide an overview of efforts to defend against nuclear terrorism and to develop concepts related to networked detection. Finally, the article discusses considerations that may affect the policy of the development and deployment of such a system. Included in these considerations is a rough-order-of-magnitude estimate of the cost of detector system deployment, a brief examination of the potential benefits and drawbacks of the radiation detector network, and a review of other concepts that could be, or are currently employed for nuclear detection.

Suggested Citation

Cazalas, Edward. "Defending Cities Against Nuclear Terrorism: Analysis of A Radiation Detector Network for Ground Based Traffic." *Homeland Security Affairs* 14, Article 10 (December 2018). <https://www.hsaj.org/articles/14715>

Introduction

The threat of nuclear terrorism has loomed over the United States and the international community for decades. World leaders, U.S. Presidents, and politicians spanning time, geography, political rank, and party recognized this threat as serious. Nuclear weapons or materials for a weapon may originate from countries that hold nuclear weapons, have nuclear weapons programs, or operate internal enrichment or reprocessing facilities. Radiological materials, on the other hand, may be accessed from devices or facilities that utilize radiological isotopes, including blood irradiators and therapy tools in hospitals, well loggers, or thermoelectric generators. Bad actors may weaponize highly enriched nuclear material into improvised nuclear devices (INDs) capable of great destruction or weaponize radiological material into radiological dispersal devices (RDDs). Either can be utilized to attack governmental or financial centers, populace, or critical infrastructure. The consequences of a nuclear weapon or IND detonation could be substantially higher, compared to the use of an RDD, in terms of lives lost, damage to infrastructure, spread of radioactive fallout, and subsequent disruption to the economy.¹ It is for this reason that the author emphasizes the examination of nuclear materials, rather than radiological materials, in this work.

Here, we will examine a specific concept to aid nuclear threat interdiction by detecting nuclear weapons or INDs being smuggled into a city. The concept also aims to augment consequence management by measurement of post-detonation fallout radiation. The concept involves a methodology of threat detection that relies on the placement of radiation detectors, in a networked fashion, along roadsides, highways, intersections, etc. We will discuss the prior work conducted in this area and the efforts of various government agencies in dealing with

the threat of nuclear terrorism. We will investigate the technical feasibility of this concept by utilizing calculations and simulations, which will provide insight into the concept's effective application and its shortcomings. The article will also discuss cost considerations, benefits and drawbacks of such a concept, as well as alternative concepts that are in place or could be incorporated. Finally, future work will provide guidance on what additional efforts should be undertaken.

Current Efforts at Preventing Nuclear Terrorism

In order to reduce the risk of attack by a nuclear weapon, homeland security authorities utilize a layered defense system. This type of approach focuses on reducing the quantity and number of locations of source materials, while strengthening the physical security of remaining sites.² International efforts along these lines have included the Global Threat Reduction Initiative (GTRI), which was established within the National Nuclear Security Administration (NNSA) under the Department of Energy (DOE). These efforts have helped to improve the security of nuclear facilities, processes, and materials outside the U.S. These improvements included upgrading security of nuclear facilities, disposal of surplus fissile materials, strengthening regulatory and inspection regimes, and providing detection and interdiction capabilities.³

Meanwhile, the Global Nuclear Detection Architecture (GNDA), which is coordinated by the Domestic Nuclear Detection Office (DNDO) of the Department of Homeland Security (DHS), has improved capability to detect nuclear materials smuggled into the U.S. In cooperation with agencies such as U.S. Customs and Border Protection (CBP), the U.S. Coast Guard, and the NNSA, for example, the DNDO administers the detection and interdiction regime to reduce the risk of nuclear attacks by the non-destructive assay and physical inspection of cargo, vehicles, and persons travelling into the U.S. through ports, airports, or border crossings.⁴

Despite the on-going efforts to secure and intercept nuclear material, the risk remains that these threat materials could still be accessed, smuggled, and utilized in an attack, due to substandard security and the existence of rogue actors. The growth and possible spread of terrorist ideologies to countries with access to nuclear materials or weapons underscores the significance of this threat.⁵

Introduction to a Networked Detector Concept

Detection of threat materials typically relies on detection of radiation, notably gamma-rays and neutrons. The detection of nuclear materials is complicated by the many potential entryways or transport modes available for smuggling.⁶ Additionally, the radiation signals detected from these materials are relatively weak and especially difficult to detect at distance. For example, the neutron emission from a HEU (highly enriched uranium) -based weapon

would be equal to the level of ambient background neutrons for a detector measurement less than two meters away. While the gamma-ray emissions from a HEU-based weapon are of relatively high energy and intensity (compared to a Pu-based weapon), they are easily shielded by a few centimeters of lead.⁷ Further absorption and scattering of the emitted neutrons and gamma-rays takes place by surrounding hydrogenous mediums, air between the weapon and detector, and the transport vessel's or vehicle's steel or aluminum siding. Often, the technical difficulties are magnified by operational constraints, such as the demand for speedy cargo throughput at seaports.⁸

This article will examine the potential of detectors to identify and track nuclear weapons or weapon materials. The detection of nuclear materials could play a role in thwarting such attacks as part of an integrated defense concept. We will describe a network concept for detecting the local transport of such materials within an urban area. If integrated with appropriate operational responses, such a network might interrupt an attack, or even deter its attempt due to its presence. This research shows that a network of these detectors may be able to offer some performance against a Pu-based weapon unless the weapon is highly shielded.

The concept of detector networks has been identified to enhance both detection and, as discussed below, consequence management.⁹ Detector networks combine many individual detector nodes that are geographically dispersed with each detector capable of sharing information with each other or with a central processing node.¹⁰ These networks have the potential to serve multiple roles including detection for counter-smuggling, pinpointing a location of attack, and post-blast fallout monitoring. The ubiquity of detectors in a network may increase detection of nuclear materials by preventing an adversary from detouring around known checkpoints at borders and ports. Additionally, the ability of the detector network to pinpoint attack location and monitor fallout would aid emergency response and enhance consequence management.

Consequence Management after a Nuclear Detonation

Obviously, the prevention of such attacks is the focus of many efforts. But prevention may fail, and coping with the consequences of an attack present challenges as well. Fallout from a nuclear weapon may cause prompt radiation poisoning, as well as increasing lifetime cancer risk for those exposed to intermediate-to-high dose levels. Consequently, the radioactive debris would restrict the operational deployment of emergency-response personnel and resources in the area of the blast site and downwind. This places a priority on understanding the distribution of such radioactive debris. Currently, the primary method of assessing the dose and providing information for decision making is to combine information from radiation pagers carried by emergency-response personnel with computational models that consider the location of the blast, local geography, and weather conditions.¹¹ Unfortunately, this approach places emergency-response personnel at risk and can waste time, by potentially requiring the redeployment of resources which have inadvertently entered or find themselves in higher dose areas, and may waste resources, by requiring personnel who have acquired administrative dose limit levels to be restricted from activity in potentially radiation-contaminated regions and requiring decontamination of personnel and equipment.¹²

The concept of consequence management plays an increasing role for state and federal agencies in response strategies for mitigating the risk of nuclear terrorism.¹³ Consequence management may be aided by efficient and informed decision-making for the deployment of emergency-response personnel and resources.

The specific network described in this article is a concept that may provide a means to gather the real-time assessment of dose from fallout across a city or geographic region that can aid decision making for the deployment of emergency response personnel and resources. Together with the network's potential to detect or deter covert transport of some weapons, the concept explored within this article appears promising and justifies further detailed analyses that investigate topics such as placement and density of detectors in a network; who operates, supports, and manages the detector network; and what procedures should be carried out by local, state, and federal authorities in the instance of detection.

Description of a Traffic-Based Detector Network

The detector network is made up of many detector nodes that are, ideally, deployed at an existing traffic-monitoring device location, such as locations of speed or stop-light camera systems. Unlike some other detector network concepts, the network concept described here is intended to be in place and operational well before a search for a nuclear weapon is undertaken or a nuclear detonation takes place. Pairing the detectors with traffic-monitoring devices will allow information from the detector and traffic-monitoring device to be fused (or correlated). Also, communication and electrical power may be accessed through existing feeds that supply communication and power to the existing traffic-monitoring devices. The detectors may be deployed across a city adjacent to roads, highways, on/off-ramps, intersections, or construction zones. Each detector node communicates to a central node that can process and fuse detector information, such as count rate, radiation type, time, and detector location, with information from the traffic-monitoring device, such as photographs of the vehicle, license-plate information, or speed and direction of travel.

Nuclear Material Model in a Detector Network Scenario

Figure 1 shows an illustration of a scenario of a threat vehicle passing by a single detector node paired with a traffic-monitoring device. The radiation detector detects neutrons and is installed under the highway signs, as in Figure 1a. As the threat vehicle, which contains a WGPu (weapons grade Pu) weapon drives toward, under, and away from the detector, the detector neutron measurement displays the presence of neutron-emitting material, as shown in Figure 1b. The detection of an amount of neutrons above a predefined threshold triggers the traffic-monitoring device to activate (photograph), as displayed in Figure 1c. If the detector neutron measurement exhibited an exceptionally large amount of neutrons above background, information from the traffic-monitoring device could be used by local authorities to interdict the vehicle. Otherwise, an additional detector measurement may be

taken if the vehicle travels by a second detector node to verify the initial detector reading, and information from the second traffic-monitoring device can be used to corroborate the identity of the threat vehicle.

The probability of detecting a threat vehicle is, in-part, a function of conditions that may be out of the control of those designing or operating the detection network. Conditions such as the route taken to the destination and traffic or road conditions can affect the detection probability in a stochastic manner. Primarily, however, detection probabilities increase for a growing number of detector nodes encountered on a given route, reduced distance between the threat vehicle and detector, and increasing time spent in the vicinity of a detector. Hence, the network's effectiveness would be improved if detector nodes were located at choke points, like bridges, or where vehicles are necessarily slowed, like intersections or on/off-ramps. The puzzle of where to place a limited number of detectors to cover a wide possibility of routes to maximize the overall detection probability of the network is a challenging task. This task is not researched here but is an active area of study.¹⁴

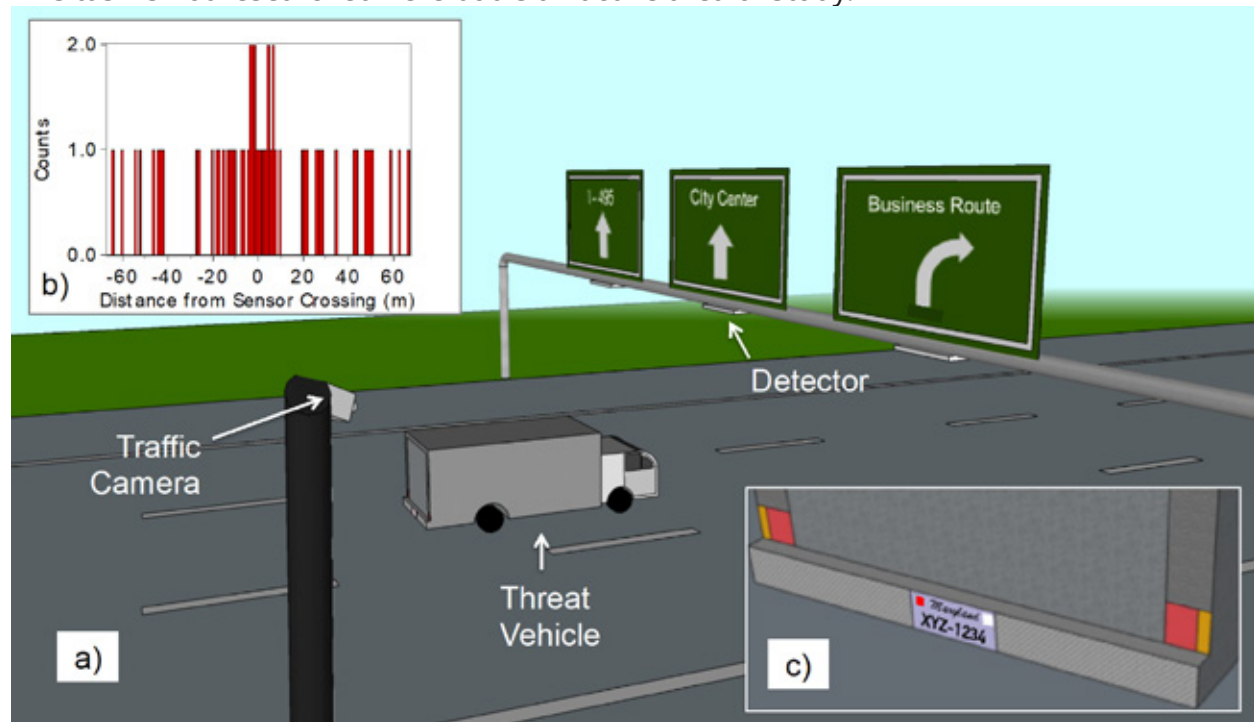


Figure 1: a) A scenario of a vehicle containing threat material (Pu-based weapon) passing by a traffic-monitoring device (traffic camera) and under a radiation detector. b) The neutron measurement of the detector as the threat vehicle travels toward, under (at distance = 0 m), and away from the radiation detector. c) The traffic-monitoring device provides additional information of the threat vehicle, such as a photograph of the vehicle or license plate, or speed information.

A distinct scenario from nuclear materials detection and interdiction is that in which a nuclear attack has already taken place. In this scenario, reliable information of dose as a function of geography and time is important to prevent sending emergency response into high-dose areas. Detector nodes in the blast radius would be destroyed and power may be lost to otherwise operational detectors. However, installing batteries with the detector nodes can mitigate loss of power. Other detonation effects, such as the blast, thermal radiation,

and electromagnetic pulse effects will have impact on the operational survivability of the nodes within the network. It is not expected that the addition of batteries will mitigate these effects to individual nodes, as these effects will likely also damage beyond operability the more fragile radiation detection equipment of an affected node before reducing battery performance. Thus, the addition of a battery is to provide power in the event of grid-wide power loss. The information provided by the detector network may be utilized by emergency-response personnel for assessment of radiation-dose levels at node locations and the time and dose evolution of fallout due to weather conditions across a geographical area of the detector network. This information may aid in the decision making regarding the deployment of emergency personnel and resources via roads and highways or provide information to guide possible public alerts for sheltering or evacuation.

Prior Work

Research into general detector networks has recently gained momentum through the Defense Advanced Research Projects Agency (DARPA), under the Department of Defense (DOD), and the DNDO. DARPA recently funded (as of 2014) the SIGMA program, which aims to spur the development of lower cost, more capable detectors. These detectors may be deployed in a ubiquitous or networked fashion and enable the enhancement and development of new concepts-of-operation to counter nuclear terrorism.¹⁵

A more direct parallel to the study undertaken here is the recently completed work by DNDO (ending in 2014) on the Intelligent Radiation Sensing System (IRSS) that attempted to develop technologies to determine the location of a radiation source through networked portable detectors.¹⁶ DNDO has also funded work (since 2014) on the Radiation Awareness and Interdiction Network (RAIN). RAIN has the goal of developing technologies for monitoring for radiation sources in free-flow traffic fused with other detectors, such as video cameras or license plate readers. To date, it appears that technical analyses from these projects have largely focused on specific technology development or statistics-based analysis of network systems. While some literature exists focused on the specific aspects of technical feasibility, limiting operational considerations, or policy implications of a radiation-detector network, these publications rarely consider the overlap of all these aspects, particularly for a concept combining the roles of both detection and fallout monitoring. Herein, the overlap of these aspects is considered.

The concept of a network for detection and location of nuclear materials has been studied from the aspects of detector hardware and experimentation,¹⁷ detection and localization statistics,¹⁸ communications between detector nodes or with a central processing node,¹⁹ and operational concepts.²⁰ One such study investigated a concept that involved the deployment of detectors into personal vehicles to be scanned at scan stations similar to tolling stations.²¹ While deployment of a detector onto a personal vehicle would extend the integration time of the detector and enhance the proximity of the detector to potential threat materials, a difficulty of the concept is in having public acceptance of invasive monitoring of personal property and susceptibility of the detectors to removal, spoofing, or sabotage. There is an existing literature on policy-related aspects such as preventing nuclear terrorism,²² and measuring the effects of a nuclear blast in a city.²³

The concept analyzed in the paper herein does not rely on invasive deployment into personal property. Moreover, it can employ logistics of maintenance already in existence for traffic-

monitoring systems. Additionally, the detectors deployed in the entailed concept are less susceptible to sabotage, especially when attached to above-road signs. While deployment of detectors on a roadside (on the ground) would present a higher potential for sabotage, failures of or abnormal readings from individual detector units may be quickly recognized through existing communication networks and addressed.

Analysis of the Technical Feasibility of Detection

The detection of radiation emitted from nuclear materials involves the absorption of gamma-rays or neutrons in the detector medium. Gamma-ray detection relies on the absorption of the gamma-ray energy, whereas neutron detection typically relies on the thermalization of neutrons through scattering in a hydrogenous medium in order to enhance absorption by isotopes such as ^{10}B or ^6Li , for a converter-style detector.²⁴ Once the neutron is absorbed, the energy of the reaction particles is absorbed in the detector medium forming a detection event. It is possible for a detector to detect both gamma-rays and neutrons. Analog electronics or digital algorithms such as pulse height or pulse shape discrimination are utilized to distinguish the difference. To model accurately the number of detection events in a given detector medium, it is first necessary to determine what materials (and subsequent emission type and energy spectrum) should be considered for modeling and then to model the emitting source and intermediary media. Finally, the number of energy-depositing absorption events may be calculated for a detector of a given detection medium thus facilitating the evaluation of the efficacy of a detector system.

Difficulties of Detecting Nuclear Materials

Detection and interpretation of gamma-ray signals are typically easier than that for neutrons, due to the detection equipment used, relative ease of obtaining spectrographic information from gamma-ray detection, the need for radiation-type discrimination in neutron detection, and use of thermalization mediums for neutron detection.²⁵ However, gamma-ray detection of threat materials is complicated by the much higher prevalence of gamma-ray emitting, naturally occurring radioactive materials (NORM), such as bananas (^{40}K) or cat litter (^{232}Th decay chain). NORM may cause unacceptable rates of false alarms in detector systems or may be utilized to mask the signal from threat materials. Additional complications are added due to the relative ease of gamma-ray shielding, which may be accomplished with a few centimeters of high-Z materials such as lead and unavoidably by the frame and siding of vehicles. Finally and importantly, the signal received by the detector from a threat source may be masked by gamma-ray background radiation, which is approximately an order of magnitude higher for gamma rays than neutrons.²⁶

Considering alone the relative difficulty of gamma-ray detection (vs. neutron detection) of a nuclear weapon in the presence of background radiation, a 'back-of-the-envelope' calculation is performed, with results in Table 1. The calculation 1) assumes a number of emitting gamma rays and neutrons from the surface of a weapons grade U (WGU) and WGPu weapon source; 2) determines the number of gamma rays or neutrons that reach a detector surface by estimation of the source-detector solid angle; and 3) compares the number of gamma

rays and neutrons reaching the detector surface to the background radiation at the detector surface by the respective radiation type. The calculation does not consider absorption of radiation in air, as this is assumed negligible, or the detection efficiency of the detector, as it is assumed that the detection efficiency of signal and background of a given radiation type are similar. Table 1 shows the low number of gamma rays that may be detected relative to background. Table 1 also shows the low number of neutrons that may be detected from WGU relative to background, and the high number of neutrons that may be detected from WGPu relative to background. Partially given the results of Table 1 and the other complications of gamma-ray detection, this study will investigate the efficacy of a detector system for detection of WGPu.

Table 1: The results of a calculation considering emission of neutrons and gamma rays from the surface (labeled 'Surface') of a weapons grade U weapon (WGU, 12 kg) and a weapons grade Pu weapon (WGPu, 4 kg), as adapted from S.Fetter, *et al.* (1990).²⁷ The table shows the number of neutrons or gamma rays arriving at a detector of area 1000 cm² at a distance of 5 m from the weapon of interest (labeled 'Detector'). The table also shows the ambient background neutrons and gamma rays for the same detector with background flux of 0.01 n/s-cm² and 0.3 g/s-cm² for neutron and gamma-ray background, respectively (labeled 'Bg').²⁸

	Neutron (n/s)		Gamma-ray (g/s)	
	WGU	WGPu	WGU	WGPu
Surface	1400	400000	100000	60000
Detector	0.3	99.9	25.0	15.0
Bg	10	10	300	300

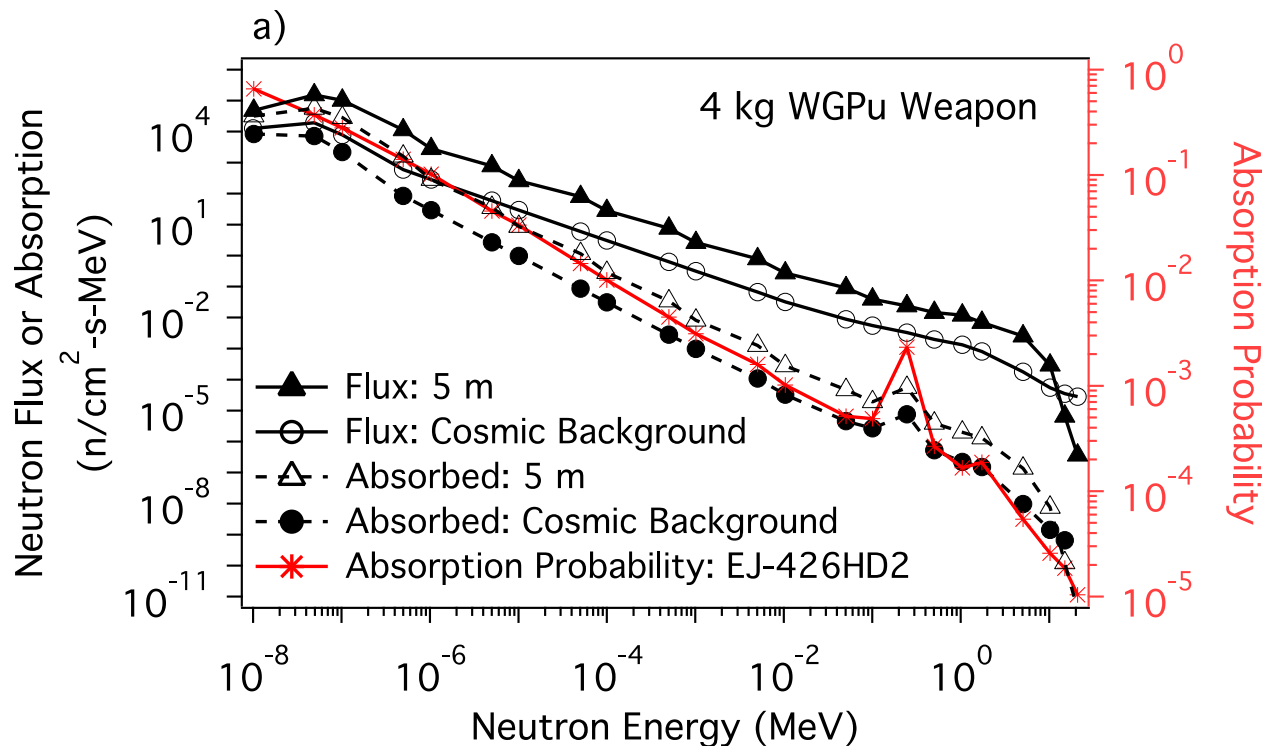
Simulation and Calculations of Detecting Nuclear Materials

The study undertaken herein investigates a hypothetical WGPu weapon. The model adapts that created by S.Fetter, *et al.* (1990)²⁹ and integrates a 4 kg shell of WGPu into a weapon form. The model considers a 1000 cm² area Zinc Sulfide (ZnS) -based detector 5 or 10 m from the WGPu weapon and includes intermediary air. The model is created in a Monte Carlo-based computational simulation to determine the flux of neutrons travelling onto the surface of the ZnS-based detector. The Monte Carlo simulation (MCNP6.1.1) computes scattering, absorption, and fission of source neutrons in the weapon itself as well as scattering and absorption in the intermediary air.³⁰ Information regarding neutron and gamma-ray emission rates is based on S.Fetter, *et al.* (1990)³¹ and G.W. Philips, *et al.* (2005)³².

The detector used in this study is a ⁶Li:F loaded ZnS(Ag) plate. ZnS(Ag) is a scintillating material that, when loaded with ⁶Li:F, becomes sensitive to neutrons due to neutron capture by the ⁶Li and scintillation by energy deposition of the reaction particles. Previous studies have shown ZnS-based detectors to be potentially the most promising ³He-free neutron detector technology, due to the relatively high neutron detection efficiency and potential for neutron-gamma discrimination capability.³³ Additionally, for this study the large detection

areas that may be obtained and the commercial availability of ZnS-based detectors are important. Due to the limited world-wide supply of ^3He , ^3He -free neutron detectors or replacement technologies have become an important area of research, can be implemented into neutron detection systems, and are often considered the “gold-standard” for use in neutron detection.³⁴ For the purposes of calculating the absorption of neutrons into the detection medium, the material properties (including atomic density of ^6Li and mass density of the ZnS plate) of EJ-426HD2 by Eljen Technology are considered.³⁵

The calculations are conducted in two parts: first, the number of neutrons that reach the detector face (flux) are determined as a function of neutron energy. The neutron flux spectra for both emitted neutrons from the WGPu at a distance of 5 m and from background are shown in Figure 3a. Second, the number of neutrons absorbed by the detection medium is calculated considering the absorption spectrum generated by the ^6Li isotopic density in a single plate of the ZnS-based detector and the flux spectra for emitted neutrons from WGPu and from background, also shown in Figure 3a. The absorption cross section is determined from ENDF libraries.³⁶ It is important to perform the calculations in terms of energy spectra, as absorption is not uniform across the energy range. The neutron spectra may then be summated to arrive at the total number of neutrons expected for flux and to be absorbed, as in Figure 3b. In Figure 3b a distance of 10 m and at the surface of the WGPu weapon is also considered. As expected from the calculations in Table 1, Figure 3b shows higher flux (and absorption) for a distance of 5 m compared to background, however, at 10 m the flux (and absorption) and background are similar.



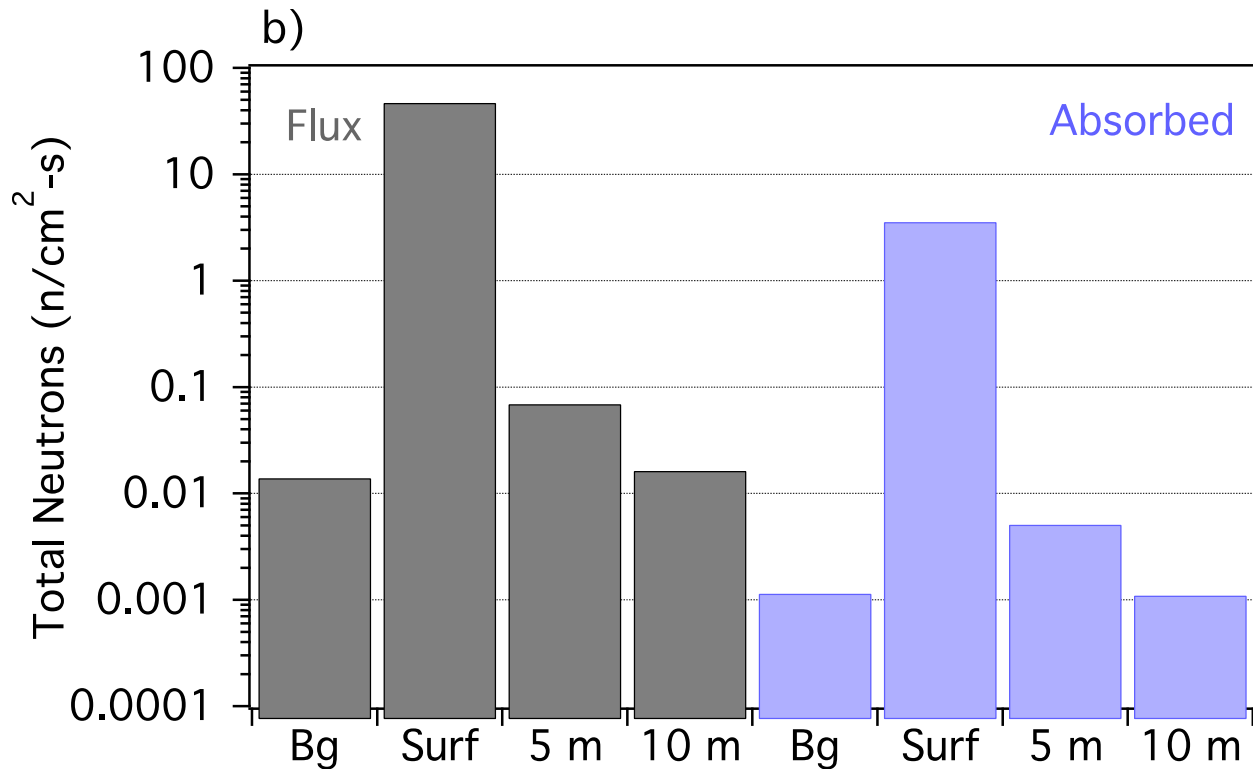
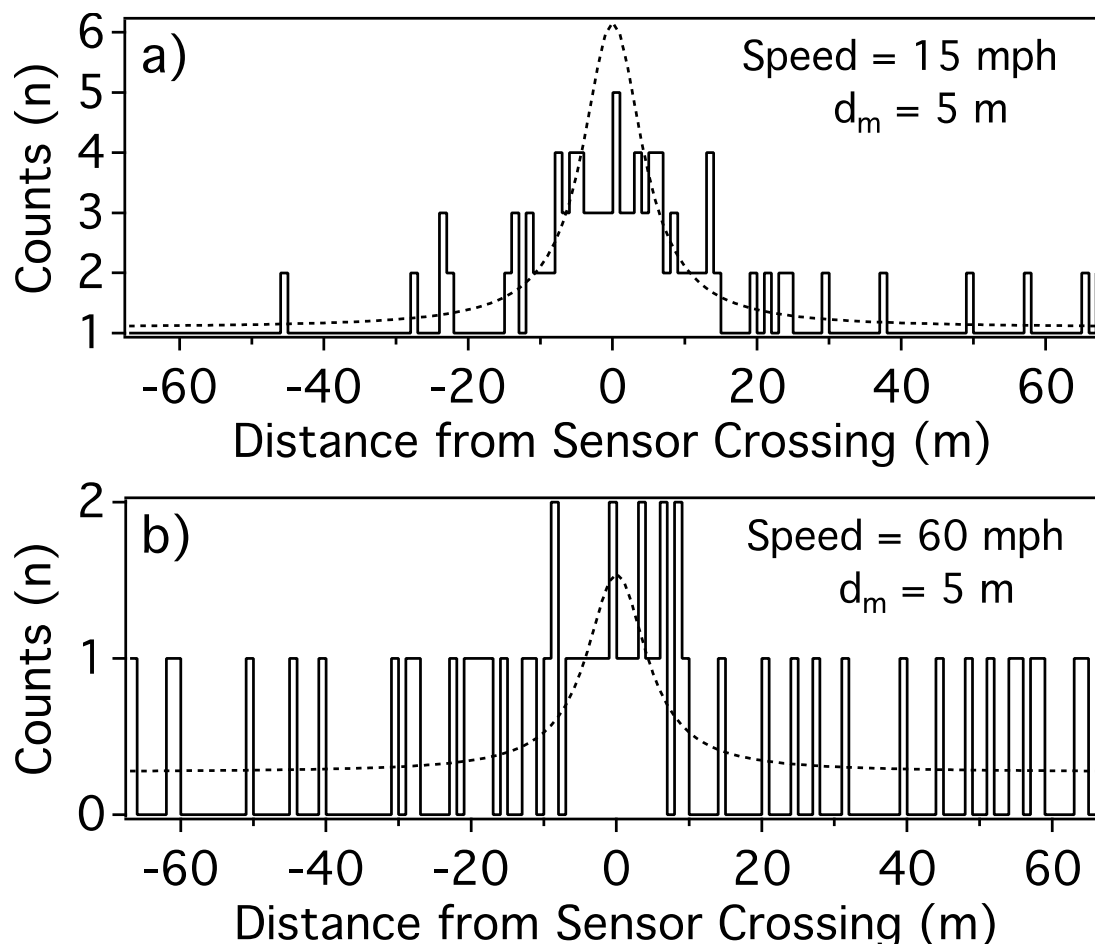


Figure 2: a) The neutron flux from WGPu at a detector distance of 5 m (solid line, black triangle markers) and due to background³⁷ (solid line, empty circle markers) is shown as a function of neutron energy. Neutron absorption into the detector as a function of neutron energy is also shown for neutrons from WGPu (dotted line, empty triangle markers) and background (dotted line, solid circle markers). On the right axis, the absorption probability for a 1 cm² portion of the ZnS-based (based on a single plate of EJ-426HD2 manufactured by Eljen Technology)³⁸ detector is shown (solid red line, star markers). **b)** Summation of the neutron spectra in a) yields the total number of neutrons incident onto the detector face (flux, in grey) on the left; while on the right the total number of neutrons absorbed into the detector (absorbed, in blue) is shown (background labeled as 'bg', source-detector separation distances of 5 and 10 m labeled as '5 m' and '10 m', respectively). In addition, the neutron flux and absorption is shown for the surface of the WGPu weapon (labeled 'Surf').

The calculations of flux and absorption only consider a single plate of the ZnS-based detector and an efficiency of converting an absorbed neutron into a detection event (count) as unity. Neutron-detector systems utilizing ZnS-based plates are likely to be formed of several plates with absorption-to-count efficiencies less than unity.³⁹ To address both these issues, it was assumed that the ZnS-based detector would meet an absolute neutron detection efficiency standard developed by R.T. Kouzes, *et al.* (2009)⁴⁰, which states that the detector would be able to generate 2.5 counts/second-nanogram from a ²⁵²Cf source at a distance of 2 m from the detector. This standard was applied to the calculation results in Figure 3 by correcting the relative efficiency of the detector to meet to the standard, thereby forming a detector that considers multiple plates and a non-unity absorption-to-count efficiency.

Once the detector was corrected with the efficiency standard of R.T. Kouzes, *et al.* (2009)⁴¹, it was scaled to an area of 1000 cm² and was studied in a traffic scenario to investigate and predict potential measurement results. The area of 1000 cm² was selected because it is

large enough to be effective in detecting WGPU at smaller distances (5 m, in this study), but is small enough to be feasible for commercial manufacturing and deployment. The traffic scenario examines the passage of a vehicle by a network detector, as in Figure 1. Figure 3a and b show sample temporal distributions of the predicted detector response and analytical response as a function of vehicle distance from crossing the detector. The responses are for total neutron counts (neutrons from WGPU and background). The analytical response is the probability of the detector producing counts from the passage of the vehicle by the detector, considering background neutrons. The predicted sample detector response discretizes the analytical response to whole counts and employs a random number generator to disperse counts according to the predicted detector response and the total number of counts within the full distance range displayed. In Figure 3c, the receiver-operator characteristic (ROC) curves show the probabilities of detecting WGPU vs. producing false alarms due to background neutrons. The ROC curves are given to exemplify the effects of vehicle speed and distance of closest approach to the detector, d_m . The distance of closest approach occurs when the vehicle is crossing nearest by the detector. Speeds were selected to approximate vehicles travelling on the highway (60 mph), using on/off ramps or roads (30 mph), and in heavy traffic or turning through an intersection (15 mph). The distance of closest approach of 5 m was selected as this distance roughly corresponds to the clearance height of a sign or bridge above a road, as in Figure 1. A distance of 10 m was selected as this distance roughly corresponds to a lane and a half of highway, including the shoulder, as in Figure 1 if the detector were placed on the ground at the base of the pole holding the traffic camera.



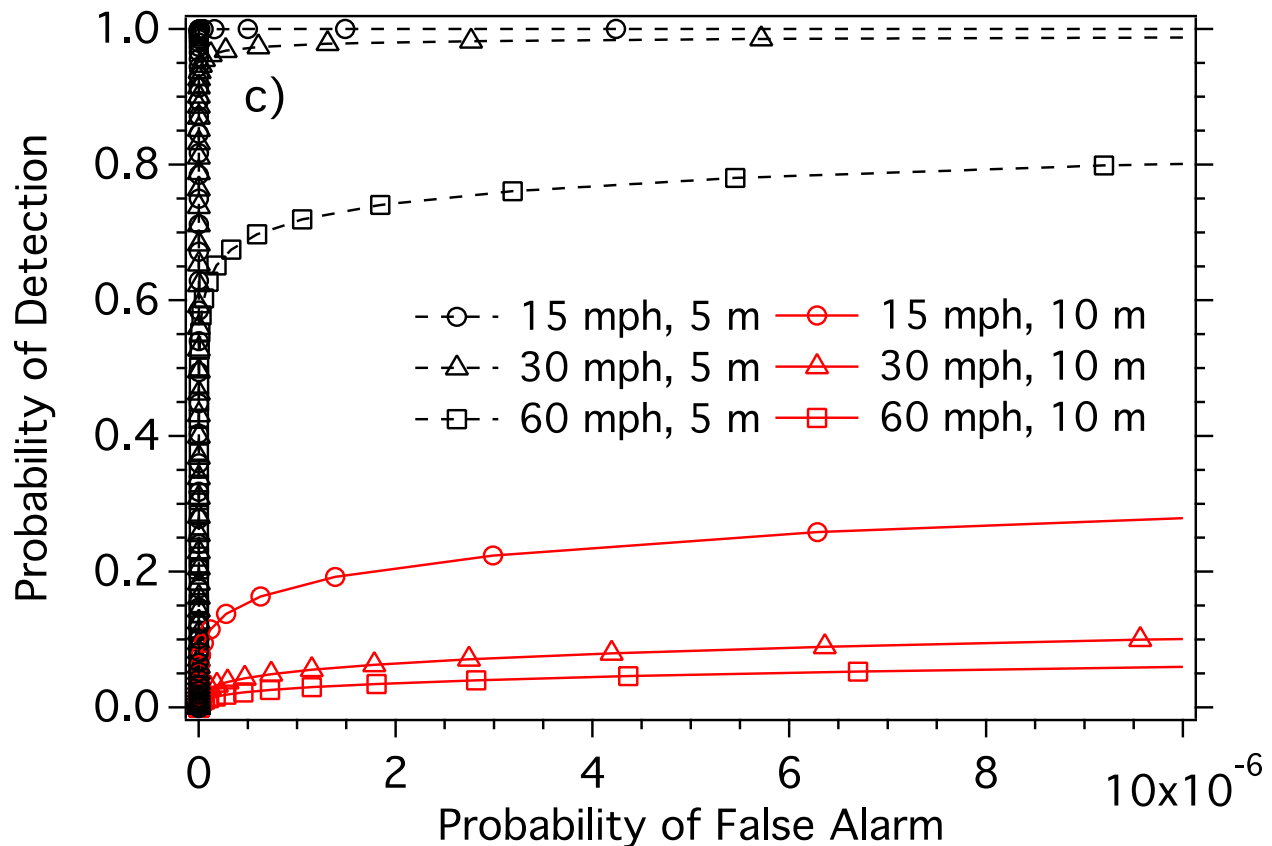


Figure 3: a) Displayed is the analytical response (dotted line) and predicted sample detector response (solid line) as a function of distance from crossing the detector for a scenario of a threat vehicle passing a network detector at minimum approach distance, $d_m = 5$ m, at a speed of 15 mph and b) 60 mph. c) The receiver operating characteristic (ROC) curves are given for $d_m = 5$ m (dotted black lines) and $d_m = 10$ m (solid red lines) for 15 (circle marker), 30 (triangle marker), and 60 (square marker) mph.

Figure 3a shows that the predictions for the passage of a vehicle containing the WGPU at a speed of 15 mph and $d_m = 5$ m would generate a clearly greater than background detector response (solid black line). Meanwhile, at a speed of 60 mph (Figure 3b), it becomes difficult to determine, by eye, the presence of the WGPU. However, according to the ROC curve in Figure 3c, the vehicle travelling at a speed of 60 mph and $d_m = 5$ m (dotted black line, black square markers) would have a fairly good probability to be detected, even for relatively small probabilities of false alarm. For $d_m = 5$ m, speeds less than 60 mph (i.e. 30 and 15 mph) have a much greater probability of detection for even smaller probabilities of false alarm. Unfortunately, at $d_m = 10$ m, the probability of detection is low compared to $d_m = 5$ m, regardless of vehicle speed. The conclusion drawn from Figure 3c is that vehicle speed is less important than distance of closest approach of vehicle to the detector, even for slower (15 mph) vehicle speed at larger distances. This conclusion is expected due to the non-linear (one over the distance squared) reduction in count-rate due to increasing distance as compared to the linear drop of count-rate due to reduction of counting time (represented by higher vehicle speed). Also, at $d_m = 5$ m detection probability is only marginally increased by slowing the vehicle lower than 30 mph. Finally, the detector is capable of detecting WGPU at $d_m = 5$ m up to highway speeds, with reasonably low probabilities of false alarm. While it is generally

expected that distance between the vehicle and detector is more important than count time (vehicle speed), the use of distance and speed parameters that closely resemble what would likely be encountered in a detector deployment scenario illustrate the importance of this effect.

Threat Interdiction and Fallout Monitoring

Detection probability rates can be increased by combining measurements of several detectors along the line of travel of a vehicle. When a sufficient number of neutrons are recorded by a detector node within a time window, as in Figure 3a, and this number is greater than a predefined threshold, a detection alarm occurs, which may activate a traffic-monitoring device such as a camera or speed tracker. This information may be used to identify and predict the line of travel of the vehicle. Should the line of travel pass by additional detector nodes, the detector measurements can be combined. By aggregating several measurements of independent detector nodes, detection probability rates can be improved by increasing the total measurement time. Importantly, information from multiple traffic-monitoring devices can confirm that the measurements are taken of a particular vehicle (by photograph, for example) and that the vehicle's time of arrival at a subsequent detector position is reasonable considering the vehicle's speed (if measured). While not examined here, of notable importance is the stochastic nature of the network's effectiveness based on possible vehicle route and placement of detectors and traffic-monitoring devices. Hence, the deployment of a detector network would benefit from a thorough study of this stochastic effect on detector placement considering any particular city's roadway layout.

Interdicting a Threat Vehicle

In the traffic-based detector network concept, detection of threatening nuclear material is only a part of the equation to help prevent nuclear terrorism. Another major aspect is the interdiction of the threat-containing vehicle. By coupling the detector with a traffic-monitoring device, the network may obtain the vehicle's identity or appearance along with information such as location, direction of travel, and speed. This information on the threat vehicle can aid local law enforcement to search for and interdict the vehicle.

A benefit of any prototype effort would be the development of the operational concept for the use of any detection alarm and the subsequent development of a command and control system that supports that operational concept. The development of concepts of operation (CONOPs) focused on detection and interdiction of a threat vehicle would require forethought into how a network detection concept may be integrated with existing communication, assessment, and response assets. Once a concept for the interdiction response is established and practiced, such a command and control system would link the processed traffic information to a dispatch system that can communicate to police in the field for interdiction.

Detector Network for Fallout Measurement

In the unfortunate circumstance that a nuclear device detonates or an accident occurs, radioactive fallout would likely be dispersed. Emergency-response personnel and resources would be distributed around the blast zone to help evacuate and triage victims. Many emergency-response personnel units carry radiation detection equipment, such as personal radiation monitors, or pagers.⁴² These radiation monitors can assess dose rate for the person wearing the device once they have already entered the fallout zone. Depending on the dose rate, the emergency responders may have limited time to conduct activities, or may have to evacuate themselves from the area. Evacuation may be tricky, due to the quickly evolving nature of fallout, which is dependent on local weather conditions. Generally, there is not an efficient method of ascertaining dose rate as a function of location and time other than the use of radiation monitors worn by emergency responders (with some exceptions, such as the deployment of radiation monitors at firehouses in the District of Columbia).⁴³ This method of assessing dose rates may place response personnel at risk of excessive radiation exposure. Time and resources may potentially be wasted if, for example, repeated redeployment is necessitated by unpredictably changing dose rates.

Given that a communications network would need to support the transfer of nodal information, the radiation detector network could provide information of fallout dose rates as a function of location and in real-time. This information may be relayed from the decision makers at the central node. While some detector nodes would be destroyed in the blast, there would still be an array of nodes outside the blast zone, depending on the size of the blast. These surviving nodes can continue operating with backup batteries in the case of loss of electrical power. However, the damage to electronics and communications due to electromagnetic pulse effects would also have to be considered and studied. There would also need to be contingencies for the event that the local central node is damaged or destroyed, such as the implementation of a remote central node.

Calculations of mRem/hr dose to count rate for $a^{137}\text{Cs}$ (662 keV) gamma ray suggest that for an unshielded ZnS-based detector the effective range of dose measurement is between 0.1 to 1000 mRem/hr. below 0.1 mRem/hr, and the gamma-ray flux at the detector is not great enough to determine the certain existence of radioactive fallout. Above 1000 mRem/hr, the detector becomes overwhelmed by the gamma-ray flux and detector dead-time and pulse pileup begins to affect the detector performance,⁴⁴ however it may still be possible to correlate detector measurements to dose above 1000 mRem/hr. The calculations do not consider the use of an electronic-based gamma-ray discrimination algorithm, which may be shut off during measurements of gamma rays. Assuming that the information from the detector network is transmitted to and processed by a central node, this information can then be forwarded to decision makers directing emergency response efforts. The range of dose that the ZnS-based detector can measure places its utility within a "hot zone" area where lifesaving activities can be conducted under close monitoring of accumulated dose of response personnel.⁴⁵ While the assessment of fallout and dose in urban environments after a nuclear blast can be predicted with computational models, the modeling results may not be immediately available. Also, dose information from the detector network provides actual data points that can be appropriated by models and compared with model results. The ability of the detector network to provide dose-rate information may be important in deciding if, when, and where emergency response personnel and resources may be deployed. The detector network can provide information of potential evacuation routes, and can track the evolution of dose from fallout.

The exact nature and evolution of the fallout would be dependent on detonation location. The detonation target and actual location where detonation takes place may not be the same. It is assumed that the likely target for the blast in many cities would be the city center. However, the actual location of the blast would be dependent on factors like size of the weapon, routes taken by the vehicles, and possible premature detonation. Assessments of likely target locations would be beneficial in determining deployment locations and densities of network nodes to prevent the weapon's detonation at the target or to redirect the detonation location to a less devastating area. Also, assessment of likely detonation locations could inform models to analyze likely routes to those locations. Modeling of likely detonation locations (and effective blast radius) would be beneficial in determining the efficacy of the network in fallout monitoring and detector-node placement. However, it is noted here that optimal placement of nodes for the objective of fallout monitoring may not be at the same locations as for the objective of threat detection (identification of vehicles on the way to a likely blast location).

Cost of a Prototype Network

The cost of deploying a prototype detector network for ground traffic is roughly estimated, producing a ROM (rough-order-of-magnitude) cost. For this estimate, the city of Washington D.C. was used as an example with detectors installed at 140 traffic-monitoring device locations, particularly all red light cameras (50 estimated)⁴⁶ and all speed traps (90 estimated)⁴⁷. The anticipated cost per installation is \$25,000, while the cost per detector is assumed to be \$200,000 for Li-based scintillating neutron detector systems.⁴⁸ The estimated ROM expenditure for deployment of a detector network for ground traffic is expected to be approximately \$32 million dollars for the city of Washington D.C. It is possible that economies of scale can reduce the cost of the detector systems, but that is not assumed. This cost also does not consider the likely significant expenditures required for communications network installation, monitoring, and maintenance, nor does it consider the cost to ensure network security standards, which are necessary to prevent hacking. The security of the communications network would likely need to be more robust and resilient to hacking than those implemented for traffic cameras.

In order to provide useful information on real false alarm rates, as well as to catalyze the development of operational responses, the system must be maintained and operated. The operational costs of the network, and of repairing and replacing parts of the network, are not estimated in detail here. Still, a very rough estimate helps bound these costs. Older, film-based, red light cameras in 2001 had operational costs of approximately \$60,000 per year per location.⁴⁹ Since this requires regular access to the camera for film change, processing, etc., the purely electronic information from the nuclear detectors is assumed to be cheaper to access, but at the same time, the cost of spare parts and maintenance might be more. Using that number, though, would indicate about \$8.4 million per year in operational costs, or approximately the acquisition cost for 4 years of operation (for Li-based detectors). This cost does not consider the operational cost of law enforcement interdiction activities, reach-back support, or cost to develop, test, and train on CONOPs.

The deployment of detectors onto mobile platforms, such as law enforcement vehicles, may add deterrence value, as discussed in Section VII. If such an approach is considered, the cost of installation of the detector is considered in this study to be negligible compared to the cost of the detector itself. Thus, the cost of deployment of the studied detectors onto

law enforcement vehicles would be approximately \$200,000 per vehicle,⁵⁰ or the cost of the detector. For the same \$31.5 million that could be used to deploy a detector network at traffic-monitoring systems (140 locations) in Washington D.C., approximately 160 law enforcement vehicles could be equipped with the same technology. It should be noted that additional studies should be carried out to assess the technical efficacy of such a method of detection and deployment. Again, this cost does not consider the operational cost of law enforcement interdiction activities, training, or reach-back support.

Determining the affordability of such a detection network is challenging due to factors such as actual damage done by a nuclear detonation (i.e. if the detonation was a full or only partial yield), location of the blast, amount of destruction and remediation of damage and fallout required, and the full cost of the network itself. One comparative scenario is the terrorist attacks on the World Trade Center in New York City on September 11th 2001. The total economic impact to New York City due to the 9/11 attacks is approximated as at least 83 billion dollars with about \$22 billion due to physical destruction and \$9 billion dollars of that accounted by human potential loss.⁵¹ Assuming that the devastation caused by a nuclear blast in a city of similar density would result in at least an order of magnitude larger area of destruction and lives lost, the economic impact could result in the magnitude of hundreds of billions to trillions of dollars in impact from physical damage and human potential loss alone. It would seem such a calculation easily suggests the affordability of deploying a detection network, which is estimated to be less than a hundred million dollars. However, there are some probabilistic points regarding the cost equivalent of the consequences of a possible attack, including: a) an actual attack is carried out, b) the weapon is Pu-based (which, also has cost implications for development and deployment of the detector network), c) the weapon is detected by the network, and d) interdiction occurs without detonation or is detonated off-target.

Potential Benefits of the Network

The described radiation detection network has several advantages not necessarily true of other detection networks. First, the detectors may be coupled with existing traffic-monitoring devices. By doing so, costs of providing power can be reduced as they may be shared with the existing traffic-monitoring device. The traffic-monitoring device can also provide supplementary information (photograph, for example) of the threat vehicle, which can be fused with detector measurements to verify measurements made by additional detector nodes and thus increase the probability of detection. The same supplementary information can be used for identifying the threat vehicle to aid in search and interdiction of the vehicle. It should be noted that there exist uncertainties in a given threat vehicle route and difficulties in detecting threat material at longer distances and shorter measurement times (faster vehicle speeds) with greater difficulty for increasing distance. While there are technical challenges in the fusion of data, such as temporally aligning detector data with traffic-monitoring information, such a concept has been previously proposed, for example, in Operation Sentinel.⁵² Second, the detector network has dual purposes: to help prevent an attack with a nuclear device by detecting and aiding the interdiction of threat materials, and to assist emergency response in the event of a nuclear attack by collecting dose-rate information as a function of location and time. Decision makers can utilize the dose-rate information to aid the determination of efficient deployment of emergency personnel and resources.

Third, the concept of the detector network can first be utilized in the development of operational CONOPs and in understanding and navigating policy implications. However, given the fairly advanced state of work of neutron detectors and their commercial availability, limitations of deploying such a detector network are beginning to shift from detector capabilities to operational considerations.⁵³ A limited prototype network that couples with traffic-monitoring systems could be set up to assess the efficacy of individual detectors and the whole network, which can be iteratively applied to improve the design and data analysis of the detectors, the network, the data they produce, and the method and means of interdiction. Importantly, the operational aspects of the use of the detection network can be established, studied, and grounded in testing experiences. They may also be integrated with other modalities of detection. As noted above, such operational aspects include the cooperation of various local, state, and federal resources to interdict a threat vehicle, or experimenting with various detector deployment locations or configurations to enhance detection probability and speedy interdiction. Development of CONOPs and exercises would provide valuable knowledge that may improve the efficiency and effectiveness of command and control systems, and threat response. The lessons learned from deploying, operating, and improving such a limited prototype network would likely provide valuable insights for other detector modalities or other types of networked threat search and monitoring. The development of CONOPs, however, would likely need additional analyses to identify the most likely targets of an attack and effective sensor-deployment locations and density to interdict approaches to these potential target epicenters.

Potential Drawbacks of the Network

The radiation detection network explored in this work also has some drawbacks. Unpredictability of node locations or node density may help to deter nefarious activities by adding an unknowable aspect to an adversary's plan. However, in this concept, unlike some radiation detector networks that are based on moving, unlocatable, or otherwise unpredictable node locations or density, the detectors of the network in this work are fixed in location. Not only are the locations of the detectors fixed, but also they are knowable since the detectors are deployed in the vicinity of a traffic-monitoring device.

To overcome the important issue of unpredictability and deterrence of the network, moving detector nodes should be also explored, which would be an addition to and would work in cooperation with the network. Such moving nodes may include detectors installed on vehicles. Given the size of the detector studied (1000 cm²), mobile detector systems could be deployed on law enforcement vehicles, for example, that monitor nearby or passing vehicles for the presence of WGPu. In the occurrence of a detection alarm, the law enforcement vehicle carrying the detector could attempt to follow the potential threat vehicle to accumulate longer measurement times, lowering the probability of false alarm. The advantages of identification of the threat vehicle for aiding interdiction, as carried out by the coupling with traffic-monitoring systems, would be assumed by the law enforcement officer. Mobile platforms could increase deterrence value by adding uncertainty to the prospect of being discovered, as the presence of law-enforcement vehicles or which ones are equipped with a detection system cannot be preplanned by an adversary. Another method to increase deterrence value is the deployment of dummy detectors, or equipment that mimics the appearance of a functional detector system. These dummy detectors would add deterrence value by varying the adversary's calculus of planning to avoid detection. Adversaries may

reconsider executing an attack, given an encounter with a much larger and denser network of potentially functional detectors. Even with the knowledge that some detectors are dummies, not knowing which ones are functional would add some deterrence value to the detection network concept.

Second, for the passive detectors investigated in this study, the use of sufficient amounts of appropriate shielding can attenuate neutrons exiting the source, hiding the nuclear material from the detector. Such shielding certainly complicates the plan to transport a weapon, which would have some indeterminate deterrent effect, but it is feasible. In the case of shielding, parameters of network node density, detector size, vehicle speed, or source-detector distance may be of little importance. In part, it is because of this shielding problem that active interrogation detector systems are a large and essential part of on-going research in the field of nuclear-materials detection.⁵⁴

Third, the detection probability of a detector within the network was analyzed for only WGPu due to the relatively small number of neutrons emitted from uranium. It is estimated that the detection of uranium would not be feasible in the network-detection concept for ground-based traffic. This leaves a sizable gap in nuclear materials detection capability.

Comparison with Other Alternatives

There are alternatives to the concept explored in this paper for threat-source search and post-blast fallout and radiation monitoring. Some of these alternatives include the deployment of personal radiation detectors (PRDs) onto law enforcement and first responder vehicles and personnel, or the use of radiation sensors on unmanned aerial vehicles (UAVs). Both of these alternative concepts may be utilized in threat-source search and post-blast radiation and fallout monitoring. Here, we will briefly examine some of the costs, benefits, and drawbacks of these alternatives. Another strategy to source-search is the scanning of vehicles and cargo at border crossings, ports, and airports. This strategy relies on a wall-like defense against the smuggling of nuclear materials into the country. This strategy will also be briefly discussed.

Personal radiation detectors (PRDs) are typically belt-worn or handheld pager-sized detectors with electronics that allow ease of use and customized setting of exposure alarm, all at a price usually below \$10,000 per unit.⁵⁵ They can be worn by law enforcement officers and first responders, and the concept of implementing them as part of the strategy to detect nuclear and radiological materials has already been undertaken as part of "Securing the Cities" program of DHS.⁵⁶

A first approximation of the number of PRDs that would likely be worn by law enforcement officers in D.C., for example, would be 2800, or the number of body cameras deployed.⁵⁷ The officers who would wear body cameras are also likely the officers that would provide operational impact to nuclear materials search and radiation monitoring by wearing PRDs. Considering a lower-end price of \$2,000 per PRD would bring the total equipment cost to \$5.6 million, or about 17.5% of the equipment cost of the traffic detector network. The equipment cost does not consider required training, reach-back support, or cost to respond to detection-alert scenarios. A benefit of these detectors is the ability to distribute them widely, due to the low price point per unit. Another benefit is that the PRD can alert officers, who already have some authority to stop attacks and maintain public safety, to localized

elevated rates of radiation. Yet another benefit is the relatively random distribution of law-enforcement officers and their PRDs about a city. While an adversary may likely try to avoid close proximity to an officer, this cannot be guaranteed, thereby adding to deterrence. A drawback of PRDs is their significantly smaller volume of detection (typically no larger than a few cm²), which requires the detector to be in much closer proximity to the radiation source or to have much longer dwell time than the detector analyzed for the traffic network concept.

Another alternative to source-search and post-blast fallout and radiation monitoring is the use of radiation detectors on unmanned aerial vehicles (UAVs). The technology of compact UAVs has advanced significantly in the past years to the point where UAVs equipped with radiation detection capabilities are commercially available. While many of these systems are designed for gamma-ray detection, a custom setup could be built, using a detector panel from the traffic detector network concept fixed onto a UAV. A 1000 cm² ZnS:LiF detector would weigh approximately 3 lbs.⁵⁸ Even with required electronics and power supply, the weight of the detection system would be within the payload capacity of current commercially available UAVs (20-25 lbs.), such as the DJI Agras MG-1.⁵⁹

If we use the DJI Agras MG-1 as an example, the cost per UAV is approximately \$15,000. With the previously calculated cost per detector at \$200,000,⁶⁰ the equipment cost per detector-equipped UAV comes to \$215,000. This does not consider the cost of required communications systems, reach-back support, usage training, or any modifications to extend flight time or range. If we consider the number of UAV detector systems to equal the number of traffic-based detector systems (140), the total equipment cost of this alternative is \$30.1 million, which is approximately equal to that of the traffic-based detector network concept cost.

A benefit of UAV-based detection concept is the control, within the limits of the physical range and battery life of the UAV, of where, when, and for how long the detectors dwell at a location. Another benefit is the ability to follow objects of interest (within the speed limitation of the UAV) or bring multiple detectors to a point of interest for better detection capability. In post-blast fallout and radiation monitoring, UAVs have an advantage of potentially being deployed after the blast, thereby preserving them from destruction. They also have the advantage of being mobile to assess radiation levels along evacuation routes or to develop understanding of the nature of the fallout due to weather conditions. Drawbacks, however, can be operationally substantial with limitations on the operation time and range of a given UAV. Additionally, while the CONOPs of a UAV-based system would need to be fleshed out, perpetual deployment would seem unlikely. The UAVs would instead likely be deployed during major events (e.g. sporting events) or in response to information that threat material was in the area or that an attack was imminent. This contrasts with the relatively perpetual operation of the detectors in the traffic-based concept. However, when UAVs are deployed in source-search, deterrence value is added due to the highly mobile nature of the UAVs.

An alternative to placing detectors in urban environments is the strategy of scanning vehicles and cargo coming into the U.S. through ports, airports, and border crossings, which is already carried out by DND in cooperation with other federal agencies.⁶¹ As this line of defense is a fundamental part of preventing nuclear smuggling into the U.S., it should strive continuously for improvement. Covert field tests of the integrity of this line of defense were carried out by the CBP and showed varied levels of success. A Government Accountability Office report recommended a risk-assessment study should be conducted to prioritize the makeup and deployment of resources.⁶² Additionally, an unavoidable deficiency with this defense includes susceptibility to circumvention by going around or avoiding known checkpoints.⁶³ While there may be some deficiencies with this particular line of defense, it is

part of a multi-layered defense strategy of the GNDA that also includes inland inspection of trucking cargo at weigh stations.⁶⁴ The concept of a traffic-based detector network explored in this article is not intended as a replacement for existing defenses but may be integrated as yet another layer of this multi-layered strategy. In the event that port, airport, or border detection fails, the traffic-based detector network provides scanning opportunities at likely targets of substantial devastation – in the cities.

A strong defense against a nuclear attack would likely rely on the combination of detection concepts. The benefits of the described concepts may overlap to overcome drawbacks. In any case, CONOPs of the system would need to be developed, which ideally emphasize the key benefits of each concept, such as the pervasiveness of PRDs, mobility of UAVs, and operational perpetuity of traffic-based detectors. The radiation detection concepts discussed here could also become a part of the multi-layered defense strategy that includes the GTRI, which secures nuclear materials and processes at facilities,⁶⁵ and the GNDA, which seeks to reduce the risk of nuclear attacks by inspection of cargo, vehicles, and persons travelling into the U.S. through ports, airports, or border crossings.⁶⁶

Conclusion

The threat of nuclear terrorism to U.S. cities is serious and the consequences of such an attack would be significant. The potential consequences of a nuclear detonation in a city include loss of life, widespread destruction, and a substantial negative impact on the economy. The U.S. government has responded by establishing and supporting agencies, such as the NNSA and the DNDO, with the purpose of reducing the threat of nuclear terrorism. These agencies advance programs that reduce and secure nuclear materials and strengthen inspection regimes at home and abroad. These agencies and others (such as the Defense Threat Reduction Agency and the Defense Advanced Research Projects Agency) along with their parent departments (DOE, DHS, and DOD) have made appreciable investments into radiation-detection technologies and research to help track, scan, and search for nuclear materials and weapons.

This article reviews and investigates one such concept in terms of technical feasibility – the use of radiation detectors in a networked configuration and deployed next to roads for ground-based traffic monitoring with the possibility of deployment onto mobile platforms. This investigation lays out the basis of the concept, however analysis of the integration of such a network with command and control systems, the details of the operational process, and assessing the likely epicenter targets, vehicle travel routes, and optimal placement of detectors is also required for any successful development of even a prototype test network.

Detectors within the network measure the presence of neutron radiation from nuclear materials and weapons that may be contained in passing vehicles. The detectors would be deployed at existing traffic-monitoring system locations (stop light or red light cameras, for instance) such that when a detection alarm occurs, the traffic-monitoring device can be activated to identify the threat vehicle. While not explicitly analyzed here, additional detector measurements and traffic-monitoring device information may be taken along a vehicle's line of travel to verify vehicle identity and increase the certainty of detection. Other aspects of the concept not explored here but which would require further investigation are how measurements from the detector and information from the traffic-monitoring device would be communicated to a central node, how that information is fused and interpreted, and the

decision-making process of vehicle interdiction. If interdiction were carried out, information from the traffic-monitoring device(s) would aid the search for the threat vehicle. In a scenario in which a nuclear weapon detonation or nuclear accident has already occurred, the detector network could provide location and time-dependent measurements of radioactive fallout. Measurements of dose rate can be fed to the central node, interpreted, and utilized to aid in the decision-making for the deployment of emergency-response personnel and resources. Here again, transfer and interpretation of information, and decision-making are aspects that would require in-depth investigation.

The study finds that the detection network concept appears to be feasible for neutron detection of weapons grade plutonium, but not uranium, up to highway speeds (60 mph) at a minimum detector distance of 5 m from the plutonium, which is plausible. The neutron emission from weapons-grade uranium, compared to background, was estimated to be too low to be detected by a detector in the concept of ground-based traffic. At a minimum detector distance of 10 m from the plutonium, the detector is capable of detecting the presence of plutonium but at relatively low probabilities of detection. It was shown that decreasing the minimum detector distance from the plutonium is more important than the vehicle speed for the speeds studied (15, 30, 60 mph).

Opportunities for Future Work

Future work analyzing the detector network for ground-based traffic concept should include the evaluation of other neutron (other than ZnS-based) detector types and detector sizes to optimize the potential efficacy of the network and/or minimize costs, and should examine how to fuse the detector measurement and traffic-monitoring system information in order to identify a threat vehicle. Further studies should explore the effect of aggregating multiple detector measurements and investigate the concept of moving detector nodes to enhance the detection network concept's deterrence value. Additional future work should also be carried out to understand the effects of shielding on detection capabilities, traffic-flow modeling for optimal detector placement, and likely epicenter targets and blast radii for understanding the capability of the network for fallout monitoring. This additional future work would reveal limitations of the concept that may affect its overall feasibility or point to aspects of the concept which may be strengthened. Finally, future work should also be carried out to explore the effectiveness of the combination of multiple detection modalities.

Importantly though, the concept explored here is not expected to be only solution to the challenging issue of nuclear terrorism. Instead, further investigation should be carried out to explore how this traffic-based detector network concept and potential alternative technologies and concepts can be appropriately mixed to strengthen the layered defense homeland security strategy to prevent nuclear terrorism.

About the Author

Edward Cazalas is an Assistant Professor of the Nuclear Engineering program within the Civil and Environmental Engineering Department at the University of Utah. Edward was also a former postdoctoral researcher at the Air Force Institute of Technology and a former Stanton Nuclear Security Postdoctoral Fellow at RAND Corporation where he performed the origination of this work. Edward holds a Ph.D. in Nuclear Engineering from the Pennsylvania State University. He has research interests in developing radiation-detection science and technologies and advancing the understanding of dosimetry for nuclear and radiological exposure events and processes. He may be reached at edward.cazalas@utah.edu.

Notes

- 1** C. Meade, & R.C.Molander, *Considering the Effects of a Catastrophic Terrorist Attack*, Santa Monica, CA: RAND Corporation (2006), Available at: http://www.rand.org/pubs/technical_reports/TR391.html.
- 2** Bunn, et al., *Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?* Cambridge, MA: Report for Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School (2016).
- 3** National Nuclear Security Administration, Prevent, Counter, and Respond – A Strategic Plan to Reduce Global Nuclear Threats (2017) https://www.energy.gov/sites/prod/files/2017/11/f46/fy18npcr_final_november_2017%5B1%5D_0.pdf.
- 4** K. Guthe, "The Global Nuclear Detection Architecture and the Deterrence of Nuclear Terrorism," *Comparative Strategy* **33**, 424–450 (2014).
- 5** W.Stern and E. Baldini, "Global Threat Reduction Initiative Efforts to Prevent Radiological Terrorism," *Federation of American Scientists: Public Interest Reports* **44** (2013).
- 6** L.Cuéllar, et al., "Probabilistic Effectiveness Methodology: A Holistic Approach on Risk Assessment of Nuclear Smuggling," *IEEE International Conference on Technologies for Homeland Security*, 325–331 (2011).
- 7** S. Fetter et al., "Detecting Nuclear Warheads," *Science and Global Security* **1**, 225–253 (1990).
- 8** A.D. Lavietes et al., "Technical Review of the Domestic Nuclear Detection Office Transformational and Applied Research Directorate's Research and Development Program," *IEEE Access* **1**, 661–690 (2013).
- 9** T. Kijewski-Correa et al., "Real-time Plume Detection in Urban Zones Using Networked Sensing Data," *Proceedings of Chem-Bio Defense Physical Science and Technology Conference* (2008).
- 10** R.W. Nelson, "Concept of Operations for CBRN Wireless Sensor Networks," (Naval Postgraduate School, 2012).
- 11** B.R. Buddemeier et al., *National Capital Region Key Response Planning Factors for the Aftermath of Nuclear Terrorism*, Lawrence Livermore National Laboratory, LLNL-TR-512111 (2011).
- 12** International Atomic Energy Agency, *Manual for First Responders to a Radiological Emergency*, (2006), available at: <https://www-pub.iaea.org/books/IAEABooks/7606/Manual-for-First-Responders-to-a-Radiological-Emergency>.
- 13** C. Meade and R.C. Molander, *Considering the Effects of a Catastrophic Terrorist Attack*, (Santa Monica, CA: RAND Corporation, 2006), Available at: http://www.rand.org/pubs/technical_reports/TR391.html; U.S. Department of Homeland Security, *Quadrennial Homeland Security Review*, (2014) available at: <https://www.dhs.gov/quadrennial-homeland-security-review>.
- 14** A. Liu, Simulation and Implementation of Distributed Sensor Network for Radiation Detection, Master's Thesis, California Institute of Technology, Pasadena, CA, 2010.
- 15** Defense Advanced Research Projects Agency, DARPA SIGMA (2016), available at: <http://www.darpa.mil/program/sigma>.
- 16** Department of Homeland Security, FY 2016 Congressional Budget Justification, (2016), available at: <https://www.dhs.gov/publication/congressional-budget-justification-fy-2016>.
- 17** T. Kijewski-Correa, et al., "Real-time Plume Detection in Urban Zones Using Networked Sensing Data," *Proceedings of Chem-Bio Defense Physical Science and Technology Conference* (2008); S.M. Brennan, A.M Mielke, and D.C. Torney, "Radioactive Source Detection by Sensor Networks," *IEEE Transactions on Nuclear Science* **52**, 813–819 (2005).
- 18** R.J. Nemzek et al., "Distributed Sensor Networks for Detection of Mobile Radioactive Sources," *IEEE Transactions on Nuclear Science* **51**, 1693–1700 (2004); J.C. Chin et al., "Identification of Low-level Point

- Radioactive Sources Using a Sensor Network," *ACM Transactions on Sensor Networks* **7**, 21:1–21:35 (2010); D.S.Hochbaum and B.Fishbain, "Nuclear Threat Detection with Mobile Distributed Sensor Networks," *Annals of Operations Research* **187**, 45–63 (2011); H.Wan, T. Zhang and Y.Zhu, "Detection and Localization of Hidden Radioactive Sources with Spatial Statistical Methods," *Annals of Operations Research* **192**, 87–104 (2012); K. Grunden, G. Guerra and W. Leonard, *Ubiquitous (CB)RN(E) Sensor Networks: Analysis and Framework Study*, TASC INC. (2014); L.M. Wein and M.P. Atkinson, "The Last Line of Defense: Designing Radiation Detection-Interdiction Systems to Protect Cities from a Nuclear Terrorist Attack," *IEEE Transactions on Nuclear Science* **54**, 654–669 (2007).
- 19** Y. Yang *et al.*, "A Network Protocol Stack Based Radiation Sensor Network for Emergency System," *International Journal of Computer Science and Network Security* **8**, 312–318 (2008); F. Ding *et al.*, "A GPS-Enabled Wireless Sensor Network for Monitoring Radioactive Materials," *Sensors and Actuators A: Physical* **155**, 210–215 (2009).
- 20** R.W. Nelson, "Concept of Operations for CBRN Wireless Sensor Networks," (Naval Postgraduate School, 2012); D. Srikrishna, A.N Chari and T.Tisch, "Deterrence of Nuclear Terrorism with Mobile Radiation Detectors," *Nonproliferation Review* **12**, 573–614 (2005); S. Johnson, "Stopping Nuclear Terrorism is a Game of Odds, Not Certainty," *Wired* (2015).
- 21** D. Srikrishna, A.N Chari and T. Tisch, "Deterrence of Nuclear Terrorism with Mobile Radiation Detectors."
- 22** A. Mauroni, "Nuclear Terrorism: Are We Prepared?" *Homeland Security Affairs* **8**, Article 9 (June 2012). <https://www.hsaj.org/articles/222>.
- 23** R.Harney, "Inaccurate Prediction of Nuclear Weapon Effects and Possible Adverse Influences on Nuclear Terrorism Preparedness," *Homeland Security Affairs* **5**, Article 3 (September 2009). <https://www.hsaj.org/articles/97>.
- 24** Government Accountability Office, *Neutron Detectors: Alternatives to Using Helium-3*, GAO-11-753 (2011).
- 25** G.F. Knoll, *Radiation Detection and Measurement*, 3rd Ed. (Wiley, 2011).
- 26** G.W. Philips, D.J. Nagel and T. Coffey, *A Primer on the Detection of Nuclear and Radiological Weapons*. Defense Technology Paper 13 (2005); G.E. McMath, G.W. McKinney and T. Wilcox, *MCNP6 Cosmic & Terrestrial Background Particle Fluxes – Release 4*, Los Alamos National Laboratory, LA-UR-14-24445 (2015).
- 27** S. Fetter *et al.*, "Detecting Nuclear Warheads," *Science and Global Security* **1**, 225–253 (1990).
- 28** G.W. Philips, D.Nagel, and T.Coffey, *A Primer on the Detection of Nuclear and Radiological Weapons*, Defense Technology Paper 13 (2005); G.E. McMath, G.W. McKinney and T. Wilcox, *MCNP6 Cosmic & Terrestrial Background Particle Fluxes – Release 4*. Los Alamos National Laboratory, LA-UR-14-24445 (2015).; S.Fetter *et al.*, "Detecting Nuclear Warheads."
- 29** S. Fetter *et al.* "Detecting Nuclear Warheads."
- 30** T. Goorley, *MCNP6.1.1-Beta Release Notes*, (2014).
- 31** S. Fetter. *et al.*, "Detecting Nuclear Warheads."
- 32** G.W. Philips, D. Nagel and T. Coffey, *A Primer on the Detection of Nuclear and Radiological Weapons*.
- 33** J.H. Ely *et al.*, *Final Technical Report for the Neutron Detection without Helium-3 Project*, (2013), Pacific Northwest National Laboratory, PNNL-23011 (2013).
- 34** S. Fetter *et al.*, "Detecting Nuclear Warheads."
- 35** *Thermal Neutron Detector EJ-426*, Eljen Technology (2016), available at: <http://www.eljentechnology.com/index.php/products/neutron-detectors/ej-426>.
- 36** Brookhaven National Laboratory - *Evaluated Nuclear Data File (ENDF/B-VII.1)*, National Nuclear Data Center (2011), available at: <https://www.nndc.bnl.gov/exfor/endl00.jsp>.
- 37** S. Fetter *et al.*, "Detecting Nuclear Warheads."

- 38** *Thermal Neutron Detector EJ-426*, Eljen Technology (2016), available at: <http://www.eljentechnology.com/index.php/products/neutron-detectors/ej-426>.
- 39** J.H. Ely *et al.*, *Final Technical Report for the Neutron Detection without Helium-3 Project*.
- 40** R.T. Kouzes *et al.*, *Neutron Detector Gamma Insensitivity Criteria*, Pacific Northwest National Laboratory, PNNL-18903 (2009).
- 41** Ibid.
- 42** B.R. Buddemeier *et al.*, *National Capital Region Key Response Planning Factors for the Aftermath of Nuclear Terrorism*, Lawrence Livermore National Laboratory, LLNL-TR-512111 (2011).
- 43** Ibid.
- 44** J.H. Ely *et al.*, *Final Technical Report for the Neutron Detection without Helium-3 Project*; J.B. Mosset *et al.*, "Evaluation of Two Thermal Neutron Detection Units Consisting of ZnS/6LiF Scintillating Layers with Embedded WLS Fibers Read Out with a SiPM," *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* **764**, 299–304 (2014).
- 45** B.R. Buddemeier *et al.*, *National Capital Region Key Response Planning Factors for the Aftermath of Nuclear Terrorism*.
- 46** *Red-Light Camera Locations*, Metropolitan Police Department (2016), available at: <https://mpdc.dc.gov/publication/automated-traffic-enforcement-camera-locations>.
- 47** *Speed Camera Locations*, Metropolitan Police Department (2016), available at: <https://mpdc.dc.gov/publication/automated-traffic-enforcement-camera-locations>.
- 48** Centers for Disease Control and Prevention, *Injury Prevention & Control: Motor Vehicle Safety – Invention Fact Sheets for Automated Enforcement*, (2015), available at: <http://www.cdc.gov/motorvehiclesafety/calculator/factsheet/redlight.html>.
- 49** Ibid.
- 50** Department of Homeland Security, *Standoff Radiation Detectors Market Survey Report*, National Urban Security Technology Laboratory (2013).
- 51** W.C. Thompson, *One Year Later - The Fiscal Impact of 9/11 on New York City*, Report by the Comptroller of the City of New York, 2002.
- 52** A. Baker, "City Would Photograph Every Vehicle Entering Manhattan and Sniff Out Radioactivity," *The New York Times*, (2008).
- 53** R. Stone, "Researchers Rise to the Challenge of Replacing Helium-3," *Science*. **353**, 15-16 (2006).
- 54** A.D. Laviertes *et al.*, "Technical Review of the Domestic Nuclear Detection Office Transformational and Applied Research Directorate's Research and Development Program," *IEEE Access* **1**, 661–690 (2013); J. Medalia, *Detection of Nuclear Weapons and Materials: Science, Technologies, Observations*, Congressional Research Service, R40154 (2010).
- 55** Department of Homeland Security, *Personal Radiation Detectors (PRDs) and Spectroscopic PRDs Market Survey Report*, National Urban Security Technology Laboratory (2017).
- 56** Department of Homeland Security, Domestic Nuclear Detection Office, FY 2018 Congressional Budget Justification, (2018), available at: https://www.dhs.gov/sites/default/files/publications/CFO/17_0524_Domestic_Nuclear_Detection_Office.pdf.
- 57** Metropolitan Police Department, Annual Report (2016), available at: https://mpdc.dc.gov/sites/default/files/dc/sites/mpdc/publication/attachments/MPD%20Annual%20Report%202016_lowres.pdf#page=41.

- 58** M. Schear *et al.*, "Monte Carlo Modeling and Experimental Evaluation of a 6LiF:ZnS(Ag) Test Module for Use in Nuclear Safeguards Neutron Coincidence Counting Applications (IAEA-CN--220)," Symposium on International Safeguards, International Atomic Energy Agency (2015).
- 59** G. J. Herrera, J.A. Dechant and E.K Green, "Technology Trends in Small Unmanned Aircraft Systems (sUAS) and Counter-UAS: A Five-Year Outlook," Institute for Defence Analyses (2017).
- 60** Centers for Disease Control and Prevention, *Injury Prevention & Control: Motor Vehicle Safety – Invention Fact Sheets for Automated Enforcement* (2015), available at: <http://www.cdc.gov/motorvehiclesafety/calculator/factsheet/redlight.html>.
- 61** K. Guthe, "The Global Nuclear Detection Architecture and The Deterrence of Nuclear Terrorism."
- 62** Government Accountability Office, *Combating Nuclear Smuggling: Risk-Informed Covert Assessments and Oversight of Corrective Actions Could Strengthen Capabilities at the Border*, GAO-16-191T (2015).
- 63** L. Zaitseva and F. Stienhausler, "Illicit Trafficking of Weapons-Usable Nuclear Material: Facts and Uncertainties," *Physics & Society*, American Physical Society, vol. 33, no. 1 (2004).
- 64** K. Guthe, "The Global Nuclear Detection Architecture and the Deterrence of Nuclear Terrorism," Multimodal Integrated Safety, Security and Environmental Program Strategy, Transportation Research Board, 87th Annual Meeting, 08-2644 (2008).
- 65** National Nuclear Security Administration, *Preventing Proliferation of Nuclear Materials and Technology* (2011), available at: <https://nnsa.energy.gov/mediaroom/factsheets/dnnfactsheet2011>.
- 66** K. Guthe, "The Global Nuclear Detection Architecture and The Deterrence of Nuclear Terrorism."

Copyright © 2018 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS). Cover image by [Millertime83](#)



CENTER FOR HOMELAND
DEFENSE AND SECURITY

NAVAL POSTGRADUATE SCHOOL

SPONSORED BY

U.S. DEPARTMENT OF HOMELAND SECURITY
NATIONAL PREPAREDNESS DIRECTORATE, FEMA



FEMA

THE NATION'S HOMELAND SECURITY EDUCATOR