

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 21-04-2015		2. REPORT TYPE Master of Military Studies Research Paper		3. DATES COVERED (From - To) September 2014 - April 2015	
4. TITLE AND SUBTITLE The Electronic Counterinsurgency: Enabling Virtual Resistance Networks in the Megacity				5a. CONTRACT NUMBER N/A	
				5b. GRANT NUMBER N/A	
				5c. PROGRAM ELEMENT NUMBER N/A	
6. AUTHOR(S) Relihan, Colin R.				5d. PROJECT NUMBER N/A	
				5e. TASK NUMBER N/A	
				5f. WORK UNIT NUMBER N/A	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068				8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A				10. SPONSOR/MONITOR'S ACRONYM(S) N/A	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES N/A					
14. ABSTRACT A U.S. joint military/interagency task force can identify, enable, and protect electronic social networks in a megacity environment to provide both intelligence and information operations (IO) advantage. A JIATF can take advantage of the megacity's connectivity, global links, and density to support layered defenses for these virtual resistance networks (VRN) in the face of coercion by non-state armed groups. It will be impossible to isolate megacities of the future because of three qualities: their increased electronic connectivity, globalized social and economic links, and high population and commercial density. Growing penetration of cellular phones, Internet, and social media use means there are new opportunities to gather information on dense, rapidly changing urban environments. But violent non-state actors can create "zones of silence" by targeting online activists, discouraging local resistance and reporting. The paper develops the proposed VRN enable/protect operating concept, which seeks to leverage the advantages of large-scale open-source information networks to combat non-stated armed groups while minimizing security risks to local VRN participants. A JIATF can take advantage of the megacity's connectivity, global links, and density to support layered defenses for VRNs. This concept will likely blur the line between intelligence collection, information operations, and civilian security.					
15. SUBJECT TERMS Megacity, open-source, intelligence, information operations, social media, crowdsourcing, diasporas, Mexico, Los Zetas, social n					
16. SECURITY CLASSIFICATION OF: Unclass			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 62	19a. NAME OF RESPONSIBLE PERSON Marine Corps University/Command a
a. REPORT Unclass	b. ABSTRACT Unclass	c. THIS PAGE Unclass			19b. TELEPHONE NUMBER (include area code) (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

**TITLE: The Electronic Counterinsurgency: Enabling Virtual Resistance Networks in the
Megacity**

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Colin Relihan

AY 14-15

Mentor and Oral Defense Committee Member: Benjamin Jensen, PhD
Approved: [Signature]
Date: 25 Apr 2015

Oral Defense Committee Member: Jonathan F. Phillips, PhD
Approved: [Signature]
Date: 28 Apr 2015

Executive Summary

Title: The Electronic Counterinsurgency: Enabling Virtual Resistance Networks in the Megacity

Author: Colin Relihan

Thesis: A U.S. joint military/interagency task force can identify, enable, and protect electronic social networks in a megacity environment to provide both intelligence and information operations (IO) advantage. A joint task force can take advantage of the megacity's connectivity, global links, and density to support layered defenses for these virtual resistance networks (VRN) in the face of coercion by non-state armed groups.

Discussion: The growing number and importance of megacities in the future environment means the U.S. military will need to develop methods to operate there. It will be impossible to isolate major urban centers because of three qualities of the future megacities: increased electronic connectivity, globalized social and economic links, and high population and commercial density. Growing penetration of cellular phones, Internet, and social media use means there are new opportunities to gather information on dense, rapidly changing urban environments. But violent non-state actors can create "zones of silence" by targeting online activists, discouraging local resistance and reporting.

The paper develops the proposed VRN enable/protect operating concept, which seeks to leverage the advantages of large-scale open-source information networks to combat non-stated armed groups while minimizing security risks to local VRN participants. A JIATF can take advantage of the megacity's connectivity, global links, and density to support layered defenses for VRNs in the face of coercion by non-state actors. So protected, the VRN will be both a likely source of information for the joint force commander and will send a clear message that the local population is able to act collectively to resist violence. In the long-run the VRNs become agents for internal change, as it can pressure the host nation government to improve its security and governance performance.

Conclusion: The VRN enable/protect concept will likely blur the line between intelligence collection, information operations, and civilian security, requiring deeper levels of cooperation between the military force, interagency elements, and the local population. But it provides benefits to the future joint force commander seeking options to operate inside an urban area without destroying that city's sources of vitality and resiliency.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents

SUMMARY	Page 2
DISCLAIMER	3
ACKNOWLEDGMENTS	5
GLOSSARY OF ACRONYMS	6
REPORT DOCUMENTATION PAGE	7
THE ELECTRONIC COUNTERINSURGENCY: ENABLING VIRTUAL RESISTANCE NETWORKS IN THE MEGACITY	9
The Promise of Social Media and Crowdsourcing for Intelligence and Information Operations	9
Problem: Globalized Megacities and Physical Violence versus Virtual Networks	13
Military/Interagency Operating Concept: Enabling and Protecting Virtual Resistance Networks in the Urban Environment	22
Concept Overview	22
Exploiting the Megacity’s Connectivity, Globalization, and Density	24
Countering Non-State Armed Group Attacks on the Virtual Resistance Network	27
Concept Scope, Limitations, and Risks	29
Virtual Resistance Network Enabling/Protection by Warfighting Function	32
Command and Control (C2)	32
Intelligence	33
Fires (Information Operations/Cyberspace)	35
Movement and Maneuver	37
Protection	38
Sustainment	39
Required Capabilities	39
Conclusion	40
APPENDIX CASE STUDY	
CARTEL VERSUS CITIZEN: INFORMATION OPERATIONS, OPEN-SOURCE INTELLIGENCE, AND PUBLIC RESISTANCE IN NORTHERN MEXICO	43
Background	44
Cartel Intimidation and Traditional and Electronic Forms of Public Resistance	46
Mexico’s Lessons Learned for Public Resistance Against Non-State Threats	53
BIBLIOGRAPHY	57

Acknowledgments

I would like to first and foremost thank my master's advisor and director for the Marine Corps Command and Staff College's Advanced Studies Program (ASP), Dr. Benjamin Jensen. His focus on the urban warfighting in this year's ASP and continual supply of new articles, concepts, and challenges truly made the development of this MMS paper possible. His guidance and support was crucial in the development of this proposed operating concept. I would also like to thank Dr. Eric Shibuya and Dr. Jonathan Phillips for their support, particularly for their comments on my Mexico case study and for developing the war game scenario to test the concept. I would also like to thank all of my fellow classmates in the ASP for their feedback and discussion, which helped me understand the wide variety of challenges and opportunities facing future warfighters in the megacity environment.

Glossary of Acronyms

Key Actors for Proposed Concept

JIATF	Joint interagency task force
NSAG	Non-state armed group (e.g. drug cartel, terrorist groups, insurgencies)
VRN	Virtual resistance network
AO	Area of operations
CCINLAC	Civic Council of Nuevo León Institutions (in Monterrey, Mexico)
CIC	Center for Citizen Integration (in Monterrey, Mexico)
CIMIC	Civil-military cooperation
CNE	Computer network exploitation
CYBERCOM	U.S. Cyber Command
DTO	Drug trafficking organization
FHA/FDR	Foreign humanitarian assistance/foreign disaster response
GAFE	Mexican Airmobile Special Forces Group
HN	Host nation
IO	Information operations
ISP	Internet service provider
IT	Information technology
ITESM	Monterrey Institute of Technology and Higher Education
JIATF	Joint interagency task force
JIPOE	Joint intelligence preparation of the operating environment
KLE	Key leader engagement
MS-13	<i>Mara Salvatrucha-13</i>
NAFTA	North American Free Trade Agreement
NGO	Non-governmental organization
PAN	National Action Party (in Mexico)
PRI	Institutional Revolutionary Party (in Mexico)
SDR	<i>Situaciones de riesgo</i> /risk situations
SSG	U.S. Army Strategic Studies Group
USAID	U.S. Agency for International Development
VPR	Virtual private network

The Electronic Counterinsurgency: Enabling Virtual Resistance Networks in the Megacity

The Promise of Social Media and Crowdsourcing for Intelligence and Information Operations

The development of megacities¹ and the rapidly evolving information and communications technology environment will likely overwhelm traditional approaches to intelligence and information operations (IO). Megacities are the focal point for a vast array of electronic and physical networks, with highly globalized social and economic connections. Rapid demographic change can stymie any military force's attempt to gain an understanding the battlespace. Information and communications innovations such as "big data" analytical techniques and social media offer new opportunities to understand human terrain. Intelligence analysts can exploit methods like sentiment analysis and social network mapping, while these same technologies create new ways for IO planners to push narratives to target audiences on a massive scale.² "Crowd-sourced" intelligence has proven useful for military operations without a human adversary, like foreign humanitarian assistance/foreign disaster response (FHA/FDR).³ Pushing further, both academic theorists and U.S. security professionals have seen rowing global

¹ Megacities are commonly defined as an urban area of greater than 10 million people. See Marc Harris et al., *Megacities and the United States Army: Preparing for a Complex and Uncertain Future*, (Washington, DC: Chief of Staff of the Army, Strategic Studies Group, June 2014). This study will define megacities more broadly based on their heavy concentration of economic, social, and political links to globalized networks.

² For a discussion of the benefits and limitations of these approaches in the intelligence realm, see Kalev H. Leetaru and Charles R. Ehlschlaeger, "Modeling the Discourse of Megacities: Assessing Remote Populations in Non-Western Worlds," in *Understanding the Reconnaissance, Surveillance, and Intelligence Paradigm*, ed. Charles R. Ehlschlaeger. Topical Strategic Multi-Layer Assessment (SMA) and U.S. Army Engineer Research Development Center (ERDC), April 2014.

³ Crowd-sourcing techniques have been used to provide mapping and resource management services for humanitarian disasters in Japan, the Philippines, and the United States. Steve Lohr, "Online Mapping Shows Potential to Transform Relief Efforts," *New York Times*, March 28, 2011, http://www.nytimes.com/2011/03/28/business/28map.html?_r=0; Declan Butler, "Crowdsourcing goes mainstream in typhoon response," *Nature*, November 20, 2013, <http://www.nature.com/news/crowdsourcing-goes-mainstream-in-typhoon-response-1.14186>; Homeland Security Studies and Analysis Institute (HSSAI), *The Resilient Social Network: @OccupySandy #SuperstormSandy*, (Falls Church, VA: HSSAI, 30 September 2013).

connectivity as a means to challenge existing power structures and adversaries alike.⁴ Both proponents of anti-elite “counter-power” and U.S. power can be right. The expansion of open-source electronic social networks will blur the line between intelligence collection, information operations, and civilian security. But “techno-optimism” may be premature, as non-state armed groups (NSAGs)—drug cartels, terrorist groups, and ethnic militias—are likely to attack and subvert electronic networks that challenge their influence over the operational environment.

The operating concept proposed in this paper recommends a partnership between a U.S. or Coalition joint interagency task force (JIATF) and virtual resistance networks (VRN). A VRN is an online social network that is willing to report on NSAG activity. This proposed operating concept will describe how a U.S. JIATF can identify, enable, and protect electronic social networks in a megacity environment to provide both intelligence and information operations (IO) advantage. A JIATF can take advantage of the megacity’s connectivity, global links, and density to support layered defenses for VRNs in the face of NSAG coercion. So secured, the VRN can become a mechanism for electronic counterinsurgency, particularly in environments where local host-nation (HN) governance is too weak or corrupt to be that focus for resistance.

A VRN with thousands of participants willing to provide information online can produce massive amounts of sociocultural data, security atmospherics, and other intelligence for the JIATF commander. These participants can come from the local urban area or involve global allies, such as diaspora members, activists, and connected commercial actors. The development

⁴ Manuel Castells, “Communication, Power, and Counter-Power in Network Society,” *International Journal of Communication* 1, 2007, pp. 238-66; Kalev H. Leetaru and Charles R. Ehlschlaeger, “Modeling the Discourse of Megacities: Assessing Remote Populations in the Non-Western World,” in *Understanding Megacities with the Reconnaissance, Sureveillance, and Intelligence Paradigm*, Charles R. Ehlschlaeger, ed., (Topical Strategic Multi-Layer Assessment (SMA) and U.S. Army Engineer Research Development Center (ERDC)), April 2014; John P. Sullivan, “Policing Networked Diasporas,” *Small Wars Journal*, July 9, 2007, <http://smallwarsjournal.com/blog/policing-networked-diasporas>.

of a VRN can also serve as an IO objective in and of itself, as the mere existence of an open-source online network can help overcome the collective action problem inherent in resisting NSAG coercion. While the threat of reprisal can deter local civilians from publicly speaking out against NSAG influence, a public VRN can indicate to the average civilian that he will be one of many, not few, to resist, making crossing the threshold from inaction to action easier.⁵ If the U.S. military seeks to use this open-source data to weaken transnational criminal organizations, terrorist groups, and ethnic insurgencies in megacities, it must devise counterintelligence, force protection, and economic development strategies that protect local nationals providing this information.

Effective collective action by the megacity public is only likely if there is sufficient security. But the solution to physical threats to virtual networks will not likely be found by exerting more direct control—increased classification of intelligence sources and centralization of IO messaging—but by accepting the information decentralization of the evolving urban environment. The JIATF helps achieve VRN security and resiliency by leveraging the megacity’s density and connectedness to disperse sources and create electronic safe havens abroad. Indirect influence over massive, private social networks creates security and IO risks, but open-source electronic media provides speed and volume advantages to the military planner not available through military and government resources alone. Moreover, an operating concept rooted in the openness and transparency of private open-source networks is likely more in line with the American way of war. The U.S. constitutional focus on a free press and strategic focus on bolstering partner countries suggests that more transparent IO strategies hold advantages for

⁵ For a discussion of how individual thresholds for action drive collective behavior, see Mark Granovetter, “Threshold Models of Collective Behavior,” *American Journal of Sociology*, 83:6, May 1978, 1420-1443.

American military decision makers over more deceptive and centralized strategies like the Russian “reflexive control” concept.⁶

A JIATF will need to develop ways to jumpstart local confidence in collective resistance in environments where NSAGs are initially able to use violence and subversion to prevent the spontaneous emergence of effective VRNs. Also HN security forces likely will have too little capacity or will be too corrupt to protect their own citizens’ resistance efforts. To use terminology developed by sociologist Manuel Castells to describe online resistance efforts, the JIATF will play a supporting role in shepherding an online “network of outrage,” reporting on NSAG violence, into a “network of hope,” pressuring the host nation government to improve its security sector performance.⁷ If the JIATF succeeds in defending actors in the online network from NSAG violence or threats, a virtuous cycle can result as increased security encourages more civilian VRN participation, which expands the JIATF intelligence picture. In the long-run the VRNs become agents for internal change, as seen in the Mexico case study provided below. The social network is flexible enough to shift from providing immediate anti-NSAG intelligence to pressuring the host nation government to improve its governance performance.

This paper is divided into three sections. The first is a review of the problems and opportunities posed by the megacity, its growing electronic and global links, and how NSAGs can undermine the megacity’s vitality. It concludes with a discussion of the collective action problem posed to private actors seeking to resist NSAG influence, as it is the primary problem that the second section seeks to address. That section lays out a proposed operating concept, military support to enable and protect the virtual resistance network (VRN), which is the

⁶ Timothy Thomas, “Russian’s Reflexive Control Theory and the Military,” *Journal of Slavic Military Studies*, 17:2, 2004, 237-256.

⁷ Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age*, (Cambridge: Polity Press, 2012), 14.

electronic social network maintained by civilians in the megacity and abroad that will provide information to counter NSAG influence. The concept focuses on how the U.S. military can protect the VRN from NSAG reprisal and shepherd it to the point where it can act as an effective agent for change within the host nation government, with details on related tasks by warfighting function. The appendix is a case study on public reactions to drug cartel influence in northern Mexico since 2006. The study addresses how the public organized online to resist cartel violence, the cartel counter-response, and emerging Mexican solutions that relied on the three elements of the megacity defined in this paper: electronic connectivity, globalized linkages, and density.

Problem: Globalized Megacities and Physical Violence versus Virtual Networks

There are currently 20 megacities worldwide with greater than 10 million people, with that number likely approaching 40 by 2025, according to a recent U.S. Army Strategic Studies Group (SSG) paper.⁸ David Killcullen writes that four trends—rapid population growth, increasing urbanization, increasing littoralization, and increasing global connectedness—will drive future conflict trends away from rural insurgencies like in Afghanistan towards operations in rapidly growing megacities in the developing world like Mumbai, India, and Mogadishu, Somalia.⁹ Traditional U.S. military doctrine has recommended isolating urban areas in order to retain initiative and ability to maneuver, but the SSG paper suggests that it will be impossible to

⁸ Harris, 3.

⁹ David Killcullen, *Out of the Mountains: The Coming of Age of the Urban Guerrilla*, (Oxford: Oxford University Press, 2013), 25, 66.

physically or virtually isolate a megacity, due to its massive size and connectedness to the outside world through the Internet and other communications technologies.¹⁰

Isolation is likely impossible because of three qualities of the future urban environment this paper will address: increased electronic connectivity, globalized social and economic links, and high population and commercial density. Internet and cellular phone usage is highest in developed countries, but developing countries are seeing rapid adoption of these technologies. A Pew Research Center 2014 study shows that the 18-29 year-old generation is rapidly adopting Internet, social networking, and smartphone technology far ahead of their older counterparts.¹¹ Both Castells and James Jay Carafano write about how the urban environment served as an incubator for the combination of youth social movements, modern information technologies, and global online activism that fed the 2011 Arab Spring and 2009 “Green Revolution” in Iran, respectively.¹² Globalized connections are critical to the megacity in particular, according to John P. Sullivan, who sees these major urban centers as not just national economic, social, and political centers, but hubs for entire regions, binding elites in particular to the global community.¹³ Existing urban operations doctrine stresses the high density of people and infrastructure as a key aspect of the urban terrain.¹⁴ But these megacities are therefore not just full of people, but also have a high density of commercial and social links. These regional hubs,

¹⁰ Harris, 8.

¹¹ Pew Research Center, “Emerging Nations Embrace Internet, Mobile Technology,” February 2014, 12-13, <http://www.pewglobal.org/files/2014/02/Pew-Research-Center-Global-Attitudes-Project-Technology-Report-FINAL-February-13-20147.pdf>.

¹² Manuel Castells, *Networks of Outrage and Hope*, 53-66, 94-105; James Jay Carafano, *Wiki at War: Conflict in a Socially Networked World* (College Station, TX: Texas A&M University Press, 2012), 57-62.

¹³ John P. Sullivan and Adam Elkus, “Command of the Commons: Towards a Theory of Urban Strategy,” *Small Wars Journal*, September 26, 2011, <http://smallwarsjournal.com/printpdf/11533>.

¹⁴ Joint Staff, *Joint Urban Operations*, JP 3-06 (Washington, DC: Joint Staff, November 20, 2013), I-2-3.

with their high density of such networked links no matter their actual population, likely experience megacity-like challenges, no matter their exact population..

Those challenges are many. Primarily, the opacity and complexity of social connections in urban areas inhibit understanding by government forces. Previous writing on urban security operations emphasizes the importance of acquiring intelligence from local urban populations to understand NSAG activity. Transnational criminals and insurgents can take advantage of complex urban demography to nest among the most dispossessed groups in a city.¹⁵ Host governments often alienate their own urban populations, and law enforcement is unable or unwilling to acquire information from local sources, as seen in C. Christine Fair's study of urban conflicts in South Asia¹⁶ or Mike Davis' investigation of security dynamics in Los Angeles.¹⁷ Studies of more successful urban counterinsurgencies emphasized the ability of local security forces to improve intelligence gathering among the local population, shown in the Marine Corps Intelligence Activity assessment of British efforts in Belfast.¹⁸ U.S. military doctrine stresses the critical role local human intelligence plays in counterinsurgency and urban operations.¹⁹

¹⁵ See Kilcullen's description of the 2008 Mumbai, India, attackers' ability to exploit ungoverned spaces within the city, Kilcullen, 55; see also Matthew C. Ingram's study of violence in Mexican cities, where poor economic performance in outlying, marginalized neighborhoods was associated with an increased in homicides in commercial center, Matthew C. Ingram, "Community Resilience to Violence: Local Schools, Regional Economies, and Homicide in Mexico's Municipalities," in *Building Resilient Communities in Mexico: Civic Responses to Crime and Violence*, David A. Shirk, et al., eds. (Washington: Woodrow Wilson International Center for Scholars, March 2014), 25-27.

¹⁶ C. Christine Fair, *Urban Battlefields of South Asia: Lessons Learned from Sri Lanka, India, and Pakistan*, (Santa Monica, CA: RAND Corporation, 2004), 7-8.

¹⁷ Mike Davis, *City of Quartz: Excavating the Future in Los Angeles*, (New York: Vintage Books, 1990).

¹⁸ Marine Corps Intelligence Activity (MCIA), *Urban Warfare Study: City Case Studies Compilation*, (Quantico, VA: MCIA, 1995), 40.

¹⁹ Headquarters, Department of the Army, *Insurgencies and Counter Insurgencies*, FM 3-24/MCWP3/33.5, (Washington, DC: Department of the Army, May 2014), 8-4. Joint Staff, *Joint Urban Operations*, JP 3-06, (Washington, DC: Joint Staff, 20 November 2014), I-7.

The increasing complexity of threats in urban areas exacerbates the challenge of understanding the environment. Increasing globalized connectedness, both physical and electronic, foster what Kilcullen terms “dark networks,” groups that defy simple categorization. They engage in illicit and licit behavior and act as both political actors and criminal entrepreneurs.²⁰ Counter-terrorism, counter-narcotics, or counterinsurgency courses of action are insufficient on their own to weaken the armed groups. These hybrid groups also forge transnational ties, complicating responses from state actors. Drug trafficking organizations like the “Shower Posse” in Jamaica or D Company in the Indian subcontinent support political patronage networks and terrorist organizations, respectively.²¹ In recent years, this trend has also been observed online. Criminal organizations have become involved interstate conflict, such as the suspected collusion between the Russian state and Russian organized crime in cyber-attacks against the Estonian and Georgian governments in 2007 and 2008.²² The difficulty in attributing cyber attacks and increased push by criminal and political organizations to leverage cyberspace has further blurred the lines between different kinds of threats.

The role diaspora populations play in supporting hybrid threats has also shifted, as declining transaction costs in the financial and telecommunications sectors has made it easier for non-state armed groups to leverage resources from broader global communities. During the Cold War, only politically well-organized nationalist insurgencies like the Liberation Tigers of Tamil

²⁰ Kilcullen, 34.

²¹ Mahatma E. Williams, “Can the Jamaican Security Forces Successfully Reduce the Violent Impact of Gangs,” M.A. Thesis (Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 2012), 80, file:///C:/Users/Jessica/Downloads/ADA570118.pdf; David E. Kaplan, Bay Fang, and Soni Sangwan, “Paying for Terror,” *U.S. News and World Report*, 139: 21, Dec. 5, 2005, 40-41.

²² Andrew F. Krepinevich, *Cyber Warfare: A Nuclear Option?* (Washington, DC: Center for Strategic and Budgetary Assessments, 2012), 22-23.

Eelam in Sri Lanka could maintain transnational fundraising links to diaspora populations.²³ The ease of sending remittances has made those same resources available to smaller groups, as seen in the role of the Somali diaspora in London in funding organizations in the Horn of Africa.²⁴ Largely non-political groups have also benefited; for example, increased population flows between Central America and the United States have helped push once-localized gangs like *Mara Salvatrucha-13* (MS-13) beyond domestic criminal activity to a role in transnational narcotics smuggling.²⁵ So NSAGs are not only becoming more complex in their roles but are also expanding their ability to act outside the boundaries of traditional sovereign states.

But if economic globalization and the Internet have created new problems for state actors operating in dense and highly connected megacities, they also offer opportunities. Growing penetration of cellular phones, Internet, and social media use in developing world cities means there are new opportunities to gather information on dense, rapidly changing urban environments. Populations that previously existed in the city's shadows, living in slums, and participating primarily in gray or black markets, could now connect to the rest of the world through new modes of informational, social, and economic exchange. Castells expresses an optimistic viewpoint, claiming, "The emergence of mass self-communication offers an extraordinary medium for social movements and rebellious individuals to build their autonomy and confront the institutions of society in their own terms and around their own projects."²⁶ Castells later wrote about his theory of information "counter-power" in reference to physical and

²³ John La, "Forced Remittances in Canada's Tamil Enclaves," *Peace Review* 18, No. 3, 379-385.

²⁴ Laura Hammond, et al., *Cash and Compassion: The Role of the Somali Diaspora in Relief, Development, and Peace-Building*, Volume 1, Draft Paper for the United Nations Development Programme Somalia, 2011, 44.

²⁵ Douglas Farah, *Organized Crime in El Salvador: The Homegrown and Transnational Dimensions* (Washington, DC: Woodrow Wilson International Center for Scholars, February 2011), 11-18.

²⁶ Castells, "Network Society," 249.

virtual uprisings against oppressive state government during the Arab Spring, but his concept remains valid for resistance to non-state armed groups as well.²⁷

New technologies have created new ways for disadvantaged populations to participate in urban governance. “Crowdsourcing” is a common technique promoted to improve situational awareness. One such example is the Map Kibera project, which uses “volunteered geographic information” from the local population to map previously uncharted sections of Nairobi, Kenya.²⁸ According to the Homeland Security Studies and Analysis Institute’s study of the Occupy Sandy movement in New York, crowdsourcing via social media can support more effective distribution of humanitarian aid in the wake of a natural disaster.²⁹ Peter Van der Windt’s study of using cellular phone users to provide conflict data from the eastern Democratic Republic of Congo in real-time shows the potential usefulness of this approach even in war zones.³⁰ This open-source data, culled from social media, text messaging, and other sources of ground-level collection,³¹ may provide the basis for what some military thinkers have called a “social radar” for understanding the local population.³² Unlike more rural-centric counterinsurgencies in Afghanistan and Iraq’s Anbar Triangle, the emerging urban environment offers advantages to military planners looking to exploit private networks.

²⁷ Castells, *Networks of Outrage and Hope*, 42.

²⁸ Jiri Panek, “The Commercialisation of Public Data – How Does Participatory Data-Mining Look on a Global Scale?” *South African Journal of Geomatics* 2, No. 3, June 2013, 234; Douglas Batson, “Black Spots Are No Treasure Island: Land Tenure and Property Rights in Megacities,” in Ehlschlaeger, ed., 41.

²⁹ Homeland Security Studies and Analysis Institute (HSSAI), *The Resilient Social Network: @OccupySandy #SuperstormSandy*, (Falls Church, VA: HSSAI, 30 September 2013).

³⁰ Peter Van der Windt and Macartan Humphreys, “Crowdseeding in Eastern Congo: Using Cell Phones to Collect Conflict Events Data in Real Time,” *The Journal of Conflict Resolution*, Nov. 4, 2014.

³¹ For example, a JIATF elements could conduct a survey of the human terrain via an on-the-ground transect of the relevant area. Discussed in Jared Samuelson, “Canvassing for Combat: The Human Terrain Map Operational Concept,” unpublished draft, Marine Corps Command and Staff College MMS paper, February 4, 2015.

³² Michael T. Flynn, James Sisco, and David C. Ellis, “‘Left of Bang’: The Value of Sociocultural Analysis in Today’s Environment,” *Prism: A Journal of the Center for Complex Operations*, 3:4, September 2012.

Doctrinal writing on counter-insurgency and intelligence collection focuses on how military personnel can acquire useful intelligence from the population, a one-way interaction.³³ The above examples suggest that, for future conflicts in the megacity, new models of military-local interaction may be necessary. Local populations may aggregate and analyze information themselves in the open-source realm, or, as John P. Sullivan claims, “co-production” between government and civilian becomes possible. This would integrate the local population in the intelligence production cycle alongside the interagency and Coalition partners.³⁴ As a result, information technology infrastructure becomes vital terrain for megacity operations, with local information technology (IT) workers a key constituency. These local actors can promote stability, creating social media platforms to report drug cartel violence in Monterrey. Or they can increase instability, as some IT workers in Bangalore, India, did by providing logistic support to Islamist terror groups.³⁵

Other authors are less optimistic about maintaining information advantage over destabilizing actors during this time of rapid technological innovation. John Mackinlay writes that mass communications and “information anarchy” favors insurgencies over governments, claiming that state actors will have difficulty exploiting the user-generated content of the Web 2.0 era.³⁶ While crowd-sourced intelligence has proven useful for missions without a clear adversary, such as FHA/FDR, NSAGs are likely to attack and subvert electronic networks that challenge their influence over the operational environment. Criminals, terrorists, and insurgents

³³ See FM 3-24, section 3-4, where “All Soldiers and Marines collect information whenever they interact with the populace,” indicating the importance of direct collection by military units in a counterinsurgency construct.

³⁴ John P. Sullivan, “Policing Networked Diasporas,” *Small Wars Journal*, 9 July 2007.

³⁵ Lucy Conger, “The Private Sector and Public Security: The Cases of Ciudad Juárez and Monterrey,” in *Building Resilient Communities in Mexico*, 197-198; Shiva Kumar, “Bangalore hub of techie-terror network,” *The Times of India*, February 28, 2008, <http://timesofindia.indiatimes.com/india/Bangalore-hub-of-techie-terror-network/articleshow/2820775.cms>.

³⁶ John Mackinlay, *The Insurgent Archipelago* (New York: Columbia University Press, 2009), 94-95.

have always targeted local nationals who report on their activities to state or foreign authorities. They will likely continue to do so against perceived Internet or social media informants. Sullivan has written about these dynamics in reference to Mexican drug cartels, who have killed locals who reported on cartel violence via Twitter or weblog. This violence extends already existing “zones of silence” to the electronic realm, where most actors are intimidated from revealing information on cartel operations.³⁷ Islamic State forces reportedly took the drastic step of shutting down all cell towers in 2014, with the likely goal of limiting information coming out of the city ahead of a suspected Iraqi counter-offensive.³⁸ Carafano writes that only a few actors in any online information network are responsible for the vast majority of activity linking different groups, meaning armed actors can potentially disrupt the whole network by targeting only a few crucial “broadcasters”, making social media-generated mass data attractive but fragile.³⁹

Local populations seeking to resist violence or subversion by NSAGs through online social media networks face a collective action problem. A large network could provide sufficient quantities of intelligence that would allow government forces to take action against the armed group. The large network itself could also serve an IO purpose by its mere existence in the open-source realm, rallying others to see resistance as possible. Mancur Olson’s work on collective action provides useful caution against optimism, as his work demonstrates that even group with similar interests will not cooperate unless sufficient coercion or incentives to act

³⁷ John P. Sullivan, “Attacks on Journalists and ‘New Media’ in Mexico’s Drug War: A Power and Counter Power Assessment,” *Small Wars Journal*, 9 April 2011, <http://smallwarsjournal.com/blog/journal/docs-temp/730-sullivan1.pdf>.

³⁸ “Communications Shut Down: Why Extremists in Mosul Have Blocked All Telecommunications,” *niqash.org*, Dec. 4, 2014, <http://www.niqash.org/articles/?id=3589>.

³⁹ Carafano, 8-9.

exist.⁴⁰ Mark Granovetter's concept of collective behavior thresholds is helpful in addressing the NSAG subversion problem, as it describes how individuals' willingness to participate in group activity is dependent on the number of others already known to be in the group. Carafano's "broadcasters" are crucial, as those who join the social network earliest and are most active, even in the face of resistance, are the ones who push larger swathes of the population across the threshold into action.⁴¹ Without those crucial, early nodes in the network, social media is unlikely to live up to its promise by providing sufficient information for the operational-level commander.

Instead of collective action, local civilians are likely to act rationally and rely on "self-help" strategies that increase their personal security without providing broader resistance to the NSAG.⁴² But without some actor or method to coordinate these actions, thousands of individual rational decisions to avoid attracting any reaction from a violent cartel or militant group—gated neighborhoods, shuttered newspapers, and mass migration to safer areas inside or outside the host nation—destroy the city's resiliency. This can result in what Stephen Graham called "urbicide" when describing wartime Baghdad, where walls, security guards, and other security measures break down the vital economic and social activity that give the megacity life.⁴³ This lesson is particularly relevant for megacities of the future, which will likely serve at the center of regional and even global economies. In this environment, Graham's admonition that turning off

⁴⁰ Mancur Olson, *The Logic of Collection Action: Public Goods and the Theory of Organizations* (Cambridge, MA: Harvard University Press, 1971), 2.

⁴¹ Mark Granovetter, "Threshold Models of Collective Behavior," *American Journal of Sociology*, 83:6, May 1978, 1420-1422.

⁴² John Bailey, *The Politics of Crime in Mexico: Democratic Governance in a Security Trap* (Boulder, CO: Lynne Rienner, 2014), 75.

⁴³ Stephen Graham, *Cities Under Siege: The New Military Urbanism*, London: Verso, 2010, 241.

informational, economic, and other flows is a form of “suicide” (or “homicide” by NSAGs) should guide any military response.⁴⁴

Emerging information technologies offer a great deal of promise in providing the U.S. military and its partners access to large amounts of data on megacity environment. There is the added bonus that an engaged local population and its connected allies (e.g. diasporas, non-governmental organizations) can produce this data in the open-source realm. Host nation governments, because of a lack of capability or poor relations with populations where non-state threats thrive, have often been unable to gain sufficient intelligence from local civilians to improve security. Social media analysis, locally crowdsourced information, and globalized business groups all offer potential opportunities for improving intelligence collection in the megacity. But non-state armed groups can spoil these opportunities by dissuading local civilians from participating in globalized information flows through physical threats of violence. The next section of the paper will introduce the concept of military support to civilian-developed virtual resistance networks (VRN), whereby a U.S. combined joint interagency task force (JIATF) operates to enable and protect electronic resistance networks for intelligence and IO advantage, mitigating the collective action problem posed by NSAG violence.

Military/Interagency Operating Concept: Enabling and Protecting Virtual Resistance Networks in the Urban Environment

Concept Overview

The VRN enable and support mission consists of three primary groups of tasks. First, there is phase 0/1 shaping and intelligence preparation of the operating environment. The second

⁴⁴ Graham, 264.

group of tasks exploits the three qualities of the megacity identified in this paper--its electronic connectedness, globalized links, and demographic/economic density--to provide a layered, resilient defense of VRN participants from NSAG reprisal. The third group of tasks consists of a series of counter-intelligence and operational efforts to counter likely NSAG responses to the VRN's growing IO and intelligence successes.

In phase 0/1, the JIATF will identify existing forms on non-violent anti-NSAG resistance in both the physical and virtual realms. It can do so upon receiving orders to form or a geographic combatant command can investigate likely problem cities prior to the stand-up of a JIATF. The initial mission is intelligence-centric, determining what existing or potential networks could satisfy JIATF intelligence requirements in the open-source environment. To enable and protect developing VRNs, civilian and military JIATF elements will perform key-leader engagement (KLE) with key civil society organizations and reliable government, in order to identify key operations security and NSAG reprisal concerns for the local population. The goal is to provide an overall picture of how the JIATF could help protect VRN participants from NSAG coercion. This will allow the VRN to develop as a public repudiation of the NSAG's influence, a crucial IO objective.

Exploiting The Megacity's Connectivity, Globalization, and Density

To enable and protect VRNs as they develop, JIATFs can exploit the megacity's electronic connectivity, globalized links, and density. The end result is a growing *quid pro quo* relationship between the JIATF and the VRN: the VRN provides open-source intelligence and the JIATF provides protection. The megacity's ever-growing electronic connectivity is a key advantage in securing the VRN, even if public murders of bloggers and other social media activists may create the perception of reduced online safety. In reality, online networks can offer

a better level of protection and anonymity to a local VRN participant than the alternative, real-world activism. The JIATF and its partners could provide training programs, security tools, and other engagement opportunities to improve the local citizen's ability to participate in VRN information-sharing anonymously and safely. The JIATF can also intervene more directly in the megacity's online infrastructure, seeding the city with a more secure wi-fi network or partnering with a third-party corporation to develop a broadband network that improves upon existing networks' security standards.

The JIATF can also take advantage of the megacity's increasingly globalized links to provide further resiliency to the VRN's information gathering function. This may require thinking about the joint task force's area of operations (AO) in a unique fashion. The JIATF may be able to engage groups outside the megacity as a conduit for information coming from the threatened local population. The information leaves the megacity through traditional, dispersed mechanisms (e.g. telephone calls between relatives, international trucking and port traffic, university conferences, etc.). The information can then emerge through these transnational actors via the VRN's public face, more secure because because of the reporting actors' physical distance from the megacity. Because diaspora populations, multi-national corporations with heavy investments in the target urban area, and transnational activist NGOs may have close, continuing links with urban populations, the JIATF may need to include these transnational groups as part of their IO and engagement efforts. A JIATF operating in Mogadishu may seek to work with Somali diaspora groups in London and Minneapolis, or a task force in Mexico City may develop a relationship with Wal-Mart executives in Arkansas, as the company is the largest

private employer in Mexico.⁴⁵ To help provide the VRN's required resiliency, the JIATF and its U.S. government partners may need to include thumbnails of crucial human terrain within the task force's AO. These focus areas for JIATF liaison activity will be tied to the primary urban battlespace not by immediate geography but by a concentration of globalized network links between urban areas.

According to existing urban warfighting doctrine, population or building density is a problem as it canalizes maneuver and complicates fires.⁴⁶ But the megacity's density is instead a potential enabler under the VRN enable/protect mission, as it can help obscure the exact source of information provided by local civilians. As seen in the northern Mexico example provided below, NSAGs can succeed in eliminating local reporting on its activity by using the threat of violence and creating "zones of silence."⁴⁷ NSAG extortion and reprisal can encourage local self-help strategies which clear the city's commons (streets, commercial centers, media organizations) of activity, precipitating a drastic decline in outgoing information and potential "urbicide." To prevent "zones of silence," this concept focuses on jumpstarting greater amounts of commercial and social activity along city streets.

Jane Jacobs' *The Death and Life of Great American Cities* (1961) described how increased commercial flows contribute to urban security by increasing the eyes looking out for crime on any given street.⁴⁸ This concept expands on that idea to also suggest that expanding street activity helps deny NSAGs information on likely sources, as security incidents will have

⁴⁵ David Barstow, "Wal-Mart Hushed Up a Vast Mexican Bribery Case," *New York Times*, April 21, 2012, http://www.nytimes.com/2012/04/22/business/at-wal-mart-in-mexico-a-bribe-inquiry-silenced.html?_r=0.

⁴⁶ JP 3-06, I-3,5.

⁴⁷ John P. Sullivan, "Attacks on Journalists and 'New Media' in Mexico's Drug War: A Power and Counter Power Assessment," *Small Wars Journal*, 9 April 2011, <http://smallwarsjournal.com/blog/journal/docs-temp/730-sullivan1.pdf>.

⁴⁸ Jane Jacobs, *Death and Life of Great American Cities* (New York: The Modern Library, 1993, originally published 1961), 46.

no clear single reporter in high-traffic areas. The concept includes tasks to increase both physical and virtual flows. JIATF patrols can focus on key areas crucial to local commercial development, as increasing local economic activity is a common way to increase overall urban flows. JIATF patrol efforts can integrate with USAID and other interagency economic development programs for increased effect. Increasing Internet accessibility throughout the megacity, particularly in outlying neighborhoods commonly ignored in host-nation infrastructure plans, can create more opportunities for potential VRN participants. Secure businesses free from extortion will send more trucks along city streets and hire more workers who will travel between neighborhoods, increasing the number of local civilians able to report on security incidents or local atmospherics.

Countering NSAG Attacks on the VRN

If unimpeded, the above JIATF tasks should help provide sufficient security and confidence to VRN participants for the online network to grow. A self-sustaining, public intelligence cycle with IO effect should result. Open-source intelligence collection by the local population supports JIATF analysis. The intelligence cell's analysis drives security operations that increase local security perceptions and willingness to provide information. But NSAGs will likely seek to counter this system through subversion and violence, reducing civilian security perceptions and/or reducing the amount of credible information produced. NSAGs can target any point within this public intelligence cycle. NSAGs undermine physical collection by using public terrorism and business extortion to reduce commercial flows and drive potential civilian reporters from the streets. NSAGs can also undermine the electronic collection architecture by attacking or subverting the physical telecommunications network—cell towers, local Internet service providers (ISPs), and physical cables.

NSAGs can also target VRN participants directly. Even if civilians improve online security measures, NSAG cyberspace capabilities are improving.⁴⁹ The northern Mexico/Los Zetas case study below suggests that future NSAGs may exploit three broad capabilities to identify online VRN participants.⁵⁰ They can use traditional informant networks to identify online activists with insufficient offline operations security measures. NSAGs can develop organic computer network exploitation (CNE) capabilities to identify VRN participants, possibly by recruiting local IT professionals. Finally, they can bribe HN law enforcement and security personnel into providing them access into a country's telecommunication infrastructure. As a different approach from targeting the source, NSAGs can undermine the JIATF analytical effort indirectly through subversion of the VRN, having members participate in VRN activity to provide false data on opponents in other armed groups or within the government. This can reduce overall JIATF confidence in the VRN, sowing distrust in VRN data unless the JIATF intelligence cell makes a careful effort to validate key public sources of information.

According to James Jay Carafano, nations cannot rely on "crowd-sourcing" when national security is on the line⁵¹, so, unlike the open-source VRN itself, countering NSAG subversion of the public network will rely more on traditional intelligence and military capabilities. Smaller special operations teams could focus on direct action against NSAG reprisal teams. CIMIC and communications teams could "crowdseed" Internet connectivity by distributing large numbers of mobile wi-fi hotspots to local civilians across the megacity. The JIATF could also focus combat engineering capacity on repairing damage to the

⁴⁹ Krepinevich, 22-23; George W. Grayson, *Mexico: Narco-Violence and a Failed State?* (New Brunswick, NJ: Transaction Publishers, 2010), 188.

⁵⁰ Scott Stewart, "Anonymous vs. Zetas Amid Mexico's Cartel Violence," *Security Weekly*, Stratfor Global Intelligence, November 2, 2011, <https://www.stratfor.com/weekly/20111102-anonymous-vs-zetas-amid-mexico-cartel-violence>.

⁵¹ Carafano, 93.

telecommunications grid, countering any NSAG efforts to silence the battlespace and providing an IO boost in the eyes of a local population increasingly dependent on electronic connectivity.

Meanwhile, counterintelligence and CIMIC efforts should focus on countering NSAG influence within the “commanding heights” of the megacity’s electronic infrastructure. The city’s IT business sector and universities are likely sources of cyber-savvy manpower for the host-nation, the VRN, or the NSAG’s own cyber teams, so it should be treated as key human terrain. Those areas are therefore worth monitoring by intelligence assets and engaging through interagency economic development and Internet freedom programs.⁵² Limiting corruption within HN law enforcement is also crucial, as these officials may be able to provide NSAG actors access to ISP and mobile telephone data collected through a state’s legal regulatory and policing mechanisms. The U.S. military has experience operating anti-corruption task forces in Afghanistan⁵³, but a smaller JIATF in the megacity will likely only be able to maintain a small cell that focuses on HN security force corruption that provides NSAGs access to VRN-related online information.

The VRN would likely carry out broader anti-corruption messaging, with centralized guidance from the JIATF likely unnecessary and ineffective. The VRN could shift organically from its focus on NSAG activity (in line with short/medium-term JIATF goals) to demanding improved HN security force performance. As the VRN matures and its ability to monitor corruption improves, this may enable the JIATF to work with develop Department of Justice-

⁵² For example, see the State Department’s NetFreedom Task Force, established in 2006, designed interagency Internet freedom programs. Patricia Maloney Figliola, *Promoting Global Internet Freedom: Policy and Technology* (Washington, DC: Congressional Research Service, October 22, 2013), 2.

⁵³ Combined Joint Inter-Agency Task Force-Shafafiyat was established under the International Security Assistance Force in Kabul in 2010, with a broad mission to combat all forms of corruption related to the narcotics trade and the insurgency. John F. Sopko, “Letter from SIGAR to ISAF Commanding General Joseph H. Dunford, Jr.,” Office of the Special Inspector General for Afghan Reconstruction, July 31, 2013.

vett ed HN law enforcement units, creating intermediate structures that would survive the JIATF's departure.⁵⁴ This would support the likely long-term JIATF end-state of enabling HN security structures to manage the NSAG threat after the JIATF's withdrawal. As the northern Mexico example below shows, even developing country megacities will likely contain more educated populations that can pressure the HN to improve security force performance and reduce corrupt NSAG-police collusion. If the VRN is mature and its participants secure from NSAG threats, VRN participants will likely be confident enough to challenge the host nation government to improve its performance. The VRN becomes not just a mechanism for JIATF intelligence and IO goals, but it also becomes the change agent that provides grassroots pressure for longer-term improvements in civilian security.

Concept Scope, Limitations, and Risks

This concept best applies to urban stability operations and security assistance missions. The U.S. JIATF has the short-term objective of defeating and/or disrupting a NSAG in the battlespace, with the long-term objective of ensuring the host-nation (HN) government can secure its own territory. It assumes that the HN government will be at first unable or unwilling (because of corruption or other issues) to confront NSAG threats, pushing the local population to choose between online/offline resistance and self-help strategies. It also assumes interagency participation, because the State Department, U.S. Agency for International Development (USAID), and other civilian agencies will often be better interlocutors with VRN participants than the JIATF's civil-military cooperation (CIMIC) section. Because the concept focuses on the VRN as the key information provider and source of pressure on the HN government, not a JIATF

⁵⁴ See the Drug Enforcement Administration's (DEA) Sensitive Investigative Unit program, with DEA-vett ed counterdrug law enforcement units in ten countries. DEA, "International Training," <http://www.dea.gov/ops/Training/IntTraining.shtml>, accessed April 16, 2015.

of a particular size, this concept could apply to forces of any size. Its exploitation of local open-source networks suggests it is most suitable for smaller forces looking to limit strain on maneuver and kinetic fires units. Such forces could include smaller Marine Air-Ground Task Forces, embassy-run security assistance campaigns, or U.S.-supported stability/peacekeeping forces.⁵⁵

The concept's applicability may however be limited by the human terrain. The case study used for this concept involves public mobilization against drug cartels in northern Mexico. The situation there involved a relatively homogenous local population without a history of intercommunal violence and NSAGs with limited non-coerced public support, ensuring that developing VRNs will likely focus on targeted NSAGs. Part of the joint intelligence preparation of the operating environment (JIPOE) process in phase 0/1 of military operations requires identifying whether or not conditions both inside the battlespace and within the megacity's broader global area of operations (AO) are suitable for this approach. For example, fostering an electronic social network in Beirut among populations sympathetic to Lebanese Hizballah may be contrary to U.S. strategic objectives. Here is the risk of fighting an information-centric counterinsurgency with a civilian VRN.

Assessing whether a VRN would provide an IO advantage to U.S. forces is crucial, because the joint force commander or country team ambassador cannot control or direct an electronic social network. It may be possible to exploit this autonomous network for intelligence, coordinate with it through engagements with key public nodes, such as a city's IT sector,

⁵⁵ While this paper focuses on VRN support as a U.S. military operating concept, it could very well apply to United Nations and other regional organization peacekeeping forces. U.N. civilian agencies will often be perceived as more legitimate by and have stronger relationships with local civil society, fostering greater trust with VRN participants. The concept does not rely as heavily on more maneuver and kinetics fires functions, capabilities commonly lacking in multinational peacekeeping units.

business community, or diaspora organizations. U.S. forces may develop an indirect information-for-security *quid pro quo* relationship with these networks. But the fact that the joint force commander cannot control VRNs helps reinforce its power as information source and change agent. The local population will likely perceive the VRN as more rooted in the community, in line with existing counterinsurgency doctrine that stresses that the role of existing community members, not outsiders, as key mobilizers of broader social networks.⁵⁶ Creating resilient networks will likely be difficult, as a public JIATF commitment to protect open-source information providers will likely be met by a renewed NSAG efforts to subvert these networks. The offense has an asymmetric advantage here, as a few successful high-profile attacks on key VRN nodes (e.g. popular bloggers, civil society organizations) can have a chilling effect on future information sharing.⁵⁷

The openness of the approach is a risk, as the JIATF will not be as able to protect intelligence sources through traditional classification-based secrecy. It instead will need to develop a resilient layered defense that provide multiple options for the local population to share security-related information more safely. This would likely include programs focused fostering effective online anonymity, dispersing information sources through the development of “electronic safe havens” in third-party countries, and developing social media tools and methods that overwhelm NSAG counterintelligence efforts. Mechanisms that can obscure report originators through sheer mass and targeted close protection teams for key VRN participants and infrastructure, like elements of a megacity’s telecommunications sector, are also crucial. Encouraging and protecting sources of crowd-sourced intelligence online can address all

⁵⁶ Joint Staff, *Counterinsurgency*, JP 3-24, (Washington, DC: Joint Staff, November 22, 2013), II-7.

⁵⁷ Using Granovetter’s threshold model here, these actors are first movers who drive larger segments of the population to see the anti-NSAG network as a safer choice, so their death or withdrawal from the VRN could drive off even larger numbers of marginal contributors. Granovetter, 1422.

elements of this layered defense—anonymity, dispersal, and mass—and partially replace non-digital institutions, such as analog media like newspapers and radio stations with targetable physical addresses. The advantage of such an open network is that it hopefully will provide greater volumes of data than a traditional source network. It also can provide an IO effect as its very openness indicates to on-the-fence contributor that resistance is possible. There is one final concern with an open-source, uncontrolled information network has one final risk. The JIATF intelligence cell must think of source remuneration in terms of providing public goods for a public network. This concept accounts for that, as the JIATF will focus on public goods like security interventions to counter NSAG subversion and development programs to increase physical and virtual flows within the megacity and to the rest of the world. Different elements of the JIATF will have their own responsibilities for helping to provide these public goods, broken down by warfighting function below.

VRN Enabling/Protection by Warfighting Function

Command and Control (C2): The key C2 challenge for the joint force commander is that he can neither command nor control many of the concept's elements. He cannot give orders to the VRN. Attempts to overtly influence the online network would likely backfire by undermining the IO message that the local population is creating its own forms of resistance. Interagency partners will likely drive economic and electronic infrastructure development programs, and these efforts are crucial enough that civilian leadership at the embassy level will likely be co-equal with the military effort. The concept's globalized AO and cyberspace components will require effective coordination and/or ceding of control to national or COCOM-level diplomatic, military, and intelligence units. Effective coordination by civil-military engagement teams will

be a vital task, whether it is interaction with local civil society, global diaspora communities, or the city's IT community.

The task force will likely require several elements at the headquarters level that will focus broadly on analysis of the VRN analysis and anti-NSAG operations. The J2 intelligence and J2X counterintelligence cells described below will reside here, as will other rapid-reaction elements, such as the close protection teams for vital VRN participants or special operations counter-reprisal teams. Lead interagency elements, like USAID or Department of Justice, would also maintain overall control of their economic development, cyberspace, and anti-corruption programs at this level. Smaller infantry elements would likely focus on patrolling key neighborhoods, in line with the concept of encouraging increased commercial and street activity through improved security. These units would likely be supported by an intelligence detachment with a special focus on monitoring neighborhood-level social media activity and a communications detachment focused on increasing electronic connectivity for the civilian population. The maneuver unit would likely include its own CIMIC team, potentially focused on previously identified key terrain (e.g. universities, commercial centers). Lower-level units would be focused on creating the conditions for VRN success, allowing JIATF HQ to develop options to counter actual NSAG elements, which will likely be more difficult to target.

Intelligence: Intelligence is the crucial supporting element in this operating concept, as it relates to the VRN in two crucial ways. It helps protect the VRN and it exploits information produced by the VRN to provide assessments for the broader JIATF mission. Intelligence elements within the JIATF have three primary missions under this concept. First, there is the initial Phase 0/1 JIPOE effort, which should answer two questions. Is encouraging a VRN in line with U.S. strategic objectives? How can the JIATF encourage the development of an electronic

social network in a relatively information-poor battlespace? For the first question, if the NSAG has unified community support or if the VRN is likely to break apart around identifiable intercommunal or ethnosectarian lines, the VRN may not be effective as a form of resistance. To develop the VRN, the intelligence cell needs to identify potential nodes within the megacity that could or already are serving as focal points for information-centric resistance, such as clusters of heavy-traffic social media activity or active professional or commercial organizations. Using social network analysis, the intelligence cell also identifies potential sources of support outside of the megacity, such as diaspora communities, multi-national corporations, or other electronic networks that have shown interest in the megacity's plight. Finding as many potential links as possible is useful here, as David Ronfeldt claims that leaderless social conflict, or "netwar," is most effective with many diffuse networks operating as a "swarm" in multiple different geographic, social, and topical areas.⁵⁸ The goal in phase 0/1 is to establish a baseline understanding of who inside and outside the megacity will serve as the best focal points for growing VRNs.

During ongoing operations, the J2 cell is also tasked with monitoring the VRN's output to develop open-source intelligence analysis. Initially, the VRN may produce insufficient information to support stability or other operations. But as the VRN expands and its members feel more secure, they will provide more information on NSAG violence, coercion, and other atmospheric. This will create a "social radar" for the megacity.⁵⁹ Traditional intelligence collection could assist in this process, filling gaps in the open-source picture or verifying information provided by VRN members. Social network and "big data" analytical techniques

⁵⁸ David Ronfeldt, et al., *The Zapatista Social Netwar in Mexico* (Santa Monica, CA: RAND Arroyo Center, 1998), 119-121.

⁵⁹ See Michael T. Flynn, James Sisco, and David C. Ellis, "'Left of Bang': The Value of Sociocultural Analysis in Today's Environment," *Prism: A Journal of the Center for Complex Operations*, 3:4, September 2012.

will be crucial as the VRN expands, allowing a small JIATF intelligence cell to manage the input from thousands of VRN members. Geo-tagging of tweets and other forms of geospatial metadata will allow the JIATF intelligence cell to push relevant intelligence and analysis down to the appropriate ground maneuver unit. This should require less bandwidth than traditional intelligence operations, since classified systems and other operations security measures will be less necessary.

The J2X counterintelligence cell would maintain the bulk of the JIATF's traditional collection platforms. The cell would focus these assets on likely NSAG threats to VRN participants, targeting NSAG reprisal, human intelligence (HUMINT), and cyber units. J2X would also monitor the "commanding heights" of electronic operations in the urban battlespace. Those "commanding heights" include the city's telecommunications infrastructure, HN law enforcement, and the IT sector (both businesses and universities), areas where an NSAG could develop placement and access to undermine VRNs on a large-scale. Open-source analysts could support this effort by assessing which VRN members or nodes are most critical to the VRN's survival. J2X members would work closely with close protection and civil-military engagement teams to ensure that the NSAG cannot undermine the VRN by targeting its most effective elements.

Fires (Information Operations/Cyberspace): JIATF IO efforts will focus on magnifying the anti-NSAG impact of the VRN. There are several measures JIATF elements can take to effectively raise the "volume" of the VRN's messaging. Communications and engineering elements can increase the local population's ability to access online networks, especially since NSAGs may respond to VRN reporting by attacking or subverting existing ISP or cellular infrastructure. Military forces do not have to wait for the local population to connect to the

VRN, particularly if NSAGs or natural disasters reduce online connectivity. Instead, the JIATF can “crowdseed”⁶⁰ Internet connections by sowing wi-fi hubs or cheap Internet-accessible mobile phones throughout the megacity, ensuring a free Internet connection available to potential VRN participants reporting on security issues. A “multimodal” system with multiple available technologies offers flexibility to local populations if NSAGs threaten one communication platform or another.⁶¹

Engineering elements can also partner with technology corporations to provide a broadband backbone for the megacity, either directly building the a fiber optic network⁶² or indirectly by working with IT-savvy elements in the VRN to create a “crowdsourced” wi-fi network consisting of other VRN participants’ connections.⁶³ Increased bandwidth will allow VRN participants to not only post text on social media, but better enable use of cameraphone and video capabilities to improve the resonance of messages. Increased bandwidth will also increase the need for IO and intelligence cells to monitor the online “social radar” to develop counter-messages if and when NSAGs exploit improved connectivity for their IO efforts.

As a final element, interagency and private IT sectors partners can help the JIATF on the software side, helping to develop social media tools for use by VRN participants. While USAID or military oversight may be necessary to prevent NSAG co-option, partnerships with local

⁶⁰ Definition of “crowdseeding” from FrontlineSMS, “Voix des Kivus: Data Integrity Cast Study,” August 2011, <http://www.frontlinesms.com/wp-content/uploads/2011/08/Case-Study-Voix-des-Kivus-final.pdf>.

⁶¹ Castells, *Networks of Outrage and Hope*, 61-66. Castells discusses multiple techniques developed by Egyptian protesters and their global allies during the 2011 Arab Spring to get around the government’s attempts to restrict Internet access, such as Google and Twitter’s “speak-to-tweet” program that could convert voice mail messages into online tweets.

⁶² See for a discussion of fiber optic networks built by technology companies or local municipalities, Mike Rogoway, “Google Who? Oregon Cities Want Their Own Fiber Networks,” *The Oregonian/Oregon Live*, April 7, 2015, http://www.oregonlive.com/silicon-forest/index.ssf/2015/04/google_who_hillsboro_gresham_l.html.

⁶³ See Fon, a U.S. company that is developing a crowdsourced wi-fi network using portions of users’ private wi-fi connections. Ingrid Lunden, “Crowdsourced WiFi Network Fon Picks Up \$14M Led by Qualcomm, Adds Facebook Integration,” *TechCrunch*, Jan. 20, 2014, <http://techcrunch.com/2014/01/20/crowdsourced-wifi-network-fon-takes-another-picks-up-another-14m-led-by-qualcomm-adds-facebook-integration/>.

businesses to develop any social media platforms will be crucial. Local developers will be better able to develop strategies to increased local usage. In the northern Mexico example used below, local businesses helped develop Tehuan, a social media platform that focused on crowdsourced public safety and traffic reporting, not just cartel violence.⁶⁴ In comparison, a USAID-designed Twitter-like site in Cuba succeeded in gaining users but was controversial because of the its prominent U.S. government role.⁶⁵ For both software and hardware support, JIATF efforts should focus on bolstering VRN, civil society, and private sector responses.

Movement and Maneuver: JIATF unit patrols and other forms of maneuver should support the third leg of the VRN support concept, increasing the density of commercial and social contacts. Unit patrols should focus on neighborhoods, routes, and interactions with the populace that bolster local perceptions of security. Measurements of effectiveness should not focus on the number of patrols conducted or territory controlled, which is likely an inappropriate concept for the dense, complex megacity in any case. Instead, unit patrols will be effective if they increase the commercial and social flows along the city's streets, increasing opportunities for locals to report on conditions in the urban area. In line with broader counterinsurgency and community policing principles, patrols should be light, foot-mounted if possible, and avoid giving the impression of militarizing the city's public spaces, which can discourage social interactions.⁶⁶

⁶⁴ Centro de Integración Ciudadana, Tehuan, <http://www.cic.mx/tehuan-beta/>, accessed 22 January 2015.

⁶⁵ Ron Nixon, "Cuba Social Media Project Was No Plot, Agency Says," *New York Times*, April 8, 2014, http://www.nytimes.com/2014/04/09/world/americas/us-agency-defends-social-media-project-in-cuba.html?_r=0.

⁶⁶ JP 3-24, D-2; U.S. Department of Justice, "Foot Patrols: Crime Analysis and Community Engagement to Further the Engagement to Community Policing," *Community Policing Dispatch*, 2:2, November 2009, http://cops.usdoj.gov/html/dispatch/February_2009/foot_patrol.htm.

Protection: This paper focuses on the problem posed by physical violence against virtual networks, and JIATF protection operations will appropriately focus on efforts to safeguard the civilian population in both the physical and virtual realms. In the physical world, force protection efforts are centered less on security for military units, but on three categories of civilian activity. First, JIATF close protection teams will provide security for key VRN nodes or areas threatened by NSAG threats. Working with intelligence analysts, the goal should be to identify and development protection measures for central VRN participants even before the NSAG reprisal architecture itself has identified the target. Those close protection teams will also work to protect key interagency partners, such as the U.S. Agency for International Development (USAID), or partnered non-government organizations (NGOs) supporting cybersecurity and commercial development programs from NSAG reprisal.

The JIATF will support virtual protection by assisting programs to improve VRN participants' cybersecurity measures. It may be impossible to prevent a determined NSAG from identifying some VRN members, but cybersecurity experts inside and outside the U.S. government can provide training and tools to local VRN participants to increase their likelihood of remaining anonymous. Depending on the operational challenge and the HN government relationship, programs run by USAID, cyber protection teams provided by U.S. Cyber Command (CYBERCOM), or partnered NGOs may be most effective in improving civilian online security practices. The JIATF can also seek to leverage transnational partners, such as diaspora organizations or multi-national corporations. Civil affairs or State Department personnel can engage local civil society and other VRN participants through these transnational actors. Local actors are more likely to provide intelligence if it is passed through a trusted intermediary via more secure, but still private and open-source, means like virtual private networks (VPNs) and

corporate reporting mechanisms. Having multiple operations security programs both inside and outside the megacity helps provided the layered, resilient defense necessary to protect the VRN while still maintaining its open-source advantages.

Sustainment: There are limited sustainment issues particular to this concept. The ability of the JIATF to remain light under the VRN enabling/support concept is a benefit for logistics. Sustainment elements will likely need to account for interagency elements in the megacity, who may call on military elements for support. Communications logistics is a relevant concern as well, as the concept relies on personnel and equipment at the company level for the distributed wi-fi networks, computer dashboard programs for monitoring neighborhood social media traffic, and other electronic elements.

Maintaining electricity access is also important as all these electronic devices need to be powered. Besides traditional engineering support to the electrical grid, mobile charging stations and generators may be necessary stopgap measures in case of natural disaster. The joint force commander will need to balance those concerns with those of traditional and more pressing humanitarian assistance tasks like providing medical care and access to clean water. Sustainment efforts overall should nonetheless focus whenever possible on maintaining resilient mechanisms for VRN participants to connect online even in the face of NSAG attacks and natural disasters

Required Capabilities

Most of the capabilities required to enable and support VRNs already exist, either within the U.S. government or developed within the private IT sector. Electronic dashboards for monitoring social media activity, including geospatial information, are commonly used by private sector firms for customer service and brand management. These could be adapted for any JIATF headquarters or maneuver unit, as long as sufficient bandwidth and legal authorizations

for monitoring social media by intelligence and IO officers are available. The commercial sector drivers developments for bolstering online connectivity, including mobile wi-fi hubs, crowdsourced networks, new expeditionary power systems, and improved online security capabilities. Partnerships with Silicon Valley will likely suggest other mechanisms for improving U.S. government efforts to monitor and enable online social networks. The primary limitations on U.S. military adaptation of these technologies for operational purposes will likely be related to legal authorizations and organizational cultures that may regard the idea of security for a public, open-source network as an oxymoron.

Conclusion

Current military doctrine focuses on avoiding a fight in urban area, isolating them whenever possible. But megacities are too vital of terrain to cede to insurgents, drug cartels, and terrorists, as they serve as economic, social, and political hubs on a regional and global scale. While megacities create many problems, growing so quickly as to multiply security and governance issues for U.S. partner countries, those same countries require the economic vitality these urban areas produce. As a result, warfighting doctrines that disrupt or isolate those crucial flows threaten a country's overall health. Physical barriers, such as those built in Baghdad or Belfast, are isolating, as are barriers in the informational environment. NSAGs can threaten the megacity's electronic flows, threatening the local population, corrupting host-nation institutions, and preventing local reporting of security threats. Information flows like these are the urban area's nervous system, sending messages that drive change within private and public-sector institutions to counter threats to the megacity's well-being.

The VRN enable and protect concept allows U.S. military forces to help restart those flows where violent and subversive actors have been able to impose "zones of silence," leaving

host-nation government incapable or too compromised to respond. Civil society may exist but be incapable of coordinated resistance in the face of NSAG threats. But a U.S. military/interagency force can take advantage of emerging trends in the megacity to boost the local population's own ability to report and resist. Increasing electronic connectivity globally provides new options to develop forms of online "counter-power"⁶⁷ to NSAG influence, in the form of the VRN.

Globalization creates new communities of interest outside the megacity that can support the VRN's development. The megacity's own vitality, in the form of dense commercial and social networks, can become a mechanism to jumpstart reporting. The VRN and JIATF form a virtuous circle, a public intelligence cycle whereby increased reporting by VRN members on security threats improves the JIATF's ability to protect the VRN. Traditional military capabilities, such as counterintelligence and special operations direct action, buttress the VRN in areas where the public does not have the will or capacity to act.

But the end-state goal of the VRN enable/protect operating concept is to make U.S. military intervention unnecessary. The JIATF enables the VRN to grow in its early stages, helping it over the threshold of the collective action problem. Over time, it should acquire its own momentum, building its own links to global community and developing its own tools for online security. In the long run, the VRN supports real-world civil society mechanisms, such as NGOs and media organizations, previously weakened by NSAG coercion. Ultimately, the VRN is likely to challenge the host nation's own poor security and governance performance, whether a result of corruption or limited capacity. VRNs based in the megacity, a likely stronghold of political and economic strength, are well-placed to pressure the host-nation government to improve its performance and provide security. VRNs protected and shepherded by the JIATF are

⁶⁷ Castells. *Networks of Outrage and Hope*, 5.

thus able to re-establish the feedback loop between the government and the governed. This will enable U.S. military forces to hand responsibility to HN forces, now with greater incentives to counter the non-state threat in the target megacity.

Appendix

Case Study: Cartel versus Citizen: Information Operations, Open-Source Intelligence, and Public Resistance in Northern Mexico

This paper focuses on the interplay between information operations, open-source intelligence, and models of peaceful local resistance to non-state armed groups. The case study chosen to illustrate these links is the ongoing conflict between and among the Mexican government and drug cartels, with a focus on northeastern Mexico, primarily Monterrey, but also Ciudad Juárez, Nuevo Laredo, and other smaller cities. The paper focuses on the period of the 2006-2012 administration of former President Felipe Calderón. It was during this period that drug-related violence skyrocketed in northern Mexico and that, in many cases, Mexican government local and state law enforcement lost much or all of their ability to provide adequate security for the civilian population. The case study focuses on how the population resisted or avoided cartel influence, portraying civilian responses to cartel violence as a collective action problem. Some actors took self-help actions to reduce risk and others attempted to organize broader resistance to cartel influence. The role of information plays a crucial role in the analysis, as the primary cartel investigated, Los Zetas, attempted to eliminate public information on its activities. Meanwhile, traditional civil society, local media, and new forms of social media all sought means to disseminate information. The need to provide security for virtual, crowd-sourced information networks from physical threats results in a problem that blurs the line between open-source intelligence collection, information operations, and civilian security.

Background

By the 1980s and 1990s, organized crime and corruption had long been features of the Mexican political system under the 40-year monopoly of the Institutional Revolutionary Party (PRI). Major drug traffickers received protection in exchange for bribes and PRI officials resolved conflicts between cartels. This traditional patronage system managed to limit violence by keeping trafficking competitors in equilibrium.⁶⁸ Violence rose as this system broke down; between 2007 and 2011 under the administration of National Action Party (PAN) President Felipe Calderón, homicides in Mexico more than doubled to approximately 22,000 per year.⁶⁹ Democratization and economic globalization, particularly increased commercial flows due to the 1994 North American Free Trade Agreement (NAFTA), helped break up the old corrupt patronage system. Multiple Mexico analysts assessed that this system had helped to maintain peace among different drug trafficking organizations (DTOs).⁷⁰ At the same time, regional changes in drug markets created new opportunities for Mexican traffickers, namely a decline in cocaine flows from Colombia through the Caribbean Sea due to U.S. interdiction pressure and the rising U.S. demand for drugs like methamphetamine.⁷¹

These transitions took place within a Mexican political system that was still institutionally weak, suffered from widespread corruption, and had difficult responding to

⁶⁸ Paul Rexton Kan, *Cartels at War: Mexico's Drug-Fueled Violence and the Threat to U.S. National Security*, (Washington: Potomac Books, 2012), 4; Eric L. Olson, David A. Shirk, and Duncan Wood, "Introduction: Building Resilient Communities in Mexico," in *Building Resilient Communities in Mexico: Civic Responses to Crime and Violence*, Shirk, Wood, and Olson, eds., (Washington: Woodrow Wilson International Center for Scholars, March 2014), 6.

⁶⁹ Olson, Shirk, and Wood, "Building Resilient Communities in Mexico," 4.

⁷⁰ Kan, *Cartels at War*, 4; George W. Grayson, *Mexico: Narco-Violence and a Failed State?*, (New Brunswick, NJ: Transaction Publishers, 2010), 55-56; David A. Shirk, Duncan Wood, and Andrew Selee, "Conclusion: Toward a More Comprehensive and Community-based Approach to Public Security," in *Building Resilient Communities in Mexico*, 266.

⁷¹ Kan, *Cartels at War*, 3-4.

people's security needs. The new political reality broke up the corrosive, but somewhat stable, PRI-cartel patronage system and new PAN governments aggressively targeted major traffickers. Starting as early as 1989 but accelerating during the 2000s, the Mexican government, with U.S. assistance, arrested the heads of multiple large cartels.⁷² The elimination of key cartel leadership and Calderón's 2006 declaration of war on the DTOs, combined with growing drug profits, created what Paul Rexton Kan calls a "hypercompetitive illegal market,"⁷³ as new, more violent, cartels emerged to seize control of trafficking corridors and fight with old cartels over power in key border crossing points, called "plazas."⁷⁴

Northern Mexico saw both the promise and peril of these transitions. NAFTA and economic globalization allowed the region to develop into both a large-scale producer of goods for the U.S. market and as a major transit corridor for cross-border economic flows.⁷⁵ Northern Mexico, with the key plazas controlling drug flows into the United States, also saw some of the most violent intra-cartel violence. Conflict between the Juárez Cartel/Beltrán Leyva Organization, the much larger Sinaloa Cartel, and their respective enforcer gangs over control of the crucial border city of Ciudad Juárez led to skyrocketing violence, homicides increasing from 136 to 2,738 between 2007 and 2010.⁷⁶ In Nuevo León and Tamaulipas States, including northern Mexico's industrial center of Monterrey, the 2007 arrest and extradition of Gulf Cartel chief Osiel Cárdenas Guillén resulted in a growing split between Gulf leadership and its enforcement arm, the former Mexican special forces-lead Los Zetas. This led to a full

⁷² John Bailey, *The Politics of Crime in Mexico: Democratic Governance in a Security Trap*, (Boulder, CO: Lynne Rienner, 2014), 117-119.

⁷³ Kan, *Cartels at War*, 13.

⁷⁴ Kan, *Cartels at War*, 6, 55-57; Shirk, Wood, and Selee, "Toward a More Comprehensive and Community-based Approach to Public Security," 260.

⁷⁵ Steven Dudley and Sondra Rodríguez Nieto, "Civil Society, the Government, and the Development of Citizen Security," in *Building Resilient Communities in Mexico*, 66, 77

⁷⁶ Dudley, 66-67; Grayson, 83.

separation between the two in 2010 and outright war over control of key northeastern Mexico plazas.⁷⁷

Cartel Intimidation and Traditional and Electronic Forms of Public Resistance

As violence escalated throughout Mexico following Calderón's election in 2006, state and municipal-level law enforcement disappeared in many cities as an effective counter to cartel intimidation. According to a 2010 government survey, less than 25 percent of the Mexican population had confidence in all levels of law enforcement. Cartels gave police officers and other officials a choice between accepting a bribe or death, colloquially called *¿Plata o plomo?* ("Silver or lead?"), undermining law enforcement action.⁷⁸ Calderón deployed tens of thousands of soldiers and marines, who had higher levels of public confidence, but these forces at first lacked experience in community policing techniques to reassure the local population.⁷⁹ Even if murders were largely cartel-on-cartel, DTOs sought new avenues for illicit profits. Rising kidnapping and extortion of businessmen and professionals exacerbated local senses of insecurity. Journalists and media organizations, traditional gatekeepers for public information, were also commonly targeted. Some received bribes to report negatively on rival cartels, and one U.S. NGO claimed more than 80 journalists were killed in Mexico, often for covering cartel activity, between 2000 and 2012.⁸⁰

⁷⁷ Lisa J. Campbell, "Los Zetas: Operational Assessments," in *Narcos Over the Border: Gangs, Cartels, and Mercenaries*, Robert J. Bunker, ed., (London: Routledge, 2011), 56; Kan, *Cartels at War*, 35-39.

⁷⁸ Christopher Paul, Colin P. Clarke, and Chad C. Serena, *Mexico Is Not Colombia: Alternative Historical Analogies for Responding to the Challenge of Violent Drug-Trafficking Organizations*, (Santa Monica, CA: RAND Corporation, 2014).

⁷⁹ Olson, "Building Resilient Communities in Mexico," 8; Lauren Villagar, "The Victims' Movement in Mexico," in *Building Resilient Communities in Mexico*, 127.

⁸⁰ Emily Edmonds-Poli, "The Effects of Drug-War Related Violence on Mexico's Press and Democracy," in *Building Resilient Communities in Mexico*, 152; Tania Lara, "Mexican President Signs Law to Protect Journalists," *Journalism in the Americas Blog*, Knight Center for Journalism in the Americas, 25 June 2012,

Cartels, particularly newer organizations like Los Zetas, became effective at creating what John P. Sullivan called “zones of silence”, where most actors, public or private, are bribed or intimidated into not revealing information on cartel operations, resulting in little news reporting reaching the public or intelligence reaching law enforcement.⁸¹ Emily Edmonds-Poli claimed that the lack of public information in turn meant government officials felt less pressure to address cartel violence.⁸² This information gap exacerbated low levels of public trust in law enforcement, fueling a vicious circle in which law enforcement ineffectiveness reduces citizen willingness to supply intelligence to officers, which further undermines police response capacity.⁸³

In the absence of an effective government response, resistance by civil society required the organization of broad, cross-sectoral networks. These networks did not exist, as cartel leaders had proven themselves capable and willing to kill, using terms from Manuel Castells’ network theory, crucial network switchers and gatekeepers, journalists, business elites, and politicians necessary to pull disparate sections of society into effective anti-cartel alliances.⁸⁴ With no effective government presence and few feasible collective action options in many violence-racked cities in northern Mexico, organizations and individuals resorted to different self-help mechanisms to mitigate risk and/or challenge cartel influence, often with negative results. John

<https://knightcenter.utexas.edu/blog/00-10564-mexican-president-signs-law-protect-journalists>; John P. Sullivan, “Attacks on Journalists and ‘New Media’ in Mexico’s Drug War: A Power and Counter Power Assessment, *Small Wars Journal*, 9 April 2011, <http://smallwarsjournal.com/jrnl/art/attacks-on-journalists-and-new-media-in-mexicos-drug-war>.

⁸¹ Sullivan, “Attacks on Journalists and ‘New Media’ in Mexico’s Drug War.”

⁸² Edmonds-Poli, 165.

⁸³ Olson, “Building Resilient Communities in Mexico,” 8; for a discussion on similar phenomena in South Asia, see Christine C. Fair, *Urban Battlefields of South Asia: Lessons Learned from Sri Lanka, India, and Pakistan*, (Santa Monica, CA: RAND Corporation, 2004).

⁸⁴ Manuel Castells, “A Network Theory of Power,” *International Journal of Communications*, Vol. 5, 2011, 774-780.

Bailey claimed these self-help strategies were a “rational response” to a government unwilling and/or unwilling to address insecurity.⁸⁵

Some of the most common responses were defensive: businesses paid extortion fees to cartel enforcers, newspapers hired armed guards, and many fled the country altogether to avoid violence and intimidation.⁸⁶ Northern Mexico media relied primarily on self-censorship to avoid cartel attention. A 2010 media watchdog report investigated 13 Mexican regional newspapers and found only 10 percent of drug-related murders being reported, with newspapers in Nuevo León and Tamaulipas State—focus for much of the Gulf-Los Zetas conflict—reporting less than five percent even as cartel-related violence was rising in the region.⁸⁷ That same year, the Ciudad Juárez newspaper *El Diario* published an editorial addressed to the cartels asking them for guidance on what to publish following the murders of two *El Diario* journalists in two years.⁸⁸

The use of violence to create these “zones of silence” is vital to cartel information operations. This is particularly true for Los Zetas, which started as a Gulf Cartel enforcement arm founded by deserted soldiers from the Mexican Airmobile Special Forces Group (GAFE). Los Zetas has reportedly developed a sophisticated information operations and intelligence capacity, including a communications section called *La Dirección*, directed at keeping law enforcement, rival cartels, and the public from interfering in its core task of profiting from the

⁸⁵ Bailey, 75.

⁸⁶ Bailey, 88; Edmonds-Poli, 162; David Luhnow, “Elite Flee Drug War in Mexico’s No. 3 City,” *Wall Street Journal*, 10 September 2010, <http://www.wsj.com/articles/SB10001424052748704644404575482573438556534>.

⁸⁷ MEPI Foundation, “Mexico: La Nueva Espiral del Silencio: La Relación entre la Narco-Violencia y Los Medios,” 19 November 2010, http://www.fundacionmepi.org/investigaciones/la_nueva_espiral_del_silencio/; Sullivan, “Attacks on Journalists and ‘New Media’ in Mexico’s Drug War,” 6.

⁸⁸ Edmonds-Poli, 165.

drug trade and other forms of organized crime.⁸⁹ Los Zetas built upon traditional cartel information operations techniques, such as *narcomantas*, banners or other messages left on murdered bodies, on bridges, and in other public areas. According to one assessment on *narcomanta* narratives from 2009-2010, Los Zetas was one of two Mexican cartels whose IO message expanded beyond traditional efforts to silence informants to focus—over 40 percent of the time—on a broader influence over the whole local population.⁹⁰

Cartels not only attacked mass media, resulting in low levels of press reporting on drug-related violence, but also targeted more narrowcast networks, in some cases infiltrating emergency dispatch centers to kill citizens who reported incidents via Mexico's 066 emergency phone line.⁹¹ An extreme case of Los Zetas information dominance persisted in Nuevo Laredo, the busiest crossing point along the U.S.-Mexico border. By 2012, because of cartel threats, Nuevo Laredo had no effective local government, with four previous police chiefs murdered or disappeared, a local newspaper that openly claimed it would not cover cartel violence, and local NGOs, political parties, and the Catholic Church remain mute on the topic as well.⁹²

Despite the difficulty of organizing collective resistance, on multiple occasions, different local organizations attempted to counter cartel control of urban space and the information environment. Civil society coalitions tried to make up for a lack of law enforcement intelligence collection by publishing information on cartel activity, in an effort to mobilize government and other citizen actors. Two noteworthy organizations spearheaded these efforts, Todos Somos

⁸⁹ Campbell, 81; Grayson, 188; Graham H. Turbiville, "Firefights, Raids, and Assassinations: Tactical Forms of Cartel Violence and Their Underpinnings," in *Narcos Over the Border: Gangs, Cartels, and Mercenaries*, 132-33.

⁹⁰ Carlos Martin, "Categorization of Narcomessages in Mexico: An Appraisal of the Attempts to Influence Public Perception and Policy Actions," *Studies in Conflict and Terrorism*, 21 December 2011, 82.

⁹¹ Daniel M. Sabet, "Co-Production and Oversight: Citizens and Their Police," in *Building Resilient Communities in Mexico*, 248.

⁹² Dudley, 78-80.

Juárez (We Are All Juárez) in Ciudad Juárez and the Consejo Cívico de Instituciones de Nuevo León (Civic Council of Nuevo León Institutions, also known as CCINLAC) in Monterrey, both organized in large part by local business elites. These organizations published their own reports on public insecurity, and the Todos Somos Juárez security committee (Mesa de Seguridad) started its own anti-extortion campaign. It included pledges from 200 businesses not to pay cartel demands while local police agreed to patrol the central business district to keep enforcers away.⁹³ Pressure from media and NGOs also lobbied successfully for the federal government to create its own task force specifically for journalist security in 2012, allowing the government to surge protection assets to journalists who report a credible threat. The task force does not address online journalists and media professionals have complained about the task force's sometimes slow and bureaucratic response.⁹⁴

Publishing more specific information on cartel operations in the open, public realm faltered in large part because it was easy for cartel leadership to direct retaliation against fixed, knowable assets, such as newspaper offices, journalists, and NGOs. As cartel violence and subversion effectively negated any government response, it now fractured public resistance to cartel influence, as traditional forms of social organizations—business associations, newspapers, the Catholic Church, and others—sought to avoid antagonizing cartel enforcers and ceded control over public space to DTO leadership. Since neither law enforcement nor civil society could gain sufficient intelligence from a cowed population, dispersed, individual resistance remained, much of it in the form of online, pseudo-anonymous reporting of cartel activity of various social networks sites such as Facebook and Twitter.

⁹³ Lucy Conger, "The Private Sector and Public Security: The Cases of Ciudad Juárez and Monterrey," in *Building Resilient Communities in Mexico*, 180-183, 193; Dudley, 174.

⁹⁴ Edmonds-Poli, 158-159.

Online resistance should have had the advantage of being more anonymous, but it instead set off a series of escalating encounters between anti-cartel online actors and cartel counterintelligence efforts. Much of the digital anti-cartel response has focused on Los Zetas. New hybrid resistance networks consisting of local bloggers, international hackers, and Mexican information technology professionals confronted the hybrid DTO/ex-military Los Zetas organization. Online responses started at the local level and were strongest in information-poor northern Mexico. El Blog del Narco reported on drug-related crimes while the local population used the #SDR (*situaciones de riesgo*/risk situations) Twitter hashtag to report violence in specific cities.⁹⁵ Los Zetas enforcers countered by killing bloggers and threatening web sites to shut down. Four activists were brutally murdered in Nuevo Laredo in 2011 with messages attached blaming them for posting information on social media, while the administrator of a popular anti-cartel Facebook site in Tamaulipas State shut down operations after an organized crime group offered 500,000 pesos for information on him and his family.⁹⁶

A definite conclusion is unavailable, but Los Zetas had likely three mechanisms for identifying cyber informants, according to a 2011 analysis by Stratfor. It could have used its own HUMINT network to target online activity with poor offline operations security. *La Direccion* or another Los Zetas cell could have developed their own hacking capability. Finally, corrupt Mexican law enforcement could have given Los Zetas access to ISP or other telecommunications data.⁹⁷ NSAGs of the future are likely to develop one or all of these mechanisms.

⁹⁵ Edmonds-Poli, 167; El Blog del Narco, <http://www.elblogdelnarco.net/>.

⁹⁶ Shaun Waterman, "Mexico Anti-Cartel Blogger is Murdered, Decapitated," *Washington Times*, 10 November 2011, <http://www.washingtontimes.com/news/2011/nov/10/mexican-anti-cartel-blogger-is-murdered-decapitate/>; Edmonds-Poli, 167-68; "Administrador de 'Valor de Tamaulipas' anuncia cierre definitiva de la página," *El Proceso*, 7 April 2013.

⁹⁷ Stewart, Stratfor.

What were the electronic counter-reactions to Los Zetas' effective counterintelligence efforts? One response was global, the other more localized. In late 2011, following the reported kidnapping of an associated hacker in Veracruz State, some members of the loose hacker network Anonymous launched Op Cartel, threatening to reveal information on Los Zetas members and government associates to the public, exposing them to police action and/or rival cartel retaliation. The murky nature of both Anonymous and Los Zetas made confirming details—the level of actual support within Anonymous for Op Cartel or even whether anyone was actually kidnapped—difficult, but Los Zetas did reportedly release the Mexican hacker while threatening to kill ten random citizens for every name released, resulting in a draw between the two networks.⁹⁸ According to Paul Rexton Kan, this online clash was a social netwar, an effort he defines as promoting “dissident opposition movements across computer networks,” a cyber war with no government involvement.⁹⁹

Besides broad global digital networks like Anonymous, Mexican actors—members of the Mexican diaspora and large businesses—have developed new electronic forums for reporting on cartel and crime issues, linking more traditional civil society responses to insecurity to the potential for broader and more secure information collected from online platforms. Four students returning from the United States outraged by cartel domination in their city started in 2013 a local Anonymous affiliate in Ciudad Acuña, the blog Anonymous Free Acuña, which has published details on suspected ranches used by Los Zetas and claimed some credit for providing information that led to the arrest of local Los Zetas leader Alfredo Andrade Parra in 2013.

⁹⁸ Damien Cave and Ravi Somaiya, “Facts Blur as Online Feud Ends in a Draw,” *New York Times*, 4 November 2011; Stewart, Stratfor.

⁹⁹ Paul Rexton Kan, “Cyberwar in the Underworld: Anonymous versus Los Zetas in Mexico,” *Yale Journal of International Affairs*, 26 February 2013.

At the other end of the social spectrum in Monterrey, in 2010 the CEO of Mexico's largest construction materials company Cemex, Lorenzo Zambrano, launched the Center for Citizen Integration (CIC) in league with CCINLAC. Cemex and other Monterrey IT specialists supported the development of the CIC website and Tehuan, a web platform for citizens to provide security incident reports from car accidents to kidnappings, mapped for public consumption in near real-time. Since 2011, Tehuan has also been able to aggregate Twitter and SMS reporting into its database, also available via app on increasingly popular smartphones in Mexico's third-largest city.¹⁰⁰ Tehuan has received over 100,000 reports since 2010, mostly traffic and event reporting that provides an active community for reporting on security issues as well.¹⁰¹ Monterrey businessmen and activists can take advantage of Monterrey large IT community, fostered by the presence of one of Latin America's most important business and IT schools, Monterrey Institute of Technology and Higher Education (ITESM).¹⁰² IT professionals and businessmen, at home and abroad, are likely key sources of strength in any future urban conflict.

Mexico's Lessons Learned for Public Resistance Against Non-State Threats

Homicide rates in northern Mexico have leveled off since 2011, but urban populations remain vulnerable to violence from non-state actors and to the creation of new "zones of silence". Not just a threat to Mexico, but emerging megacities throughout world are commonly found in countries in similar transitional states: democratizing and globalizing, but without sufficiently strong and legitimate institutions that can maintain order during periods of rapid

¹⁰⁰ Conger, 197-198

¹⁰¹ Centro de Integración Ciudadana, Tehuan, <http://www.cic.mx/tehuan-beta/>, accessed 22 January 2015.

¹⁰² European Consortium of Innovative Universities, "Member Institutions," accessed April 20, 2015, <http://eciu.web.ua.pt/page.asp?pg=7>.

change. In the past, DTOs like the Cali and Medellin Cartels in Colombia or Christopher Coke's Shower Posse in Jamaica shown the ability to subvert the state through bribery and violence.¹⁰³ The expansion of militant groups and gangs in cities as diverse as Karachi, Greater Lagos, and Hong Kong undermines states institutions through informal links with government officials, politicians, and security forces.¹⁰⁴ The transition to more effective government institutions, if it occurs, can take decades, but local populations in the meantime perceive themselves as being left to fend for themselves, withdrawing from the public square in fear.

The northern Mexico example shows the benefit of pursuing multiple ways to restart the flow of citizen-produced information. A focus on aggregating and analyzing intelligence as produced by the local population in the open-source realm without direct intervention by security forces makes sense for several reasons. First, a future megacity in a transitional society like Monterrey will likely see similar problems with lack of capability and/or corruption in security forces. The long-term goal of an operation may be to improve the quality and effectiveness of these host nation forces, in the short-term seeking out alternatives to potentially compromised host-nation intelligence processes may prove useful. Finally, while the large majority of the population in many current megacities, particularly in Africa and parts of Asia, are not well-connected to modern communications technology, Monterrey is likely a harbinger of the future, as mobile phone and Internet penetration continues to advance and will make a larger percentage

¹⁰³ Mahatma E. Williams, "Can the Jamaican Security Forces Successfully Reduce the Violent Impact of Gangs," M.A. Thesis (Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 2012), 80; William R. Long, "Unlike Their Medellin Brethren, They Shun Open Violence: The Cali Cartel: Colombia's Gentlemen Cocaine Traffickers," *Los Angeles Times*, August 17, 1989, http://articles.latimes.com/1989-08-17/news/mn-735_1_cali-cartel.

¹⁰⁴ Fair, 121. Human Rights Watch, *Criminal Politics: Violence, "Godfathers," and Corruption in Nigeria*, October 12, 2007, <http://www.hrw.org/node/10660/section/8>; Shannon Tiezzi, "Hong Kong Police: Triads Infiltrated Occupy Movement," *The Diplomat*, October 14, 2014, <http://thediplomat.com/2014/10/hong-kong-police-triads-infiltrated-occupy-movement/>.

of future urban populations able to participate with crowd-sourced mechanisms like Tehuan or Valor por Tamaulipas.

But as the northern Mexico example shows, no force can rely on crowd-sourced open source networks for intelligence and IO effects in an interstate conflict if the local population is too afraid to participate in traditional civil society organizations or online fora. Another vicious circle is at play: as long as insecurity remains too high for widespread participation in these open-source platforms, there is a reduced chance that news of a crucial event—a massacre or egregious case of corruption—will reach broader social networks. If we look back at the Los Zetas campaign to eliminate bloggers and social media activists, there were three potential mechanisms that allowed enforcers to identify and track online activists. These were traditional HUMINT, organic cyberspace capabilities, and access via corrupt host nation law enforcement. Since we do not for sure but do know that non-state armed group cyber capabilities are likely to improve over time, all three of these techniques are potential threats to future crowd-sourced open networks.

Programs to improve security measures—sponsored by the military, development agencies, or NGOs—taken by online activists will improve the situation, but the Mexico experience suggests that one potential answer to protecting open-source virtual intelligence networks from physical threats can also include source dispersal and use of electronic safe havens. Again, megacities are well-placed terrain for developing these techniques. Their higher population density compared rural areas offers the potential for safety in numbers, many people witnessing the same cartel activities. Their higher levels of global connectedness compared to smaller cities create the opportunity to develop electronic safe havens. If online activists within a city feel threatened, they can work with outsiders located away from the non-state armed group,

such as members of Anonymous, to move information away from a more public online interface like Facebook or Twitter.

Megacities are also likely to contain or be linked to particular population groups that are themselves well-connected. In the case of Monterrey, the role of Cemex and its improved use of information technology to support crowd-sourced security efforts compared to more bureaucratic government solutions was vital. Considering the large size of the Mexican diaspora in the United States, this seems to be another potential community with close familial links that can facilitate rapid collection of information while retaining the information within the “electronic safe haven.” Even in the face of extraordinary violence, the capacity of the Mexican population to continue devising methods to resist cartel influence suggests that cities of the future may not be as fragile as we fear. Because of their globalized links, economic vitality, and density of networks, cities like Monterrey may have larger reserves of resiliency than we realize looking at their sometimes chaotic veneer.

Bibliography

- “Administrador de ‘Valor de Tamaulipas’ anuncia cierre definitiva de la página.” *El Proceso*, 7 April 2013.
- Bailey, John. *The Politics of Crime in Mexico: Democratic Governance in a Security Trap*. Boulder, CO: Lynne Rienner, 2014.
- Barstow, David. “Wal-Mart Hushed Up a Vast Mexican Bribery Case.” *New York Times*, April 21, 2012, http://www.nytimes.com/2012/04/22/business/at-wal-mart-in-mexico-a-bribe-inquiry-silenced.html?_r=0.
- Batson, Douglas. “Black Spots Are No Treasure Island: Land Tenure and Property Rights in Megacities,” in *Understanding the Reconnaissance, Surveillance, and Intelligence Paradigm*, ed. Charles R. Ehlschlaeger. Topical Strategic Multi-Layer Assessment (SMA) and U.S. Army Engineer Research Development Center (ERDC), April 2014.
- Butler, Declan. “Crowdsourcing goes mainstream in typhoon response.” *Nature*, November 20, 2013, <http://www.nature.com/news/crowdsourcing-goes-mainstream-in-typhoon-response-1.14186>.
- Campbell, Lisa J. “Los Zetas: Operational Assessments,” in *Narcos Over the Border: Gangs, Cartels, and Mercenaries*, Robert J. Bunker, ed. London: Routledge, 2011.
- Carafano, James Jay. *Wiki at War: Conflict in a Socially Networked World*. College Station, TX: Texas A&M University Press, 2012.
- Castells, Manuel. “A Network Theory of Power.” *International Journal of Communications*, Vol. 5, 2011.
- Castells, Manuel. “Communication, Power, and Counter-Power in Network Society.” *International Journal of Communication* 1, 2007, pp. 238-66.
- Castells, Manuel. *Networks of Outrage and Hope: Social Movements in the Internet Age*. Cambridge: Polity Press, 2012.
- Cave, Damien and Ravi Somaiya. “Facts Blur as Online Feud Ends in a Draw.” *New York Times*, 4 November 2011.
- Centro de Integración Ciudadana. Tehuan, <http://www.cic.mx/tehuacan-beta/>, accessed 22 January 2015.
- Conger, Lucy. “The Private Sector and Public Security: The Cases of Ciudad Juárez and Monterrey,” in *Building Resilient Communities in Mexico: Civic Responses to Crime and Violence*, David A. Shirk, Duncan Wood, and Eric L. Olson, eds. Washington, Woodrow Wilson International Center for Scholars, March 2014.
- Davis, Mike. *City of Quartz: Excavating the Future in Los Angeles*. New York: Vintage Books, 1990.

- Drug Enforcement Administration. "International Training."
<http://www.dea.gov/ops/Training/IntTraining.shtml>, accessed April 16, 2015.
- Dudley, Steven, and Sondra Rodríguez Nieto. "Civil Society, the Government, and the Development of Citizen Security," in *Building Resilient Communities in Mexico: Civic Responses to Crime and Violence*, David A. Shirk, Duncan Wood, and Eric L. Olson, eds. Washington, Woodrow Wilson International Center for Scholars, March 2014.
- Edmonds-Poli, Emily. "The Effects of Drug-War Related Violence on Mexico's Press and Democracy," in *Building Resilient Communities in Mexico: Civic Responses to Crime and Violence*, David A. Shirk, Duncan Wood, and Eric L. Olson, eds. Washington, Woodrow Wilson International Center for Scholars, March 2014.
- El Blog del Narco, <http://www.elblogdelnarco.net/>.
- European Consortium of Innovative Universities. "Member Institutions." Accessed April 20, 2015, <http://eciu.web.ua.pt/page.asp?pg=7>.
- Fair, C. Christine. *Urban Battlefields of South Asia: Lessons Learned from Sri Lanka, India, and Pakistan*. Santa Monica, CA: RAND Corporation, 2004.
- Farah, Douglas. *Organized Crime in El Salvador: The Homegrown and Transnational Dimensions*. Washington, DC: Woodrow Wilson International Center for Scholars, February 2011.
- Figliola, Patricia Maloney. *Promoting Global Internet Freedom: Policy and Technology*. Washington, DC: Congressional Research Service, October 22, 2013.
- Flynn, Michael T., James Sisco, and David C. Ellis. "'Left of Bang': The Value of Sociocultural Analysis in Today's Environment." *Prism: A Journal of the Center for Complex Operations*, 3:4, September 2012.
- FrontlineSMS. "Voix des Kivus: Data Integrity Cast Study." August 2011, <http://www.frontlinesms.com/wp-content/uploads/2011/08/Case-Study-Voix-des-Kivus-final.pdf>.
- Graham, Stephern. *Cities Under Siege: The New Military Urbanism*. London: Verso, 2010.
- Granovetter, Mark. "Threshold Models of Collective Behavior." *American Journal of Sociology*, 83:6, May 1978, 1420-1443.
- Grayson, George W. *Mexico: Narco-Violence and a Failed State?* New Brunswick, NJ: Transaction Publishers, 2010.
- Hammond, Laura, et al. *Cash and Compassion: The Role of the Somali Diaspora in Relief, Development, and Peace-Building*, Volume 1. Draft Paper for the United Nations Development Programme Somalia, 2011.

- Harris, Marc, et al. *Megacities and the United States Army: Preparing for a Complex and Uncertain Future*. Washington, DC: Chief of Staff of the Army, Strategic Studies Group, June 2014.
- Headquarters, Department of the Army. *Insurgencies and Counter Insurgencies*, FM 3-24/MCWP3/33.5. Washington, DC: Department of the Army, May 2014.
- Homeland Security Studies and Analysis Institute (HSSAI). *The Resilient Social Network: @OccupySandy #SuperstormSandy*. Falls Church, VA: HSSAI, 30 September 2013.
- Human Rights Watch. *Criminal Politics: Violence, "Godfathers," and Corruption in Nigeria*. New York: Human Rights Watch, October 12, 2007, <http://www.hrw.org/node/10660/section/8>.
- Ingram, Matthew C. "Community Resilience to Violence: Local Schools, Regional Economies, and Homicide in Mexico's Municipalities," in *Building Resilient Communities in Mexico: Civic Responses to Crime and Violence*, David A. Shirk, et al., eds. Washington: Woodrow Wilson International Center for Scholars, March 2014.
- Jacobs, Jane. *Death and Life of Great American Cities*. New York: The Modern Library, 1993, originally published 1961.
- Joint Staff. *Counterinsurgency*, JP 3-24. Washington, DC: Joint Staff, November 22, 2013.
- Joint Staff. *Joint Urban Operations*, JP 3-06. Washington, DC: Joint Staff, November 20, 2013.
- Joint Staff. *Joint Urban Operations*, JP 3-06. Washington, DC: Joint Staff, 20 November 2014.
- Kan, Paul Rexton. "Cyberwar in the Underworld: Anonymous versus Los Zetas in Mexico." *Yale Journal of International Affairs*, 26 February 2013.
- Kan, Paul Rexton. *Cartels at War: Mexico's Drug-Fueled Violence and the Threat to U.S. National Security*. Washington: Potomac Books, 2012.
- Kaplan, David E., Bay Fang, and Soni Sangwan. "Paying for Terror." *U.S. News and World Report*, 139: 21, Dec. 5, 2005.
- Kilcullen, David. *Out of the Mountains: The Coming of Age of the Urban Guerrilla*. Oxford: Oxford University Press, 2013.
- Krepinevich, Andrew F. *Cyber Warfare: A Nuclear Option?* Washington, DC: Center for Strategic and Budgetary Assessments, 2012.
- Kumar, Shiva. "Bangalore hub of techie-terror network." *The Times of India*, February 28, 2008, <http://timesofindia.indiatimes.com/india/Bangalore-hub-of-techie-terror-network/articleshow/2820775.cms>.
- La, John. "Forced Remittances in Canada's Tamil Enclaves." *Peace Review* 18, No. 3.
- Lara, Tania. "Mexican President Signs Law to Protect Journalists." *Journalism in the Americas Blog*, Knight Center for Journalism in the Americas, 25 June 2012,

<https://knightcenter.utexas.edu/blog/00-10564-mexican-president-signs-law-protect-journalists>.

- Leetaru, Kalev H., and Charles R. Ehlschlaeger. "Modeling the Discourse of Megacities: Assessing Remote Populations in Non-Western Worlds," in *Understanding the Reconnaissance, Surveillance, and Intelligence Paradigm*, ed. Charles R. Ehlschlaeger. Topical Strategic Multi-Layer Assessment (SMA) and U.S. Army Engineer Research Development Center (ERDC), April 2014.
- Lohr, Steve. "Online Mapping Shows Potential to Transform Relief Efforts." *New York Times*, March 28, 2011, http://www.nytimes.com/2011/03/28/business/28map.html?_r=0.
- Long, William R. "Unlike Their Medellin Brethren, They Shun Open Violence: The Cali Cartel: Colombia's Gentlemen Cocaine Traffickers." *Los Angeles Times*, August 17, 1989, http://articles.latimes.com/1989-08-17/news/mn-735_1_cali-cartel.
- Luhnow, David. "Elite Flee Drug War in Mexico's No. 3 City." *Wall Street Journal*, 10 September 2010, <http://www.wsj.com/articles/SB10001424052748704644404575482573438556534>.
- Lunden, Ingrid. "Crowdsourced WiFi Network Fon Picks Up \$14M Led by Qualcomm, Adds Facebook Integration." *TechCrunch*, Jan. 20, 2014, <http://techcrunch.com/2014/01/20/crowdsourced-wifi-network-fon-takes-another-picks-up-another-14m-led-by-qualcomm-adds-facebook-integration/>.
- Mackinlay, John. *The Insurgent Archipelago*. New York: Columbia University Press, 2009.
- Marine Corps Intelligence Activity (MCIA). *Urban Warfare Study: City Case Studies Compilation*. Quantico, VA: MCIA, 1995.
- Martin, Carlos. "Categorization of Narcomessages in Mexico: An Appraisal of the Attempts to Influence Public Perception and Policy Actions." *Studies in Conflict and Terrorism*, 21 December 2011.
- MEPI Foundation. "Mexico: La Nueva Espiral del Silencio: La Relación entre la Narco-Violencia y Los Medios." 19 November 2010, http://www.fundacionmepi.org/investigaciones/la_nueva_espiral_del_silencio/.
- Niqash.org. "Communications Shut Down: Why Extremists in Mosul Have Blocked All Telecommunications." Dec. 4, 2014, <http://www.niqash.org/articles/?id=3589>.
- Nixon, Ron. "Cuba Social Media Project Was No Plot, Agency Says." *New York Times*, April 8, 2014, http://www.nytimes.com/2014/04/09/world/americas/us-agency-defends-social-media-project-in-cuba.html?_r=0.
- Olson, Eric L., David A. Shirk, and Duncan Wood. "Introduction: Building Resilient Communities in Mexico," in *Building Resilient Communities in Mexico: Civic Responses to Crime and Violence*, Shirk, Wood, and Olson, eds. Washington: Woodrow Wilson International Center for Scholars, March 2014.

- Olson, Mancur. *The Logic of Collective Action: Public Goods and the Theory of Organizations*. Cambridge, MA: Harvard University Press, 1971.
- Panek, Jiri. "The Commercialisation of Public Data – How Does Participatory Data-Mining Look on a Global Scale?" *South African Journal of Geomatics* 2, No. 3, June 2013.
- Paul, Christopher, Colin P. Clarke, and Chad C. Serena, *Mexico Is Not Colombia: Alternative Historical Analogies for Responding to the Challenge of Violent Drug-Trafficking Organizations*. Santa Monica, CA: RAND Corporation, 2014.
- Pew Research Center. "Emerging Nations Embrace Internet, Mobile Technology." February 2014, 12-13, <http://www.pewglobal.org/files/2014/02/Pew-Research-Center-Global-Attitudes-Project-Technology-Report-FINAL-February-13-20147.pdf>.
- Rogoway, Mike. "Google Who? Oregon Cities Want Their Own Fiber Networks." *The Oregonian/Oregon Live*, April 7, 2015, http://www.oregonlive.com/silicon-forest/index.ssf/2015/04/google_who_hillsboro_gresham_1.html.
- Ronfeldt, David, et al. *The Zapatista Social Netwar in Mexico*. Santa Monica, CA: RAND Arroyo Center, 1998.
- Sabet, Daniel M. "Co-Production and Oversight: Citizens and Their Police," in *Building Resilient Communities in Mexico: Civic Responses to Crime and Violence*, David A. Shirk, Duncan Wood, and Eric L. Olson, eds. Washington, Woodrow Wilson International Center for Scholars, March 2014.
- Samuelson, Jared. "Canvassing for Combat: The Human Terrain Map Operational Concept." unpublished draft, Marine Corps Command and Staff College MMS paper, February 4, 2015.
- Shirk, David A., Duncan Wood, and Andrew Selee. "Conclusion: Toward a More Comprehensive and Community-based Approach to Public Security," in *Building Resilient Communities in Mexico: Civic Responses to Crime and Violence*, David A. Shirk, et al., eds. Washington: Woodrow Wilson International Center for Scholars, March 2014.
- Sopko, John F. "Letter from SIGAR to ISAF Commanding General Joseph H. Dunford, Jr." Office of the Special Inspector General for Afghan Reconstruction, July 31, 2013.
- Stewart, Scott. "Anonymous vs. Zetas Amid Mexico's Cartel Violence." *Security Weekly*, Stratfor Global Intelligence, November 2, 2011, <https://www.stratfor.com/weekly/20111102-anonymous-vs-zetas-amid-mexico-cartel-violence>.
- Sullivan, John P. "Attacks on Journalists and 'New Media' in Mexico's Drug War: A Power and Counter Power Assessment." *Small Wars Journal*, 9 April 2011, <http://smallwarsjournal.com/blog/journal/docs-temp/730-sullivan1.pdf>.

- Sullivan, John P. "Attacks on Journalists and 'New Media' in Mexico's Drug War: A Power and Counter Power Assessment." *Small Wars Journal*, 9 April 2011, <http://smallwarsjournal.com/blog/journal/docs-temp/730-sullivan1.pdf>.
- Sullivan, John P. "Policing Networked Diaspora.," *Small Wars Journal*, July 9, 2007, <http://smallwarsjournal.com/blog/policing-networked-diasporas>.
- Sullivan, John P. "Policing Networked Diasporas." *Small Wars Journal*, 9 July 2007.
- Sullivan, John P., and Adam Elkus. "Command of the Commons: Towards a Theory of Urban Strategy." *Small Wars Journal*, September 26, 2011, <http://smallwarsjournal.com/printpdf/11533>.
- Thomas, Timothy. "Russian's Reflexive Control Theory and the Military." *Journal of Slavic Military Studies*, 17:2, 2004, 237-256.
- Tiezzi, Shannon. "Hong Kong Police: Triads Infiltrated Occupy Movement." *The Diplomat*, October 14, 2014, <http://thediplomat.com/2014/10/hong-kong-police-triads-infiltrated-occupy-movement/>.
- Turbiville, Graham H. "Firefights, Raids, and Assassinations: Tactical Forms of Cartel Violence and Their Underpinnings," in *Narcos Over the Border: Gangs, Cartels, and Mercenaries*, Robert J. Bunker, ed. London: Routledge, 2011.
- U.S. Department of Justice. "Foot Patrols: Crime Analysis and Community Engagement to Further the Engagement to Community Policing." *Community Policing Dispatch*, 2:2, November 2009, http://cops.usdoj.gov/html/dispatch/February_2009/foot_patrol.htm.
- Van der Windt, Peter, and Macartan Humphreys. "Crowdseeding in Eastern Congo: Using Cell Phones to Collect Conflict Events Data in Real Time." *The Journal of Conflict Resolution*, Nov. 4, 2014.
- Villagar, Lauren. "The Victims' Movement in Mexico," in *Building Resilient Communities in Mexico: Civic Responses to Crime and Violence*, David A. Shirk, Duncan Wood, and Eric L. Olson, eds. Washington, Woodrow Wilson International Center for Scholars, March 2014.
- Waterman, Shaun. "Mexico Anti-Cartel Blogger is Murdered, Decapitated." *Washington Times*, 10 November 2011, <http://www.washingtontimes.com/news/2011/nov/10/mexican-anti-cartel-blogger-is-murdered-decapitate/>.
- Williams, Mahatma E. "Can the Jamaican Security Forces Successfully Reduce the Violent Impact of Gangs," M.A. Thesis. Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 2012.