The Centre for the Study of Terrorism and Political Violence
Journal of Terrorism Research

ISIL'S Battlefield Tactics and the Implications for Homeland Security and Preparedness

by Joshua Tallis, Ryan Bauer, Lauren Frey

Abstract

This proposed article investigates the emergency management implications of a terrorist attack directly planned and executed by ISIL in the United States. To do so, we operationalize the Department of Homeland Security's National Preparedness Goal (NPG) to demonstrate how ISIL-directed attacks might stress national preparedness Core Capabilities. In so doing, we provide a proof of concept, demonstrating how viewing the ISIL threat through an emergency preparedness lens can help better benchmark existing national preparedness activities and policies against emerging threats.

Introduction

Of the numerous tactics that ISIL has cultivated on the battlefields of Iraq and Syria, could any present threats in an American domestic context? Relatedly, once we understand what types of threats ISIL could employ in an attack against the United States,[a] how can we discuss them in a manner that proves meaningful for policymakers at all levels of government?

Answering the first question requires, at the outset, an understanding of the tactics ISIL has employed on the battlefield. Fortunately, a report written by CNA's Center for Stability and Development, *Adaptive and Innovative: An Analysis of ISIL's Tactics in Iraq and Syria*, expertly navigates this landscape. Leveraging its findings, we isolated 10 of the report's 14 tactics that exhibit the greatest relevance to the domestic context. To select these ten, we filtered out those tactics in the report that were geographically bound to unique Iraqi and Syrian contexts. This primarily resulted in excluding tactics related to capturing and holding cities. We also considered the process by which tactics might be transferred from the battlefield to the United States, paying particular attention in our selection process (and subsequent vignettes below) to the knowledge component of ISIL's tactics. For example, the knowledge of how to conduct an attack (e.g. how to construct chemical weapons) is more easily transferred to the United States—either through returning foreign fighters or electronic communications—than actually transferring chemical weapons. This selection process was validated both through consensus among the authors and in consultation with a research team leader from the original CNA report.

The ten tactics are listed below, and will be explored in individual vignettes in turn. These vignettes serve principally to describe the tactics, as well as to offer a perspective (though not a comprehensive assessment) on how such tactics might manifest in an attack in the United States.

[a] ISIL-directed attacks, as defined here, are those where conceptual or tactical aid is provided by ISIL members to attackers (perhaps by encrypted messaging or through the direct return of foreign fighters to the United States). Lone wolves and those self-radicalized by ISIL, but not in communication with or organized by the group, do not constitute ISIL-directed attacks.

1. Operations Security
2. Intelligence Apparatus
3. Shaping the Battlespace
4. Tunnels
5. Waterways
6. Theatrical Brutality
7. Cyber Command and Control
8. Drones
9. Improvised Explosive Devices
10. Chemical Weapons

To make this identification of tactics useful for practitioners at all levels of government, we mapped each tactic to the emergency preparedness framework set in place by the Department of Homeland Security, the National Preparedness Goal. DHS (led by the Federal Emergency Management Agency, FEMA) developed the National Preparedness Goal to help ensure that all levels of government could work towards common homeland security objectives using a common language. The Goal codifies all preparedness activities into five Mission Areas—Prevention, Protection, Mitigation, Response, and Recovery—which include a total of 32 Core Capabilities (see Table 1). Core Capabilities comprise the operational elements of each Mission Area. Each Core Capability is further characterized by Critical Tasks, which represent the various tactical-level tasks that collectively define a capability. It is specifically to these tasks that we mapped each tactic. Our primary consideration when matching tactics with tasks was to capture, in our assessment, whether tactics would likely stress the delivery of a given capability.b This mapping was informed by the authors' experience contributing to the development of FEMA's 2016 and 2017 *National Preparedness Reports* and was validated through consensus.

[b]Stress is defined as the potential for a tactic to overwhelm a jurisdiction's independent capacity to counter a threat. Core Capabilities specific to the Recovery Mission Area were excluded from this article in the spirit of analytical humility, as including them would require making judgements on the potential fallout from an attack, not simply on the tactics employed.

Prevention	Protection	Mitigation	Response	Recovery
Planning				
Public Information and Warning				
Operational Coordination				
Intelligence and Information Sharing		Community Resilience	Infrastructure Systems	
Interdiction and Disruption		Long-term Vulnerability Reduction	Critical Transportation	Economic Recovery
Screening, Search, and Detection		Risk and Disaster Resilience Assessment	Environmental Response/Health and Safety	Health and Social Services
Forensics and Attribution	Access Control and Identity Verification	Threats and Hazards Identification	Fatality Management Services	Housing
	Cybersecurity		Fire Management and Suppression	Natural and Cultural Resources
	Physical Protective Measures		Logistics and Supply Chain Management	
	Risk Management for Protection Programs and Activities		Mass Care Services	
	Supply Chain Integrity and Security		Mass Search and Rescue Operations	
			On-scene Security, Protection, and Law Enforcement	
			Operational Communications	
			Public Health, Healthcare, and Emergency Medical Services	
			Situational Assessment	

Figure 1. Core Capabilities and Mission Areas of the National Preparedness Goal[1]

In addition to providing practitioners a common language for preparedness activities (no small feat, considering preparedness efforts span everyone from small-town part-time emergency coordinators to FBI agents), these capabilities also provide a means for the government to track spending on grants and programs related to emergency preparedness, which are often categorized by relevant capability. As a result, by mapping ISIL's tactics to Core Capabilities, we can provide a means for practitioners to reflect on whether their jurisdiction's level of proficiency or spending in a given capability is sufficient to meet the threat. Our mapping simultaneously offers practitioners an opportunity to reflect on the tactics that map to the greatest variety of Core Capabilities, to see if their jurisdiction's overall distribution of proficiency or funding meets the complex threat of some particularly multidimensional tactics.

Importantly, we cannot make these judgements for practitioners. ISIL is only one of a variety of threats and hazards that emergency management and homeland security professionals face. As a result, we cannot simply

look at spending on a Core Capability that our mapping identifies and say whether this level of resourcing is or is not sufficient. Practitioners must factor in, using their professional judgement and a host of risk assessment tools, how large a portion of scarce resources they choose to devote to the threat of an ISIL-executed terrorist attack in their community. Nevertheless, we believe that providing this mapping offers practitioners a more educated starting point in their self-evaluations.

Finally, this mapping depicts a relatively novel approach. While the Goal sets the standard language and operations for emergency preparedness cooperation and planning, it includes no explicit mechanism for benchmarking how a given threat relates to operational capabilities. The mapping we employ provides a means of operationalizing the Goal. This, in turn, makes it simpler to discuss emerging threats in the context of the nation's shared preparedness lexicon, bringing counterterrorism and emergency management professionals from all levels of government into a single conversation on countering ISIL.

ISIL Tactics

In this section, we discuss the 10 ISIL tactics, originally cultivated on the battlefield, that we assessed were potentially employable in an attack in the United States. Each tactic includes a description and explores how its employment in a U.S. attack could stress national preparedness capabilities. Charts throughout this section illustrate the Core Capabilities that these tactics might stress.

Tactic 1: Operations Security

On the battlefield, ISIL has not only adapted its methods of operations security (OPSEC) in response to coalition force actions, such as airstrikes, but it has also learned how to protect operational information leading up to an attack. In the 2015 assault on Ramadi, Iraq, for example, ISIL fighters arrived to the area in groups of two or three in nondescript vehicles, instead of using military caravans, reducing the likelihood of forces being identified en route.[2] Fighters also began moving within the wider flow of civilian traffic, sometimes using their own families as concealment.[3] In addition to its evolving ability to employ OPSEC in practice, ISIL's OPSEC policy is pointedly elucidated. The group has used a modified written OPSEC manual from a Kuwaiti company, which has been distributed to troops throughout the terrorist organization, as a model for how to employ OPSEC.[4] OPSEC has even stretched into cyberspace, with the embrace of encrypted messaging services by ISIL operatives (more on this below).

In a domestic context, this robust and institutionalized knowledge of OPSEC could serve to complicate interdiction operations by concealing directed attacks on western targets. Already, in the aftermath of successful attacks in Paris and Belgium, it is evident that the use of OPSEC tactics has stressed intelligence and law enforcement agencies' capacity to detect, interdict, and disrupt potential attacks. According to a report on the attacks in Paris released by French authorities, for example, ISIL operatives used disposable phones and encrypted laptops to avoid detection or compromising future operations.[5]

Tactic 2: Intelligence Apparatus

Within their controlled territory, ISIL operates a thriving intelligence structure. The group's middle and upper echelons, former Saddam-era military and intelligence officers, provide it with an experienced Ba'athist infrastructure on which a functioning security apparatus was constructed.[6] As a result, these professional underpinnings have helped to form a solidified intelligence system within ISIL, undergirded by

documentation and experience-driven practices.[7] In Iraq and Syria, this network has been used to root out dissent and launch preemptive attacks on massing Iraqi forces.[8]

Focused abroad, ISIL's intelligence structure could, in theory, be deployed to support recruitment, extortion, targeting, and criminal activities. Some reports suggest that this is already occurring.[9] If leveraged in the same professionalized manner as seen in Iraq and Syria, this intelligence apparatus could pose a serious challenge to intelligence agencies, cyber security operators, and western governments attempting to counter violent extremism and interdict planned attacks. An interview conducted by *The New York Times* with a returning foreign fighter incarcerated in Germany details how ISIL's bureaucratized and professionalized process is already being employed to identify, recruit, train, and deploy foreign fighters for attacks in Europe.[10] The former ISIL recruit also notes that those same forces focus extensively on online communication and guidance for those undergoing radicalization in the United States, raising the prospect for an attack orchestrated by ISIL using homegrown extremists.[11]

Tactic 3: Shaping the Battlespace

ISIL has shown a depth of tactical patience in its approach to shaping operations. The group has infiltrated sleeper cells into targeted cities and villages, a few people at a time, over weeks—and even months—prior to planned attacks.[12] Efforts such as smuggling in fighters and pre-staging weapons, conducting reconnaissance, and perhaps even making contact with sympathizers have helped to provide ISIL with a depth of support even before a campaign is launched.[13] This detail-oriented approach to long-running intelligence gathering, surveillance, and reconnaissance prior to an assault presents counterterrorism, intelligence, and first responder personnel with a strategically adept adversary.

The porous nature of borders in parts of Europe may facilitate the access of poorly vetted individuals into international transportation flows. ISIL's skill in shaping operations could, therefore, stress domestic interdiction and disruption operations; screening, search, and detection programs; and access control and identity verification (with respect to accessing critical locations, like airports or border crossings). A deliberate, inconspicuous planning process also portends sophisticated coordinated attacks, which further complicate physical protective measures and related operations.

Public Information and Warning			✕
Intelligence and Information Sharing	✕	✕	
Interdiction and Disruption	✕	✕	✕
Screening, Search, and Detection	✕		✕
Access Control and Identity Verification			✕
Cybersecurity		✕	✕
Physical Protective Measures			✕
Threats and Hazards Identification	✕		✕
Situational Assessment	✕		

Tactic 4: Tunnels

In response to aerial surveillance and coalition airstrikes, ISIL has moved to exploit existing Saddam-era (and some ancient) tunnel networks in the territory it holds, as well as to excavate new tunnels.[14] While tunnels are frequently used to conceal and protect the movement of people and resources (e.g., Hamas activities in the Gaza Strip), ISIL has also exploited the subterranean domain as a staging ground for covert assaults. In the attack against Ramadi, for example, the organization used a tunnel to detonate a massive improvised explosive device (IED) underneath a fortified Iraqi Army base.[15]

While it is unlikely that an 800-foot tunnel and mounds of explosive material would go unnoticed in a U.S. city, the nearly 50 tunnel-based IEDs deployed by ISIL in Iraq and Syria reflect tactical ingenuity with respect to operational space.[16] Moreover, since tunnels have long been used on the U.S. southern border to facilitate the illicit movement of people and contraband into and out of the country, the prospect of similar uses by a terrorist organization may not be unreasonable. ISIL's conception of operational space is similarly reflected in the group's use of "urban tunnels" (holes blasted between adjoining buildings),[17] a tactic similarly used by the Israeli Defense Forces in Gaza to minimize exposure to ambush.[18] In a potential confrontation with law enforcement in the U.S., ISIL's operational familiarity with subterranean and urban spaces could afford the attackers greater capacity to evade capture or prolong the engagement. In addition, unobserved movement could threaten controlled access to critical infrastructure or facilities. Ultimately, failure to adequately identify and prioritize such threat vectors in protective and risk management programs may leave infrastructure and populations vulnerable.

Tactic 5: Waterways

The operational utility of employing waterways for terrorist attacks was made glaringly evident in the 2008 Lashkar-e-Taiba attack on Mumbai, wherein attackers entered India from Pakistan by boat. ISIL has already ventured into the maritime space by using waterways both as supply and infiltration routes.[19] ISIL has demonstrated an interest in using Iraq's rivers both to transport people and to stage attacks. On January 10, 2015, ISIL launched an offensive on Kurdish forces by crossing the Tigris and Great Zab Rivers in boats.[20] While the attack was ultimately unsuccessful, Peshmerga forces were outflanked by the riverine assault.[21] Ultimately, U.S. Central Command recorded destroying 21 ISIL boats by air in support of Kurdish forces in that assault, demonstrating the breadth of ISIL's utilization of waterways.[22] Moreover, ISIL's attacks on Dhuluiya (Iraq) in September 2014,[23] Ramadi (Iraq) in May 2015,[24] and villages near Kobani (Syria) in April 2015,[25] similarly reflect their use of waterways during operations.

ISIL has also demonstrated an interest in controlling or destroying waterborne critical infrastructure, such as dams[26] and bridges[27]—tactics with clear implications in an attack on western targets. Boat-borne explosive devices were reportedly destroyed by Iraqi forces in March 2015,[28] and Shia militia forces similarly destroyed a waterborne bomb on a collision course with the Tigris River's Saamarra Dam.[29] In a domestic scenario, the use of waterways not only threatens maritime critical infrastructure, but places a jurisdictionally complicated domain at the center of an attack. Waterways often serve as dividing lines between states or municipalities and are subject to a variety of authorities, from the Coast Guard to local police. As a result, coordination and communication in response to a waterborne attack could prove complicated in certain environments.

Tactic 6: Theatrical Brutality

ISIL is infamous for its barbarity; the organization has thrived in part by brutalizing and striking fear into the populations it seeks to control. While specific tactics, such as mass executions, are not a common threat in regions free of ISIL control, the group's broader focus on theatrical brutality informs the likely nature of potential terrorist attacks. Barbarity serves as a force multiplier,[30] augmenting the group's impact by projecting an image of unbridled violence. If fear is the ultimate tactic in any terror campaign, ISIL's mastery of psychological warfare (not only the gruesome nature of its beheadings, for example, but the use of excessive violence as a central marketing tool) suggests that attacks carried out by the group would be refined to cause maximum panic.

Because of the barbarous quality of a potential attack and subsequent distribution of violent images online, western authorities could be challenged on a number of fronts. For example, a focus on disturbing and 'marketable' attacks impact risk management and community resilience programs, which may fail to consider ISIL's radical risk profile (e.g., the targeting of a nursing home or daycare facility). Moreover, if the fear generated by an incident was manipulated to create widespread panic, the result would threaten authorities' ability to message to the public and control the narrative during an attack. Even the mere rumor of gunfire at New York's Kennedy airport in August 2016 (and then at Los Angeles's LAX only weeks later) prompted mass hysteria. As rumors of a suspected shooter emerged, travelers broke through secure doors onto the tarmac, and airport employees reportedly removed their uniforms and fled.[31] This environment challenged response officials trying to manage the panic,[32] even without a concerted campaign by a group like ISIL attempting to leverage violence to maximize havoc.

Tactic 7: Cyber Command and Control

Much has been written on ISIL's unprecedented success on social media. This success feeds into the fear mentioned above, and serves to inspire attacks by self-radicalized individuals in the West (as occurred in San Bernardino, CA). Less, however, has been written on the group's understanding of the role of cyberspace as a tactical tool. In battles waged across Iraq and Syria, as well as online, ISIL has leveraged social media and online forums as "command and control" (C2) platforms.[33] During the ISIL operation to take Mosul, Iraq in 2014, for example, leadership used such tools both to direct the campaign and, simultaneously, to obfuscate local situational awareness through a massive propaganda assault including 40,000 tweets.[34]

The implications of using social media to conduct real-time command and control in a potential terrorist attack cannot be overstated. In the 2008 Mumbai attacks, operators staged in Pakistan leveraged social and traditional media information platforms to glean operational and response details and feed orders and targets to attackers on the ground, to a devastating effect.[35] With the adoption of encrypted social messaging apps,[36] ISIL will continue to use technology to coordinate its operations, wherever they take place. This will ultimately stress domestic capacity to leverage cyber assets to interdict and disrupt planned attacks in the West.

Core Capabilities	Tunnels	Waterways	Brutality	Cyber C2
Public Information and Warning			✖	
Operational Coordination		✖		
Interdiction and Disruption	✖	✖	✖	✖
Access Control and Identity Verification	✖	✖		
Cybersecurity				✖
Physical Protective Measures	✖	✖		
Risk Management for Protection Programs and Activities	✖	✖	✖	
Supply Chain Integrity and Security		✖		
Community Resilience			✖	
Infrastructure Systems		✖		
Critical Transportation		✖		
Facility Management Services			✖	
Mass Care Services			✖	
Mass Search and Rescue Operations			✖	
On-scene Security, Protection, and Law Enforcement	✖		✖	
Public Health, Healthcare, and Emergency Medical Services			✖	
Situational Assessment			✖	

Tactic 8: Drones

ISIL has exploited commercial drones in support of its operations in both Iraq and Syria. This support has manifested into three different functions. The first is for the purpose of propaganda development, in which ISIL uses drones to capture footage of its attacks for use in propaganda videos.[37] By providing footage such as aerial views of coordinated assaults and suicide attacks, ISIL demonstrates its technical capacity while enhancing fear of the organization and promoting recruitment.[38] The second function is for conducting reconnaissance before an attack. In August 2014, for example, ISIL used a drone to conduct surveillance of the Tabqa military airfield in Syria before the group moved in and captured the base.[39] The third—and, arguably, most daunting—function of ISIL's drone practice is to provide real-time command and control and targeting for the organization. This was demonstrated in ISIL's assault last year on the Baji oil refinery complex in Iraq, in which ISIL commanders sitting in an operations room used drones to direct the assault and provide real-time targeting for fighters on the ground.[40]

The skills necessary to use drones in these fashions are potentially transferable, certainly portable, and may even be deployed remotely, thus raising the potential for drones to play a role in an ISIL-planned attack on domestic targets. ISIL's ability to perform functions such as live targeting and reconnaissance has the potential to severely strain first-responder capabilities and threaten responders with highly coordinated assaults and follow-on attacks as they seek to provide on-scene security and protection. Drones could simultaneously stress interdiction and disruption capabilities, as the use of drones informs the movement of terrorists during an incident. In addition, the use of drones could cause confusion over jurisdictional

responsibility, as regulations continue to evolve outlining which entities—whether local, state, or federal—assume responsibility for low-altitude airspace or regions near certain pieces of infrastructure. Finally, the ease and affordability of obtaining commercial drones raises the potential of ISIL using them for coordinated IED attacks, given the group's level of expertise in constructing novel IEDs (see below).

Tactic 9: Improvised Explosive Devices

ISIL has built a robust institutional knowledge in the construction and deployment of IEDs. One prominent example is in the construction of super vehicle-borne improvised explosive devices (super-VBIEDs), which are deadlier and more powerful versions of previous VBIEDs used by terrorist organizations in the region. While traditional VBIEDs were sedans or occasionally trucks with an explosive charge, super VBIEDs are typically up-armored bulldozers, dumpsters, or even tanks. And whereas IEDs have been used historically as traps or for small operations, ISIL is increasingly relying on super VBIEDs (such as bulldozers packed with explosives comparable to the Oklahoma City bombing) as a primary front-line weapon.[41] In April 2015, for instance, ISIL launched approximately 27 super VBIEDs in its assault on Ramadi, which effectively penetrated Iraqi defensive perimeters and destroyed entire city blocks, allowing ISIL forces to flow into the city amid a haze of fear.[42] ISIL has heavily relied on employing IEDs for defensive purposes, as well, in an effort to secure cities or curtail the advancement of Iraqi and Kurdish ground forces. As these forces have pushed to retake ISIL-captured cities such as Ramadi and Tikrit, troops have encountered serious difficulties moving through areas littered with IED booby-traps.[43] The ingenuity with which ISIL attaches IEDs to people, cars, trucks, boats, tunnels, roadways, and potentially drones—both to stage attacks and to routinely control the flow of pedestrian or vehicle traffic—suggests an organization with adaptable and transferable explosives expertise.

One area of national preparedness that this expertise could strain is in developing physical protective measures for critical infrastructure. With a range of potential targets, from nuclear power plants and military bases (high-profile facilities) to mass-populated areas like malls or businesses (soft targets), infrastructure owners and operators may be forced to consider the consequences of creatively deployed IEDs (or even super VBIEDs) in their communities more than ever before. ISIL's ability to construct IEDs at a low-cost and rapid rate also complicates domestic detection efforts for chemical, biological, radiological, nuclear, and explosive weapons, especially if this expertise were to be transferred to people who are geographically dispersed. The use of super VBIEDs, in particular, may also strain medical and law enforcement first responder efforts in the event of an attack, due to the extent of injuries and fatalities and the threat of follow-on and defensive IEDs to on-scene law enforcement personnel.

Tactic 10: Chemical Weapons

ISIL's territorial holdings and confiscated military stores provide the organization with considerable leniency to experiment with chemical weapons.[44] The product of this experimentation has resulted not only in chemical IED attacks, but also in the construction of chemical mortar shells, which have been used to target both security forces and civilians.[45] Though ISIL's crude chemical weapons are less lethal than those of military grade, as well as in comparison to other weapons such as guns or explosives, chemical attacks can have a profound psychological impact.[46] Reports that the organization is recruiting experts in chemical weapons lend further credence to the concern that ISIL could employ chemicals in a terror attack.[47]

Such knowledge is highly transferable, particularly if ISIL attracts university students or graduates in the West. A chemical terrorist attack in the United States could strain a number of capabilities, including public information and warning and first responder capacities. In either a suspected or attempted chemical attack—successful or not—the challenge of monitoring public information and providing information to calm public fears and reach affected populations would be increasingly demanding. The effects of a chemical attack (or radiological attack, for that matter) would also significantly complicate the response of law enforcement and medical personnel, given the threat of exposure to chemical (or radiological) agents when arriving on scene and the number of medical countermeasures that may be required for the exposed population.

Core Capabilities	Drones	Chemicals	IEDs
Public Information and Warning		✖	✖
Operational Coordination	✖		
Interdiction and Disruption	✖	✖	✖
Screening, Search, and Detection		✖	✖
Forensics and Attribution		✖	✖
Physical Protective Measures	✖		✖
Risk Management for Protection Programs and Activities			✖
Community Resilience			✖
Threats and Hazards Identification		✖	
Critical Transportation			✖
Environmental Response/Health and Safety		✖	
Facility Management Services			✖
Mass Care Services			✖
On-scene Security, Protection, and Law Enforcement	✖	✖	✖
Public Health, Healthcare, and Emergency Medical Services		✖	✖

Results

The three Core Capabilities impacted by the widest variety of potential ISIL tactics are Interdiction and Disruption; Physical Protective Measures; and On-scene Security, Protection, and Law Enforcement (see Figure 2).

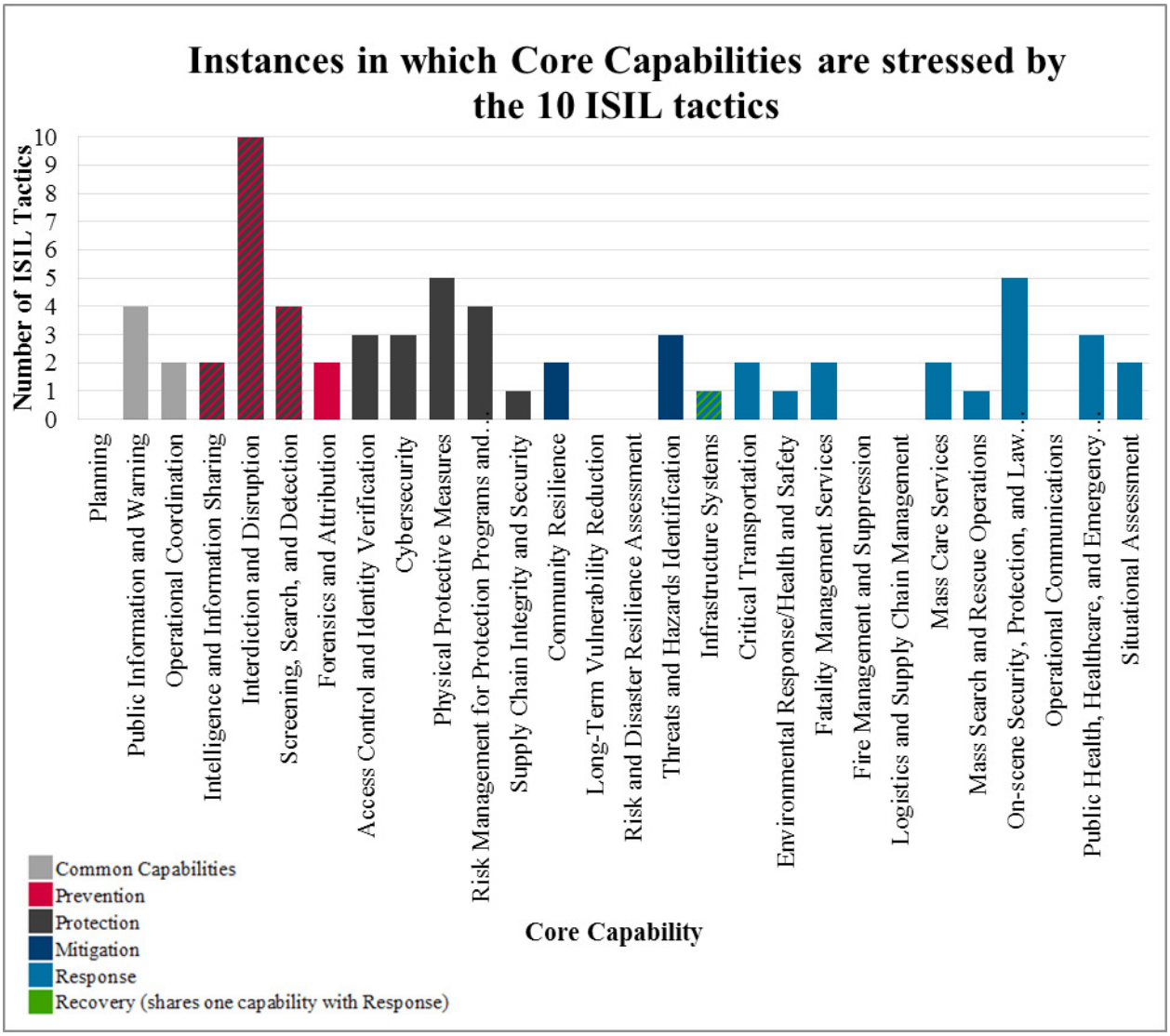

Figure 2: All ten ISIL tactics were mapped to Interdiction and Disruption in our crosswalk, while half of all tactics were mapped both to Physical Protective Measures and On-scene Security, Protection, and Law Enforcement.

Interdiction and Disruption, a responsibility shared between the Prevention and Protection Mission Areas, addresses the need to "delay, divert, intercept, halt, apprehend, or secure threats and/or hazards."[48] The connections to potential terrorist attacks are relatively straightforward. ISIL's shaping operations, combined with innovative uses of technology and a sophisticated understanding of operational space, make detecting and disrupting an ISIL-directed attack a complex endeavor.

Physical Protective Measures, under the Protection Mission Area, address the need to "implement and maintain risk-informed countermeasures, and policies protecting people, borders, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors."[49] Again, the connections are relatively straightforward. ISIL's tactical flexibility makes it difficult to maintain timely, risk-informed countermeasures, as the risk is in a state of perpetual evolution. Moreover, the unique

tactics with which ISIL approaches hard targets (adaptive uses of IEDs, tunneling, or employing waterways, for example) complicate traditional means of evaluating and securing critical infrastructure, further stressing this capability.

Finally, On-scene Security, Protection, and Law Enforcement (under the Response Mission Area) addresses the need to "ensure a safe and secure environment through law enforcement…for people and communities located within affected areas and also for response personnel."[50] Tactics that inflame public panic, involve hazardous materials, conceal attackers, or include a second strike targeting responders all place burdens on ensuring the safety of communities and those attempting to secure them.

As we noted above, these Core Capabilities may not necessarily be the highest priority for jurisdictions given broader risk considerations, but they provide practitioners a means to consider how their proficiencies and resource allocations across capabilities meet the ISIL threat. We can, additionally, provide some context on proficiency and resourcing to aid in that self-reflection. Over the last six years, for example, none of the top three affected Core Capabilities listed above have been identified as national areas for improvement or at risk of declining in *National Preparedness Reports*. This suggests that capabilities nationally are (broadly speaking) likely sufficient to meet all-hazards. As of the 2016 *National Preparedness Report*, state and territory self-evaluation rankings provide a more nuanced outlook. For both Interdiction and Disruption and Physical Protective Measures, less than half of states rated themselves as proficient (a 4 or 5 on a 5 point scale) in these capabilities—42 percent and 35 percent, respectively.[51] For On-scene Security, Protection, and Law Enforcement,c however, 60 percent rated themselves as proficient.[52]

The 2016 *National Preparedness Report* also provides a rough proxy measure of resource allocation through FEMA's non-disaster preparedness grant spending (Figure 3). For states in 2014 (the latest data reflected in the report), Interdiction and Disruption was the eighth most funded of the 32 Core Capabilities (Figure 3).[53] For comparison, Interdiction and Disruption is fourteenth when capabilities are ranked by proficiency. Physical Protective Measures is among the top-five capabilities by funding[54] and falls in the bottom ten by proficiency. Meanwhile, On-scene Security, Protection, and Law Enforcement ranked ninth overall in FEMA grant funding and third overall by proficiency.[55]

[c] In the 2016 NPR, the Core Capability is listed as On-scene Security and Protection. Some capabilities underwent renaming and slight adaptation during a 2015 revision of the National Preparedness Goal.

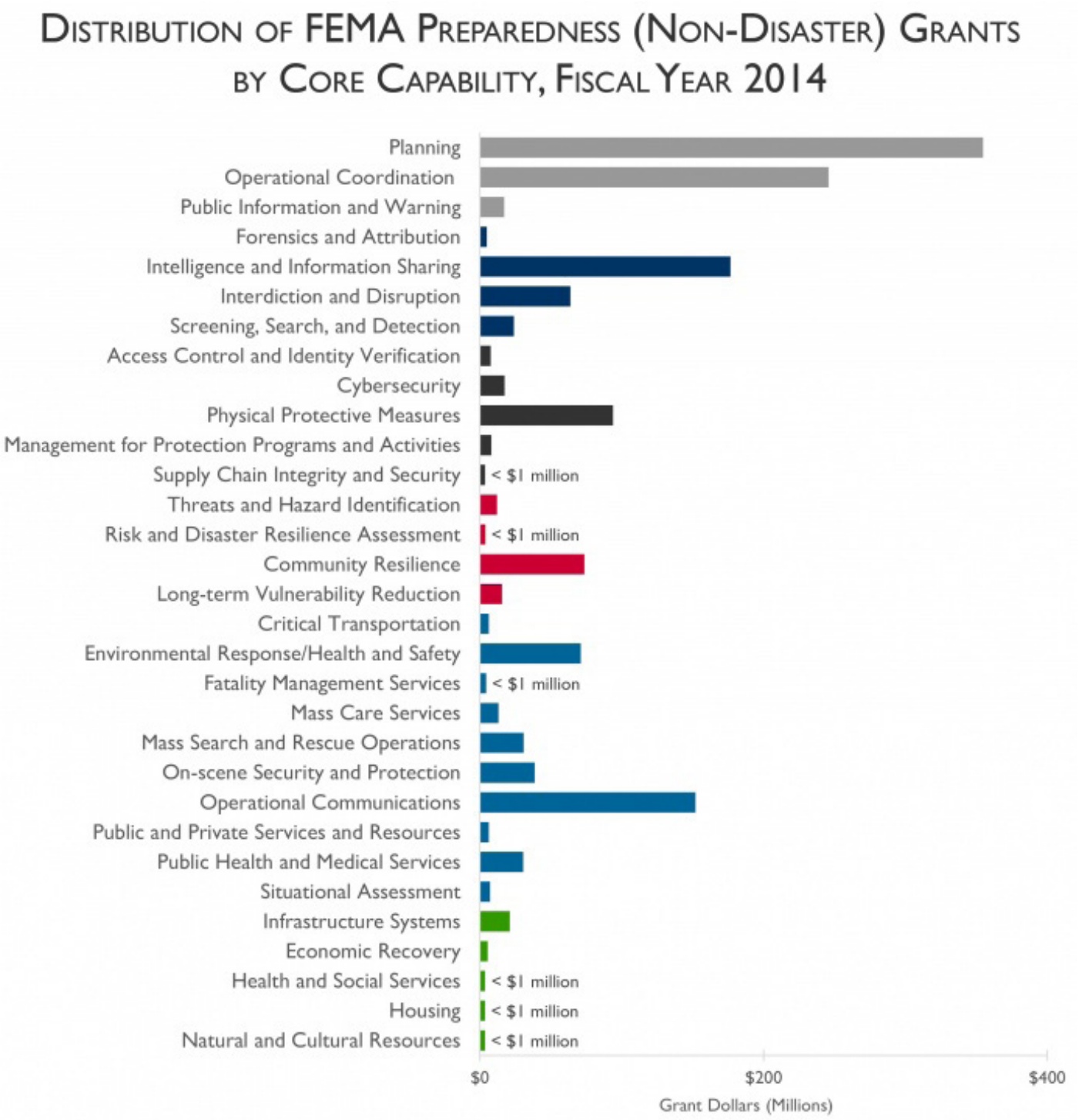

*Figure 3 Note, 2014 data does not include the newly added Fire Management and Suppression capability. In order, funding above depicts the three common core capabilities, followed by Prevention, Protection, Mitigation, Response, and Recovery. Source, "2016 National Preparedness Report," **DHS**, March 30, 2016, pg. 16.*

Finally, while some Core Capabilities are affected by a wide variety of tactics, the inverse may also be useful knowledge for practitioners: some tactics touch on a wide variety of Core Capabilities. These tactics are particularly multidimensional, and their complex character could require specific consideration. Based on our mapping, the three tactics likely to affect the greatest number of Core Capabilities are the use of IEDs, the use of theatrical brutality, and the use of waterways (see Figure 4 below).

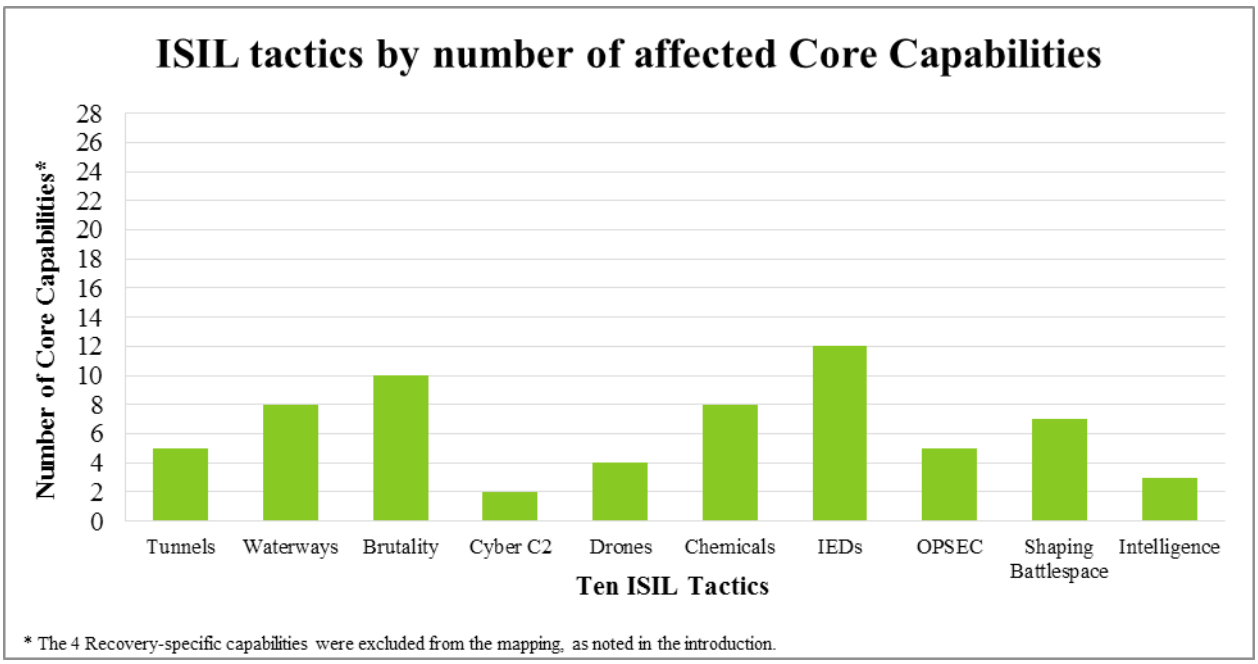

Figure 4: Of the ten ISIL tactics identified in this paper, IEDs maps to the widest number of Core Capabilities, followed by the innovative use of theatrical brutality and waterways.

For those tactics that are particularly complex, countering specific tactics could prove effective at thwarting a known adversary. Understanding specific threats is also important for ensuring that programmatic decisions taking place underneath the broader heading of Core Capabilities are informed by evolving threats and hazards. This could be particularly useful in dealing with a tactic like theatrical brutality, which presents an amorphous challenge that may not fall discretely into existing programs. Using tactics as the sole basis for decision-making is not, however, ultimately a substitute for Core Capabilities. Preparing for individual tactics alone results in less transferable skills for first responders. While the tactics identified may be specific to ISIL, the National Preparedness Goal and the system that supports it is designed to improve the capacity of first responders and emergency managers to staff, train, and equip for all contingencies.

Recommendations

For those jurisdictions that regard an ISIL-directed attack as an issue of high priority, our mapping suggests a two-fold response. First, jurisdictions should assess their level of proficiency and resourcing (which may not just be funding, but also equipment and personnel) across the Core Capabilities that were identified as affected by ISIL's tactics. To prioritize decision-making, our ranking suggests that jurisdictions pay close attention to Interdiction and Disruption; Physical Protective Measures; and On-scene Security, Protection, and Law Enforcement, which are affected by the greatest variety of threats. Given the state and territory proficiency data noted above, jurisdictions should pay particular attention to their level of proficiency for

Interdiction and Disruption and Physical Protective Measures.

Providing funding recommendations is more complicated, since all three of these capabilities are in the top half of grant funding allocated by FEMA. However, it is possible that additional resourcing (along with training and exercises) could bolster proficiency among states and territories in the capabilities of Interdiction and Disruption and Physical Protective Measures. For all three of the top Core Capabilities discussed above, a majority of states and territories regard improving proficiency in these capabilities as entirely or mostly a state responsibility, suggesting that non-federal jurisdictions have an important role to play in augmenting these capabilities.[56]

Second, our mapping suggests that practitioners also assess how their existing programs and activities across all relevant Core Capabilities meet the unique dimensions of the ten ISIL threats discussed above. In particular, we recommend that jurisdictions consider how existing plans, programs, training, and exercises wrestle with waterborne threats, the creative application of improvised explosives, and the psychological component of brutally constructed attacks. These threats are complex and multidimensional, mapping to a wide variety of capabilities across Mission Areas. Without considering specific tactics, practitioners run the risk of misaligning programs and hazards, even if the broader Core Capabilities exhibit suitable proficiency. With an organization as adaptive and tactically adept as ISIL, emergency managers and homeland security professionals must continuously strive to connect emerging threats to the framework in place to combat them.

Acknowledgements

The authors would like to thank Dave Kaufman for initiating interest in the research topic and providing support throughout the development process. Thanks as well to Yee San Su, Erin Mohres, Jonathan Schroden, and Andrea Wiltse for providing valuable feedback, and to the CNA Strategic Studies team who authored the original report on which this paper is based.

About the authors:

Joshua Tallis, *Ph.D. is an analyst at CNA. He completed his Ph.D. in International Relations at the University of St Andrews' Centre for the Study of Terrorism and Political Violence.*

Ryan Bauer *is an analyst at CNA. Ryan holds a Master's degree in Security Studies from Georgetown University's Edmund A. Walsh School of Foreign Service.*

Lauren Frey *is an analyst at CNA. Lauren holds a Master's degree in International Human Rights from the Josef Korbel School of International Studies at the University of Denver.*

Notes

[1] "National Preparedness Goal – Second Edition," *Federal Emergency Management Agency*, September 2015, pg. 3.

[2] Margaret Coker, "How Islamic State's win in Ramadi reveals new weapons, tactical sophistication, and prowess," *Wall Street Journal*, May 25, 2015, http://www.wsj.com/articles/islamic-states-gains-reveal-new-prowess-on-battlefield-1432592298.

[3] Isabel Coles and Peter Apps, "As Islamic State fighters begin to blend in, defeating them no easy matter," *Reuters*, August 31, 2014, http://www.reuters.com/article/2014/09/01/us-iraq-islamicstate-insight-idUSKBN0GV0P620140901.

[4] Kim Zetter, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits," *Wired,* November 19, 2015, http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/.

[5] Rukmini Callimachi, Alissa J. Rubin, Laure Fourquet, "A View of ISIS's Evolution in New Details of Paris Attacks," *New York Times*, March, 19 2016, http://www.nytimes.com/2016/03/20/world/europe/a-view-of-isiss-evolution-in-new-details-of-paris-attacks.html?_r=1.

[6] Isabel Coles and Ned Parker, "How Saddam's men help Islamic State rule," *Reuters*, December 11, 2015, http://www.reuters.com/investigates/special-report/mideast-crisis-iraq-islamicstate/.

[7] Richard Barrett, *The Islamic State* (New York: The Soufan Group, November 2014), http://soufangroup.com/wp-content/uploads/2014/10/TSG-The-Islamic-State-Nov14.pdf. Christopher Reuter, "The Terror Strategist: Secret Files Revealed the Structure of Islamic State," *Spiegel Online International*, April 18, 2015, http://www.spiegel.de/international/world/islamic-state-files-show-structure-of-islamist-terror-group-a-1029274.html.

[8] Anbar Daily, entry from July 10, 2015, http://anbardaily.blogspot.com/. "Islamic State fighters attack troops in Iraq's Anbar province," *Reuters*, July 10, 2015, http://www.reuters.com/article/2015/07/10/us-mideast-crisis-iraq-fighting-idUSKCN0PK1UP20150710.

[9] Rukmini Callimachi, "How a Secretive Branch of ISIS Built a Global Network of Killers," *New York Times*, August 3, 2016, http://www.nytimes.com/2016/08/04/world/middleeast/isis-german-recruit-interview.html?ref=world&_r=1.

[10] Callimachi, "How a Secretive Branch of ISIS."

[11] Ibid.

[12] Coker, "How Islamic State's win in Ramadi."

[13] David Kilcullen, "How to Defeat Islamic State" *The Australian*, accessed September 20, 2016, http://www.theaustralian.com.au/news/special-features/ramadi-palmyra-show-west-needs-new-strategy-to-defeat-islamic-state/news-story/750aa9dfd6b568615c5c998344aaba93.

[14] Michael Georgy and Ahmed Rasheed, "Tunneling through triangle of death, Islamic State aims at Baghdad from south," *Reuters*, August 4, 2014, http://www.reuters.com/article/2014/08/04/us-iraq-security-south-insight-idUSKBN0G41CO20140804.

[15] Marcus Weisgerber, "ISIS Is Using Tunnel Bombs in Iraq," *Defense One*, June 8, 2015, http://www.defenseone.com/threats/2015/06/isis-using-tunnel-bombs-iraq/114730/.

[16] Ibid. Jamie Dettmer, "Tunnel Bombs Highlight Savagery of Aleppo Fight," *VOA News*, March 5, 2015, http://www.voanews.com/content/tunel-bombs-highlight-savagery-in-fight-in-alepo/2668562.html.

[17] Ryan Lucas, "In battle for Kobani, Syria's Kurds hold out against ISIS militants," *CTV News*, October 12, 2014, http://www.ctvnews.ca/world/in-battle-for-kobani-syria-s-kurds-hold-out-against-isis-militants-1.2050909.

[18] Eyal Weizman, "The Art of War," Frieze 99, (May, 2006), https://frieze.com/article/art-war.

[19]Peter Clifford, "Kobane/Cizire Update 81: Islamic State Send Suicide Missions Across Euphrates In Vain Attempt To Distract Ypg/Fsa From Attack On Sarrin," accessed September 20, 2016, https://altahrir.wordpress.com/2015/04/24/kobanecizire-update-81-islamic-state-send-suicide-missions-across-euphrates-in-vain-attempt-to-distract-ypgfsa-from-attack-on-sarrin/.

[20] Karzan Sabah Hawrami, "Islamic State Takes Advantage of Weather and Night," *Bas News*, January 11, 2015, http://www.basnews.com/index.php/so/news/111440.

[21] Mitchell Prothero, "In heaviest fighting since August, Kurds turn back Islamic State assault near Irbil." *McClatchy DC*, January 11, 2015, http://www.mcclatchydc.com/news/nation-world/world/article24778276.html.

[22] Ibid.

[23] Ahmed Jadallah, "Islamic State launched gunboat attack on riverside town," *Reuters*, September 8, 2014, http://www.reuters.com/article/2014/09/08/us-iraq-crisis-attacks-idUSKBN0H30NU20140908.

[24] Riyadh Mohammed, "The Taking of Ramadi: Behind ISIS's Bloody Assault," *Fiscal Times*, May 21 2015, http://www.thefiscaltimes.com/2015/05/21/Taking-Ramadi-Behind-ISISs-Bloody-Assault.

[25] Clifford, "Kobane/Cizire Update."

[26] Lee Feeran, "Why Control of a Terrifying Dam in Iraq Is Life or Death for Half Million People," *ABC News*, August 7, 2014, http://abcnews.go.com/Blotter/mosul-dam-control-terrifying-dam-iraq-life-death/story?id=24878057.

[27] Clifford, "Kobane/Cizire Update."

[28] "Central gov't claims to destroy ISIS bomb boats," *Rudaw*, June 3 2015, http://rudaw.net/english/middleeast/iraq/030620154.

[29] Theodore Bell and Patrick Martin, "Iraq Situation Report: June 2-3, 2015," *Institute for the Study of War*, accessed September 20, 2016, http://www.understandingwar.org/sites/default/files/iraq%20SITREP%202015-6-03.pdf.

[30] Robert M. Danin, "What ISIS Hoped to Gain From Killing the Jordanian Pilot," *Newsweek*, February 4, 2015, http://www.newsweek.com/what-isis-hoped-gain-killing-jordanian-pilot-304336.

[31] Marc Santora, "From False Alarm to Panic: Inside Kennedy Airport's Chaotic Night," *New York Times*, August 15, 2016, http://www.nytimes.com/2016/08/16/nyregion/from-false-alarm-to-panic-inside-kennedy-airports-chaotic-night.html?emc=edit_th_20160816&nl=todaysheadlines&nlid=58153314.

[32] Ibid.

[33] Robert Hannigan, "The web is a terrorist's command-and-control network of choice," *Financial Times*, November 3, 2014, http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz42yzuCGo7. W.J. Hennigan, "Pentagon wages cyberwar against Islamic State," *Los Angeles Times*, February 29, 2016, http://www.latimes.com/nation/la-fg-isis-cyber-20160228-story.html.

[34] "Threat Tactics Report: Islamic State of Iraq and the Levant," *Complex Operational Environment and Threat Integration Directorate*, November 2014, https://info.publicintelligence.net/USArmy-TRISA-ISIL.pdf. J.M. Berger, "How ISIS Games Twitter," *Atlantic*, June 16, 2014, http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

[35] David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerilla* (London: C. Hurst & Co., 2013), 55.

[36] Hannigan, "The web is a terrorist's command-and-control."

[37] Ruth Sherlock, "ISIS jihadists use slick drone video to turn deadly battle for Kobane into computer game," *National Post*, December 12, 2014, http://news.nationalpost.com/news/world/israel-middle-east/isis-jihadists-use-slick-drone-video-to-turn-deadly-battle-for-kobane-into-computer-game.

[38] Ibid.

[39] Yasmin Tadjdeh, "ISIS Used A Miniature Surveillance Drone In Its Biggest Syria Victory Yet," *Business Insider*, August 29, 2014, http://www.businessinsider.co.id/isis-has-demonstrated-drone-capabilities-2014-8/#.V35LBdIrJhF#2ds1DFPJbgDvjbt4.97.

[40] Caleb Weiss, "Islamic State uses drones to coordinate fighting in Baiji," *The Long War Journal*, April 17, 2015, http://www.longwarjournal.org/archives/2015/04/islamic-state-uses-drones-to-coordinate-fighting-in-baiji.php.

[41] Aaron Mehta, "General: ISIL Using IEDs as Guided Munitions," *Defense News*, June 19, 2015, http://www.defensenews.com/story/defense/land/weapons/2015/06/19/isis-isil-ied-iraq-syria-coalition-pgm-suicide-truck-bomb/28984469/. Justin Fishel, "Fall of Ramadi: 30 Car Bombs, 10 as Big as Oklahoma City Blast, US Official Says," *ABC News*, May 20, 2015, http://abcnews.go.com/ABCNews/fall-ramadi-30-car-bombs-10-big-oklahoma/story?id=31188102.

[42] Coker, "How Islamic State's win in Ramadi."

[43] "Booby-traps halt Iraqi forces' advance on Tikrit," *Al Jazeera*, March 30, 2015, http://www.aljazeera.com/news/2015/03/iraqi-advance-moves-slowly-isil-held-tikrit-150329204048741. "Iraq Situation Report: October 6–15, 2015," *The Institute for the Study of War*, October 15, 2015, http://www.understandingwar.org/sites/default/files/iraq%20SITREP%202015-10-15.pdf.

[44] Damien McElroy, "Isis storms Saddam-era chemical weapons complex in Iraq," *The Telegraph*, June 19, 2014, http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/10913275/Isis-storms-Saddam-era-chemical-weapons-complex-in-Iraq.html.

[45] C. J. Chivers, "ISIS Has Fired Chemical Mortar Shells, Evidence Indicates," *New York Times*, July 17, 2015, http://www.nytimes.com/2015/07/18/world/middleeast/islamic-state-isis-chemical-weapons-iraq-syria.html?_r=1. C. J. Chivers and Eric Schmitt, "Islamic State Ordnance Shows Traces of Chemical Agents, U.S. Says," *New York Times*, September 11, 2015, http://www.nytimes.com/2015/09/12/world/middleeast/ordnance-used-by-isis-shows-traces-of-chemical-agents.html?_r=0.

[46] Ibid. Ibid.

[47] Sarah Berger, " What Is ISIS' Chemical Weapons Stockpile? Islamic State Group Has Recruited Experts From Across the World To Build Terror Arsenal," *International Business Times*, November 19, 2015, http://www.ibtimes.com/what-isis-chemical-weapons-stockpile-islamic-state-group-has-recruited-experts-across-2192871. Hamza Hendawi, Qassim Abdul-Zahra and Ken Dilanian, "Officials: IS determined to produce chemical weapons," November 19, 2015, http://bigstory.ap.org/article/b6c721d1beb34b989bf46aa101cf361a/iraqi-us-officials-working-produce-chemical-weapons.

[48] "FEMA Core Capabilities," *Federal Emergency Management Agency*, accessed September 20, 2016, https://www.fema.gov/core-capabilities.

[49] "FEMA Core Capabilities."

[50] Ibid.

[51] "2016 National Preparedness Report," *Department of Homeland Security*, March 30, 2016, 23.

[52] Ibid.

[53] Ibid., 16.

[54] Ibid.

[55] Ibid.

[56] Ibid., 24.