COMBATING TERRORISM CENTER
at West Point

THE ISLAMIC STATE AND DRONES

SUPPLY, SCALE, AND FUTURE THREATS

Don Rassler

July 2018

The Islamic State and Drones:
Supply, Scale, and Future Threats

Don Rassler

Combating Terrorism Center at West Point

United States Military Academy

www.ctc.usma.edu

July 2018

CONTACT

Combating Terrorism Center

U.S. Military Academy

607 Cullum Road, Lincoln Hall

West Point, NY 10996

Phone: (845) 938-8495

Web: www.ctc.usma.edu

ACKNOWLEDGMENTS

The author would like to thank CTC's former director, LTC(R) Bryan Price, and CTC's new director, Brian Dodwell, for their support for this effort. The critical and great feedback the author received from Daniel Milton, Alex Gallo, and Erik Skare was also most appreciated and helped to strengthen the final product. The author would also like to thank Muhammad al-`Ubaydi, Seamus Hughes, Rafaello Pantucci, and Damien Spleeters for their advice and for the helpful information they shared. The detailed copyediting support provided by Kristina Hummel and the graphic design support provided by Larisa Baste were also top-notch and helped to make this product more accurate and accessible.

Don Rassler

TABLE OF CONTENTS

List of Tables

List of Figures

Executive Summary

"[The] most daunting problem [of 2016] was an adaptive enemy who, for a time, enjoyed tactical superiority in the airspace under our conventional air superiority in the form of commercially available drones and fuel-expedient weapons systems, and our only available response was small arms fire."

—General Raymond A. Thomas III, May 2017[1]

The Islamic State is a group known for doing things a bit differently, for its capacity for innovation, and for its many 'firsts.' Two of those 'firsts' happened within months of each other. The first occurred in October 2016 when the group used a bomb-laden drone to kill, after the explosive hidden within the drone killed two Kurdish peshmerga soldiers who were investigating the device. Another 'first' happened in January 2017 when the Islamic State released a propaganda video that showed nearly a dozen examples of the group releasing munitions on its enemies from the air with a fair degree of accuracy via quadcopter drones it had modified. And it wasn't long before the group's bomb-drop capable drones would go on to kill, too.

After reaching a high point in the spring of 2017, the scale of the Islamic State drone threat—like many other dimensions of the group and its power—has already been significantly degraded. A surprisingly little amount of analytical attention, however, has been given to how the Islamic State was able to pull off its drone feats and bring its program to scale in a relatively short amount of time.

This report seeks to address this gap by evaluating the main factors that helped the Islamic State to effectively use modified commercial drones as weapons. It also highlights some of the broader threat and policy implications associated with the Islamic State's pioneering use of drones.

The following is a summary of this report's key findings:

The Islamic State's Drone Program—Making Sense of Simplicity, Supply, and Scale

- The Islamic State was able to innovate and surprise its enemies from the air by taking a relatively simple approach that creatively merged sophisticated commercial off-the-shelf technology with low-tech components and other technological add-ons. This cobbling together of high- and low-tech systems, and the small and easy-to-replicate enhancements that the Islamic State made helped to transform off-the-shelf drone products into unique and fairly capable weapons.
- The Islamic State's high-tech/low-tech approach was underpinned and facilitated by the group's ability to acquire commercial quadcopter drones and related components that were used for defensive and offensive purposes through a global and layered supply chain that involved purchases from at least 16 different companies that were based in at least seven different countries.
- Once the Islamic State had a sizable number of commercial drones in hand, which were likely supplied by multiple supply chain networks, the group's centralized and bureaucratized approach to manufacturing provided the framework needed to bring the group's drone program to scale.

The Bangladesh Factor

- While there is still a lot to learn about the Islamic State's drone program, the program appears to have been shaped by two Bangladeshi brothers who leveraged companies in the United Kingdom, Bangladesh, and Spain that they established to move funds, drones, and other dual-use components to and on behalf of the Islamic State. At least one of these brothers also played a central role in helping to create and develop Dawlatul Islam Bengal, the Islamic State's local affiliate in Bangladesh.[2]

1 David Larter, "SOCOM Commander: Armed ISIS Drones Were 2016's 'Most Daunting Problem,'" Defense News, May 16, 2017.

2 Tasneem Khalil, "Meet the ameer of ISIS in Bangladesh," People, Power, States Blog, August 4, 2017.

Future Threats & Other Implications

- The Islamic State's drone program is an important case study that highlights how the group overcame technical and cost asymmetries, and developed a novel weapons system constructed from commercial components that challenged—at least for a period of time—states' ability to respond.
- Given the Islamic State's penchant for innovation, it would be a mistake to underestimate the organization and how the group could serve as an inspiration for other terrorists and/or nation-states and proxy groups that are developing their own hybrid warfare strategies.
- As a result of these dynamics, as we look to the future, we should expect:
    1. Drones similar to the Islamic State's bomb-drop capable ones to be used in different theaters and by different types of groups
    2. The use of different drone tactics, drone targets, and drone weapons
    3. More drones to be used: not just one drone, but multiple, and land and sea drones, too
- Existing drone countermeasure gaps and seams make this issue even more poignant.
- The details highlighted in this report also speak to an emerging, seemingly apparent truth: how the 'rise' of hybrid warfare, a current of which emphasizes the combination of low-cost equipment that can be used at scale with more costly systems or forms of technology, will likely require the development of new, hybrid public-private sector approaches to effectively manage, track, and degrade future hybrid threats that leverage and/or are based off of commercial systems.
- Important supply chain gaps of knowledge likely still exist, as the firms used to procure commercial drone, rocket, and counter-surveillance equipment reviewed in this report were different from the firms used to purchase nine Islamic State quadcopter drones that were recovered in the field and retraced by a major, professional weapons-tracking non-governmental organization.
- To help close these gaps, more attention and resources should be spent on efforts that aim to prevent the delivery of select dual use items to major conflict zone areas, to investigate and map out supply chain networks, and to retrace specific equipment after it has been found in the field.

Introduction

"There was a day [in early 2017] when the Iraqi effort nearly came to a screeching halt, where literally over 24 hours there were 70 drones in the air … At one point there were 12 'killer bees,' if you will, right overhead and underneath our air superiority … and our only available response [at the time] was small arms fire."

—General Raymond A. Thomas III, May 2017[3]

Although the 'killer bees' that the Islamic State used to wreak havoc across Iraq and Syria during 2016-2017 were small in size, the impact of the group's deployment of a fleet of commercial drones it had weaponized was large and extends beyond the group. The nature of the Islamic State's offensive drone capabilities was taken so seriously that in 2016, General Thomas—the commander of U.S. Special Operations Command—identified the issue as that year's "most daunting threat."[4] Such a remark is noteworthy, especially when one considers that General Thomas leads an enterprise of nearly 70,000 personnel[5] that is responsible for responding militarily to a wide range of state and non-state security challenges.[6]

The significance of the Islamic State's creatively engineered drone fleet can also be measured by the effect it has had on the battlefield. While the impact of the Islamic State's 'killer bee' drones was not that long-lasting and did not result in a large number of deaths, the group was still able—after making a number of simple and minor modifications to stock commercial quadcopter drone platforms that are widely available to the public—to challenge the United States' air superiority tactically in a major combat zone for a defined period of time, a dynamic the United States' other state and non-state actor adversaries almost surely noticed. Second, the Islamic State identified a key security gap and asymmetrically exploited it through cheap and creative means, all while the United States and other state actors are spending millions of dollars to develop and deploy a range of drone countermeasure solutions to mitigate this specific threat.

A lot has changed for the Islamic State over the last year, and more challenges lie ahead for the group, but it would be a mistake to underestimate both the organization and how the group—and its legacy of innovations—could serve as an inspiration or model for other types of actors, to include nation-states or proxy groups that are developing their own hybrid warfare or asymmetric capabilities and strategies. An important case study in this regard is the Islamic State's do-it-yourself drone program, as instead of the group's drone innovations being 'down and out,' the enterprising drone tactics developed by the Islamic State are likely 'up and here to stay.' Such a statement is not meant to imply that the size or scale of the Islamic State drone threat will not change or that it has not changed already (the scale of the Islamic State drone threat has already been reduced), but rather that the drone methods and approach taken by the Islamic State provide a roadmap for state and non-state actors alike to emulate, to learn from, or—perhaps more importantly—to take in new directions.

To evaluate the staying power of the Islamic State drone threat and the implications associated with what other violent actors might have learned from the group's activity, it is helpful to understand how the Islamic State developed its drone program and what has made the group's program unique. This report evaluates three key factors that have defined the Islamic State's approach to creating and deploying a fleet of drones. These three factors, each of which has a bearing on the future of the drone threat, include the relative simplicity of the Islamic State's drones and drone-related tactics, which creatively blended different types of 'high' and 'low' end technologies; the global and layered nature

3 Larter.

4 Ibid.

5 "2018 Fact Book: United States Special Operations Command," USSOCOM Communication Office, 2018, p. 12.

6 For more on U.S. Special Operations Command's mission and authorities, see Ibid., p. 14.

of the Islamic State's supply chain; and the scale of the group's drone operations.

This report proceeds in three sections. A high-level overview of the Islamic State's simple tactical and operational drone innovations is provided first. That section is followed by a discussion that explores how the Islamic State sourced and manufactured its drones, and how the group was able to bring its drone program to scale—and to do so in a relatively short period of time. The third section evaluates the drone-counter-drone competition that is taking place between non-state actors like the Islamic State and nation-states and how it can inform our understanding of where future iterations of the terror drone threat might be headed so they can be either anticipated or mitigated.

Keep It Simple, Stupid! The Islamic State's Tactical and Operational Drone Innovations

The significance of the Islamic State's drone program lies less in its technical sophistication and more in the collection of simple, low-cost, and replaceable devices that made up the group's drone fleet as well as the group's use of those drones in a number of creative ways. Islamic State planners knew that the technical capabilities and financial resources of the United States and its other state adversaries in Iraq and Syria outmatched the group's own. But these same planners also likely recognized the surveillance, propaganda, and operational benefits of fielding commercial and homemade drones, including their potential to enhance the group's ability to surprise. So to develop its own drone capabilities, the Islamic State kept things simple and took some creative short cuts. Because the group and its actions were under a considerable amount of international pressure, the Islamic State built its own homemade drone platforms and privileged the acquisition and deployment of relatively low-cost commercial, quadcopter drones, and fixed-wing drone platforms, which are widely available in various countries around the globe.[7] These drones have been used by the Islamic State for different purposes, including surveillance and reconnaissance missions, for media productions, and as a platform to attack enemies.[8]

Many of the commercial drones that the group acquired were then creatively modified through the cobbling together of cheap, easily acquired add-on components that allowed the group to moderately enhance the capabilities of those drones. These simple enhancements transformed stock, quadcopter drones into devices that were capable of dropping small, and in some cases lethal, explosive munitions from the air.[9] To facilitate this new, bomb-dropping capability, the group attached plastic tubes and simple release mechanisms driven by a small servo motor to quadcopter drones (see Figure 1).[10]

7 For background on the variety of drones used by the Islamic State, as well as other actors in Syria and Iraq, see Dan Gettinger, *Drones Operating in Syria and Iraq* (New York: Center for the Study of the Drone, 2016) and Ben Watson, "The Drones of ISIS," Defense One, January 12, 2017.

8 For background, see Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones, and Supportive Technology* (West Point, NY: Combating Terrorism Center, 2016) and Don Rassler, Muhammad al-`Ubaydi, and Vera Mironova, "The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft," Combating Terrorism Center, January 31, 2017.

9 For visual examples, see "The Knights of the Dawawin," Wilayat Ninawa Media Office, January 24, 2017.

10 See Mitch Utterback, "How ISIS is Turning Commercial Drones into Weapons in the Battle for Mosul," Fox News, January 25, 2017, and Nick Waters, "Types of Islamic State Drone Bombs and Where to Find Them," Bellingcat, May 24, 2017.

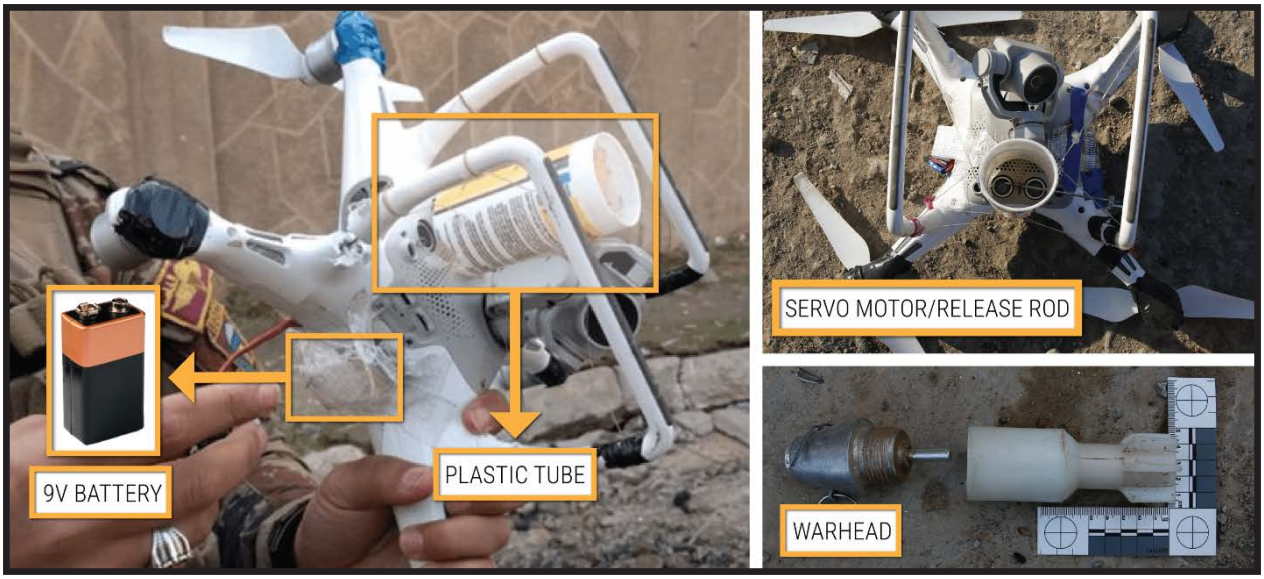


Figure 1: Commercial Drone Modified for Projectile Drop Capability by Islamic State Operatives (Photo credits: Plastic Tube (Mitch Utterback); Servo Motor, Release Rod (Conflict Armament Research); Warhead (Conflict Armament Research))

This drone bomb-drop mechanism was cheap and easy to replicate, and has been described as something a "sophisticated high schooler could put together."[11] The innovative approach that the Islamic State took was also driven by the need to be resourceful and make things work with materials group members had on hand. For example, the Islamic State's bomb capable drones used a "wide range of warheads and tails," from 40mm warheads and grenades to tails constructed of plastic, metal, wood, and other materials.[12] This flexibility (born in part out of necessity) meant that when desired materials ran low, the Islamic State just used something else.

The group also devised a variety of simple drone tactics to enhance the effectiveness of other operations and weapons. This included using drones to direct vehicle-borne suicide bombers[13] and improve the accuracy of mortar and rocket fire so those weapons would detonate or land closer to their intended target.[14] The Islamic State's combined use of drones and suicide attackers, in what might be loosely described as a systems-based targeting approach, was a tactic that the group used during its defense of Mosul. During the fight for that city, Islamic State drone operators would "act as navigators for the suicide driver, guiding him" in real time "by radio or cell phone through battle worn streets."[15] To disrupt those types of operations, the coalition "attempted to blanket all of Mosul in a red no-fly zone for commercially purchased" drones.[16] But the Islamic State reportedly was able to get around the countermeasure by either making "smart software adjustments to the unit or by placing aluminum material over the [drone's] GPS."[17] Whether this type of rudimentary countermeasure was actually effective remains to be seen, but the do-it/solve-it-yourself approach is a key factor that has contributed

11 Rassler, al-`Ubaydi, and Mironova.

12 Waters, "Types of Islamic State Drone Bombs and Where to Find Them."

13 Susannah George and Lori Hinnant, "Islamic State Turns to Drones to Direct Suicide Car Bombers," Associated Press, February 1, 2017; Clay Dillow, "Islamic State Ups the Size and Sophistication of its Drone Fleet," *Fortune*, April 18, 2016.

14 Anthony Capaccio, "Extensive Islamic State Drone Use Raising Risks in Mosul Battle," Bloomberg, October 26, 2016; Michael D. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat from ISIS: Exploding Drones," *New York Times*, October 11, 2016.

15 Mike Mawhinney, "Islamic State Using Hobby Drones with Deadly Effect," Sky, April 4, 2017.

16 Ibid.

17 Ibid.

to the Islamic State's drone successes. And it is quite likely that the Islamic State's simple, resourceful, quick, and relatively low-cost approach to building out a significant drone capability will be copied by others.

Scale, Sourcing, and Manufacturing

The takeoff of the Islamic State's aerial drone bombing campaign happened quickly. After killing two Kurdish peshmerga soldiers with a bomb hidden in a drone in October 2016, the group deployed a large number of modified commercial quadcopters to drop small grenade and bomb-like munitions on unsuspecting forces in Iraq and Syria in a short span of time.[18] The speedy scale-up, broad deployment, and eventual impact of Islamic State bomb-capable drones was not the result of overnight success, but was likely instead the result of careful and deliberate planning that started at least a year prior.[19]

The "peak of the [Islamic State drone bomb] threat came … [in spring 2017] during the fight to wrest Mosul from Islamic State control in northern Iraq."[20] Around that time, the Islamic State was conducting between 60 and more than 100 aerial drone bombing attacks per month, spread across both Iraq and Syria.[21] It appears as though the Islamic State was able to maintain that pace of operations until at least June when a Syrian Defense Force soldier interviewed by French journalists operating near Raqqa, Syria, noted how "two to three drones rotate everyday here. They target our logistic lines and our ammunition depots. So far this morning, we have been bombed three times. By the end of the day, they will have targeted us 15 to 16 times. They do this every day."[22] By the end of September, the number of reported Islamic State drone sightings, however, was down to seven for that month, a noticeable decline.[23]

The significance of the Islamic State's bomb-drop capable drones should also be measured by their psychological impact. Videos released by the Islamic State show the group dropping munitions from the air with a fair, and surprising, degree of accuracy—such as being able to successfully drop small drone-bombs on tanks, vehicles, and people. These videos, which are carefully edited pieces of propaganda, should certainly be taken with a grain of salt. Yet, other data points speak to the terror that the group was able to inflict through the use of its simple drone systems. For example, a resident of Mosul had the following to say in February 2017 about the group's drone operations: "You can't leave the house without checking the sky every single second and, even if you hear one of the drones, you don't have time to run away because they are so fast."[24] Drones deployed by the Islamic State have also been lethal; according to military officials, it is believed that the group's drone-bomb attacks killed

18 Kurdish peshmerga forces claim that a similar IED drone attempt was made in December 2015. See Rassler, *Remotely Piloted Innovation*, p. 37.

19 This is reflected in the Islamic State drone use reports recovered by Iraqi forces in Mosul, which were filled in by Islamic State fighters during 2015. The forms show very clearly a calculating and long thought-out process regarding the training of pilots and the variety of missions that they would undertake. For example, one form had a series of boxes for operatives to check to provide details about their mission. Two of those boxes were "explosive plane" and "bombing." For background, see Rassler, al-`Ubaydi, and Mironova. See also Dillow.

20 Eric Schmitt, "Pentagon Tests Lasers and Nets to Combat a Vexing Foe: ISIS Drones," *New York Times*, September 23, 2017.

21 For background, see Ben Sullivan, "The Islamic State Conducted Hundreds of Drone Strikes in Less Than a Month," MotherboardVICE, February 21, 2017, and Nick Waters, "Death from Above: The Drone Bombs of the Caliphate," Bellingcat, February 10, 2017. Prior to that, in January 2017, a representatives of the U.S. coalition said that in January they were observing approximately one Islamic State drone per day. See Watson.

22 "Exclusive: IS group's armoured drones attack from the skies in battle for Raqqa," France24, June 26, 2017.

23 W.J. Hennigan, "Islamic State's deadly drone operation is faltering, but U.S. commanders see broader danger ahead," *Los Angeles Times*, September 28, 2017.

24 Tom Westcott, "Death from Above: IS Drones Strike Terror in 'Safe' Areas of Mosul," Middle East Eye, February 22, 2017. See also Ben Kesling and Ghassan Adnan, "Islamic State Drones Terrorize Iraqi Forces as Mosul Battle Rages," *Wall Street Journal*, February 26, 2017.

more than a dozen people across time.[25] The Islamic State's drone-bombs have also injured dozens more as a result of the shrapnel they produce. In February 2017, a surgeon in Mosul estimated that his hospital was "receiving at least 10 patients every day injured by these drone attacks."[26]

A number of factors helped the Islamic State bring their drone program to scale. The Islamic State's takeover and control of large swaths of territory, as well as key cities and military facilities, for an extended period of time in Syria and Iraq was certainly a critical enabling factor. These gains provided the group with physical space and access to factories, manufacturing equipment, explosives, and other weapons, which the Islamic State could plunder and use for its own gains—and do so in a cheaper, more cost-effective way. These gains were bolstered by the Islamic State's procurement of commercial drones and drone-related components. Other factors that greatly contributed to the scale of the Islamic State's drone program lie in the group's simple and creative engineering approach and its use of the various materiel and inputs it acquired.

To better see how the Islamic State may have approached the production of its drone fleet, consider the example of its approach to other types of weapons. The Islamic State went to great lengths to standardize and industrialize the manufacture of weapons like rockets and mortars so those weapons could be developed with more precision and on a larger scale.[27] In December 2016, field investigations of Islamic State manufacturing facilities in Mosul led the independent weapons monitoring group Conflict Armament Research (CAR) to conclude that "the degree of organization, quality control, and inventory management, indicates a complex, centrally controlled industrial production system."[28] CAR went on to add that:

> "In this system, multiple manufacturing facilities work to produce weapons according to precise technical guidelines issued by a central authority. The production of any one weapon system involves the coordinated input of numerous facilities at different stages of the production cycle: from the processing of raw materials, to the mixing of chemical explosive precursors, to machining, assembly, and final sign-off by dedicated quality control personnel.
>
> To function, this production line requires a sophisticated monitoring system, in which manufacturing facilities regularly report detailed figures on production rates and the quality of output to a central procurement and production authority—all of which are critical to forecasting material requirements and to ensuring that all manufactured weapons conform to standard specifications."[29]

Islamic State documents found by Iraqi forces in Mosul demonstrate how the group took a similar approach, and tried to both standardize the operation of and institutionalize data about its drone program. One four-page Islamic State form, which was produced by a brigade subordinate to the group's Committee of Military Manufacturing and Development, contained pre-and post-flight drone checklists and areas to record after-action comments and mark which type of mission had been conducted.[30] Two of these types of forms, each with data entered about separate drone operations conducted in Iraq's Nineveh and Saladin governorates, were found in the small collection of Islamic State drone files that were recovered.[31] These two documents demonstrate how the group was trying to manage drone activity bureaucratically across different geographic areas in Iraq. Field reports published by

25 Schmitt.

26 Westcott.

27 For background, see "Standardisation and Quality Control in Islamic State's Military Production," Conflict Armament Research, December 2016.

28 Ibid., p. 4.

29 Ibid., p. 5.

30 Rassler, al-`Ubaydi, and Mironova.

31 Ibid.

journalists and photos published online also show how the Islamic State operated both larger and smaller drone manufacturing/development facilities with varying levels of sophistication.[32]

But standardized and quality-controlled manufacturing is only one major part of the scale equation, as "consistency in production also requires consistency in the supply of materials."[33] To maintain a steady supply of drones, the Islamic State has acquired a sizable number of commercially produced drones and manufactured its own homemade variants. When it comes to the manufacture of its own drones, the Islamic State appears to have been primarily occupied with the development of fixed-wing drone platforms, which have either been assembled out of wood or from stock fixed-wing airframes that the group has acquired.[34] Even though fixed-wing platforms cannot hover, they typically can fly farther from their controller than quadcopter variants, a feature that likely makes fixed-wing drones attractive for longer-range surveillance and reconnaissance and other operational missions.[35]

At present, not much is publicly known about the Islamic State's drone supply chain and how the group acquired the sizable number of commercially available drones it used in Iraq and Syria. A number of data points, however, show how the Islamic State's drone supply chain shares some similarities observed in other areas of the group's supply chain framework. For example, an in-depth CAR study of Islamic State improvised explosive device (IEDs) components discovered in Iraq and Syria found that there were "50 commercial entities and 20 countries involved in the supply chain of components used by IS [Islamic State] forces to construct IEDs."[36] Despite the global makeup of certain aspects of the Islamic State's IED supply chain, the majority of the components used by the group appear to have been procured lawfully through third-party suppliers located in Iraq or other neighboring countries like Turkey. As noted by CAR, these "many small-scale commercial enterprises appear to have sold, whether wittingly or unwittingly, components to parties linked to, or employed by, IS forces."[37]

Two key sets of data demonstrate how the Islamic State acquired commercially available drones and related components through similar global and layered acquisition channels. The first set of data, which is derived from material revealed through a collection of Islamic State-linked terrorism cases and related arrests that took place in multiple countries over the 2014-2017 time period, provides insight into a key network of individuals and companies who purchased and distributed drone, rocket, and counter-surveillance equipment to the Islamic State in Iraq and Syria. This particular network is useful as it illuminates the purchaser side (i.e., the individuals and entities who initiated specific purchases) of the Islamic State's drone technology supply chain; the distribution, payment, and communication channels used; and how the group attempted to hide their purchasing and distribution activity. While the first set of data maps out aspects of the Islamic State's drone component supply chain from the initial point of sale, the second set of data starts from a completely different place: commercial drones used by the Islamic State, which were recovered by CAR field investigators in Iraq. Using these devices and their serial numbers as a starting point, CAR then worked backward to identify some of the vendors from which the Islamic State purchased its commercial drones.

32 For a view of smaller and what appear to be less sophisticated drone workshops, see Kelsey D. Atherton, "What we know about ISIS's scratch built drones," *Popular Science*, November 6, 2016; Nick Enoch, "Inside the ISIS drone factory: Seized Mosul warehouse reveals the jihadis' crude reconnaissance planes and deadly four-wheeled robot bombs," Daily Mail, June 30, 2017; and Rassler, al-`Ubaydi, and Mironova. For a view of a larger and what appears to be a more sophisticated facility, see Mathieu Morant, "ISIS "Air Force,'" Twitter, October 19, 2017.

33 "Standardisation and Quality Control in Islamic State's Military Production," p. 5.

34 For background on the Islamic State's manufacture of fixed wing platforms, see "Islamic State's Weaponised Drones," Conflict Armament Research, October 2016. For details on the Islamic State building fixed-wing drone platforms from stock, and commercially purchasable airframes, see Rassler, al-`Ubaydi, and Mironova.

35 For background on other, potential fixed-wing platform missions, see Rassler, al-`Ubaydi, and Mironova.

36 "Tracing the Supply of Components Used in Islamic State IEDs," Conflict Armament Research, 2016, p. 8.

37 Ibid., p. 7.

From Point of Purchase to the Islamic State in Syria and Iraq: The IBACS Conspiracy

A month after the Islamic State's November 2015 multi-pronged terrorist attack in Paris, the group suffered a series of setbacks that would impact to some degree the organization's ability to source commercial technology (including drone components), funnel money to the group in Iraq and Syria, and send operational funds to Islamic State supporters outside of the Levant. The disruption was rooted in a sequence of at least four counterterrorism events that happened in a coordinated fashion, in four countries, within hours or days of each other. The first setback involved Siful Haque Sujan, a Bangladeshi Islamic State operative who worked with Junaid Hussain and played an important role in the group's cyber recruitment and military development efforts, who was killed in Syria on December 10, 2015, in a drone strike conducted near the Islamic State's headquarters in Raqqa.[38] Sujan also played a pivotal role in helping to establish and develop Dawlatul Islam Bengal, the Islamic State's affiliate in Bangladesh.[39]

Before he joined the Islamic State, Sujan and his older brother Ataul Haque Sobuj incorporated and ran a number of IT, electronics, and web services businesses in the United Kingdom, Bangladesh, and Spain—entities which were used by the two brothers and their co-conspirators as front companies to move money and materiel to the Islamic State.[40] Five of the U.K.-registered companies were branded using variations of the same name (IBACS) and included IBACS Trade International LTD, IBACSTEL Electronics LTD, IBACS IT Solutions LTD, IBACS Technologies LTD, and IBACSTEL Corporation LTC.[41] The IBACS companies were headquartered in Wales, but IBACS also had a satellite office in Dhaka, Bangladesh (where Sobuj served as the managing director for a period), and reportedly another office in Jordan.[42] According to press reports, the IBACS enterprise—in addition to the countries already listed—also engaged in business activities in Denmark, Australia, and the United States.[43] As time went on, the brothers created and/or associated themselves with other legitimate businesses. For example, from July 2015 onward, Sujan began making purchases for the Islamic State using the cover of a company called Advance Technology Global LTD.[44] His brother Sobuj did the same thing except through ISYNKTEL, a company he had established in Spain.[45] WAHMI Technologies, another firm in Bangladesh that was also established by Sobuj, played a role in the conspiracy as well.[46]

Sujan's case is not the first time that a link between Bangladeshi operatives and the Islamic State's drone program has been established. The Islamic State drone files recovered in Mosul included the names of two Islamic State fighters of Bangladeshi origin, who were supporting the group's drone

38 Sujan and his brother both played important roles for the Islamic State's Technological Development Battalion. For background on Sujan, see "IS Computer Hacker Siful Haque Sujan Killed in Air Strike," BBC, December 31, 2015. For background on Junaid Hussain, see Nafees Hamid, "The British Hacker Who Became the Islamic State's Chief Terror Cyber Coach: A Profile of Junaid Hussain," *CTC Sentinel* 11:4 (2018).

39 For background, see Khalil.

40 U.S. v. Elshinawy, "Memorandum Opinion," March 28, 2018. For background on the establishment of the U.K. registered companies, see the records available via UK Companies House search query at https://beta.companieshouse.gov.uk/search?q=ibacs.

41 For details about these companies, see their registration and filing records available via the UK Companies House website: https://beta.companieshouse.gov.uk/company/07461096, https://beta.companieshouse.gov.uk/company/07346510, https://beta.companieshouse.gov.uk/company/07602488, https://beta.companieshouse.gov.uk/company/09692097, and https://beta.companieshouse.gov.uk/company/09638157.

42 Tipu Sultan, "Funds Went to ISIL From UK via Dhaka," *Prothom Alo* (in Bengali), January 20, 2016.

43 Ibid.

44 U.S. v. Elshinawy, "Govt. Exhibit 4 – Conspiracy – Sequence of Events." For background on the incorporation of Advance Tech Global, see https://beta.companieshouse.gov.uk/company/09699478.

45 Omar Faruk, "All Members of Same Family Involved in Militant Funding," *Kaler Kantho* (in Bengali), September 26, 2017; "BDT 7.8 Million Comes From Spain; Spent in Militant Activities," *Prothom Alo* (in Bengali), September 25, 2017.

46 Faruk, "All Members of Same Family Involved in Militant Funding."

operations. At the time, the presence of these two fighters seemed slightly odd as an analysis of 4,000 leaked Islamic State personnel records conducted by the Combating Terrorism Center showed how the number of Bangladeshi recruits joining the group was low compared to other countries.[47] The arrest of Sobuj and the Bangladesh-based network with which he was associated raises additional questions about the potentially disproportionate role Bangladeshis might be playing in the Islamic State's drone program.

Other data points, like Jenan Moussa's coverage of Tunisian Islamic State drone developer Fadhel Mensi,[48] the arrest of Fijian-Cambodian Islamic State operative Neil Prakash,[49] and the targeting of Junaid ur-Rehman,[50] show how the development and management of the Islamic State's drone program also involved inputs from individuals from around the world.[51] The Islamic State has also sought out and solicited technical input from engineers and scientists through specific Telegram channels as a way to remotely crowd-source expertise and solutions.[52]

A second and third sign of trouble were two major police actions that occurred in the United Kingdom and Bangladesh within days of Sujan's death. This included the arrest in the United Kingdom of Abdul Samad, a friend of Sujan and Sobuj, who served for a period as the director of two of the IBACS companies[53] and the arrest of at least five individuals who were associated with and/or helped to run the satellite IBACS office in Dhaka.[54] The latter included Sujan's "father Abul Hasanat, his younger brother Hasanul Haque … Saiful's brother-in-law and also director of the office Tazul Islam (Sakil) and its accountant Nahiddoza Mia."[55] These individuals were arrested, as authorities in Bangladesh believed they were using the various offices of IBACS, in partnership with Sujan and Sobuj, to move money on behalf of and funnel money to and from the Islamic State in the Levant.[56]

The fourth counterterrorism event took place in the United States the day after Sujan was killed in Syria. On that day, federal agents in the state of Maryland arrested Mohamed Elshinawy on terrorism charges. For a number of months prior to his arrest, Elshinawy (who was later convicted and sentenced to 20 years in prison) received more than $8,000 in funds from Sujan and Sobuj via PayPal to conduct a terrorist attack in the United States on behalf of the Islamic State.[57] Elshinawy was not the only person outside Syria and Iraq to which Sujan, Sobuj, and their other co-conspirators sent oper-

47 Brian Dodwell, Daniel Milton, and Don Rassler, *The Caliphate's Global Workforce: An Inside Look at the Islamic State's Foreign Fighter Paper Trail* (West Point, NY: Combating Terrorism Center, 2016).

48 For background, see Jenan Moussa, "3/ ISIS drone developer Fadhel Mensi describes in document group's plan: 'UAVs loaded w/ 20 kgs of explosives used as air to ground missile," Twitter, March 29, 2017.

49 Latika Bourke, "Islamic State's extensive use of drones a 'sign of desperation', says coalition spokesman," *Sydney Morning Herald*, March 1, 2017.

50 Schmitt.

51 For other perspectives on this issue, see Bridget Johnson, "American, British ISIS Jihadists Ran Reverse Engineering Op to Mimic Captured U.S. Drone Technology," PJ Media, July 27, 2017, and Asaad Almohammad and Anne Speckhard, "Islamic State and Drones: Evolution, Leadership, Bases, Operations, and Logistics – Analysis," Eurasia Review, May 8, 2017.

52 For example, see "ISIS Engineers And Scientists Collaborate On Projects In Telegram Channel," MEMRI Cyber & Jihad Lab, March 21, 2016.

53 The author would like to thank Raffaello Pantucci for assistance with the case of Abdul Samad. Samad was arrested in December 2015 and bailed until March 2016. For details, see "IS computer hacker killed in airstrike," BBC, December 31, 2015; Jamie Merrill, "Revealed: An FBI Probe, an IS plot, and a Welsh Firm Caught in the Fallout," Middle East Eye, August 19, 2017; and Omar Wahid, "Leader killed in US drone strike paid for British teenager to become a jihadi bride and laundered money for terror group," Daily Mail, January 2, 2016. For details on the roles he played at various IBACS companies, see https://beta.companieshouse.gov.uk/company/09692097/officers, https://beta.companieshouse.gov.uk/company/09638157/officers, https://beta.companieshouse.gov.uk/company/07602488/officers, and https://beta.companieshouse.gov.uk/company/07346510/officers.

54 Sultan; "iBacs used as funds centre for terror activities," *Daily Sun*, January 20, 2016.

55 Khalil; Sultan; Kamrul Hasan, "Brother of Slain IS IT Expert Finances Local Militants," Dhaka Tribune Online, January 8, 2016.

56 Nuruzzaman Labu, "Sadarghat 256: Bangladeshi-born IS Leader's Code for Militant Financing," Dhaka Tribune Online, August 23, 2017; Sultan; Hasan.

57 Seamus Hughes, "The Only Islamic State Funded Plot in the U.S.: The Curious Case of Mohamed Elshinawy," Lawfare, March 7, 2018.

ational funds. Several days before Sujan's death in December 2015, authorities in Bangladesh seized $50,000 that was sent from one of the IBACS companies via hawala cash transfer to a "close associate" of Tamim Ahmed Chowdhury—the "mastermind" of the July 2016 attack against the Holey Artisan Bakery, an incident that killed 24 people and was claimed by the Islamic State.[58] After reviewing the local activity of IBACS, investigators in Bangladesh also reportedly found "that iBacs ... [was being] used as a platform for financing terror ... in at least 10 countries."[59] And even though Elshinawy, a self-identified Islamic State supporter, did not acquire any drones or drone-related components,[60] the evidence introduced at his trial outlined the drone-related transactions that Sujan and Sobuj made during the 2014-2015 time period.

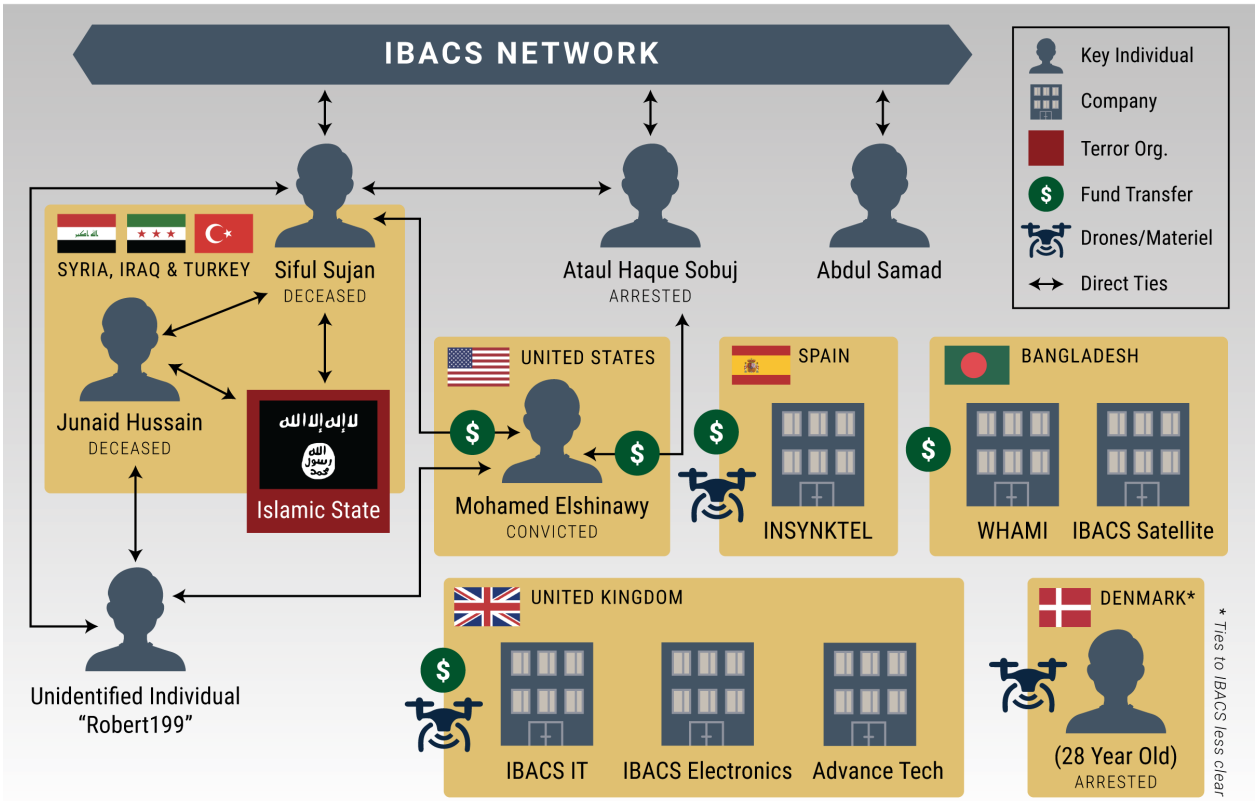


Figure 2: The IBACS Supply Network

The network's drone-related purchases, which were made by leveraging the cover of at least five different businesses headquartered in three countries, were driven by at least two main goals and appear to have occurred in two phases. Given the lack of publicly available data related to some purchases, it is not possible to discern whether those two phases were pursued separately or concurrently or if the network led by Sujan and Sobuj made additional drone-related purchases in support of other Islamic State goals.

58 Paritosh Bansal and Serajul Quadir, "New Evidence Shows Deep Islamic State Role in Bangladesh Massacre," Reuters, December 1, 2016. According to another press report, it appears that Sujan might have also tried to send money to Chowdhury through his father and younger brother. See Labu, "Sadarghat 256: Bangladeshi-born IS Leader's Code for Militant Financing." Chowdhury reportedly coordinated the attack details with Abu Terek Mohammad Tajuddin Kausar, an Islamic State operative based in Syria. For details, see Bansal and Quadir. For background on Tajuddin, see Khalil.

59 Hasan.

60 U.S. v. Elshinawy, "Plea Agreement."

Phase 1 – Acquisition of Drone, Rocket, and Counter-Surveillance Components

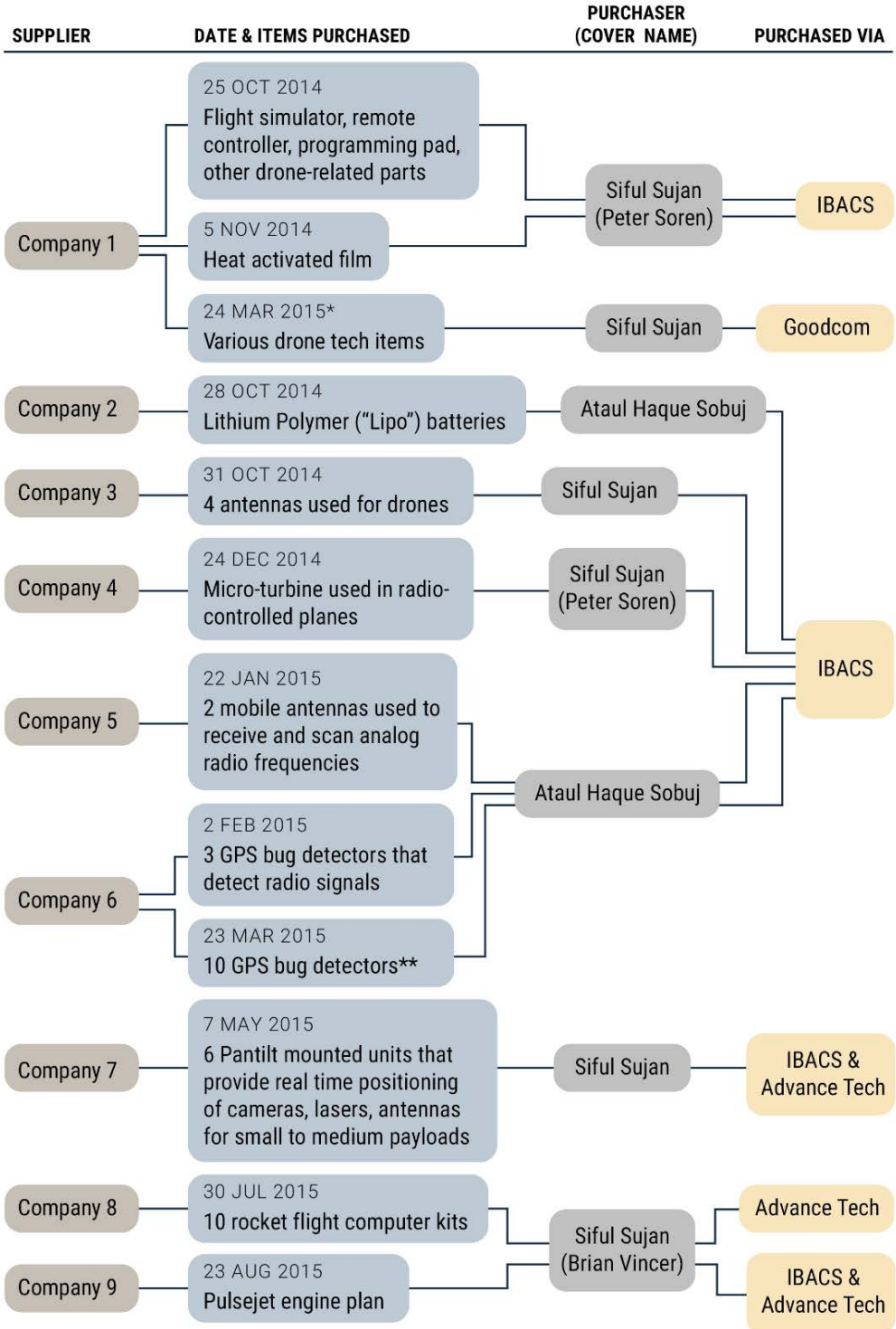
During Phase 1, Sujan and his brother used two of the IBACS companies (IBACS Tel Electronics LTD, IBACS IT Solutions LTC)[61] and Advance Tech to purchase, typically via PayPal, an array of drone-related components and other technology (see Table 1) from at least nine different companies located in the United States and Canada from October 2014 to August 2015.[62] Given the items purchased during Phase 1, it is believed that the items were requested and used by Islamic State operatives as part of a developmental program to counter or limit the effectiveness of sophisticated drones that were being operated by the United States and other parties to surveil and attack the group in Syria and Iraq.[63]

61 It is not clear if Sujan and other co-conspirators used the other three IBACS companies—IBACS Trade International LTD, IBACSTEL Corporation LTD, and IBACS Technologies LTD—as part of the conspiracy. For background on the incorporation, history, and leadership of the various IBACS companies as well as other non-IBAC companies with which Siful Sujan and Ataul Haque Sobuj were affiliated, see https://beta.companieshouse.gov.uk/.

62 U.S. v. Elshinawy, "Govt. Exhibit 4 – Conspiracy – Sequence of Events."

63 Author correspondence, FBI Special Agent. For context on the drone-counter-drone competition, see Don Rassler, "Drone-Counter Drone: Observations on the Contest between the United States and Jihadis," *CTC Sentinel* 10:1 (2017).

Table 1: List of Drone, Rocket, and Counter-Surveillance Components Purchased (Based on Evidence Filed in U.S. v. Elshinawy)[64]



**Same exact order made 11 additional times on 24 March..*
***Order later cancelled by company due to technical issue.*

64 U.S. v. Elshinawy, "Govt. Exhibit 4 – Conspiracy – Sequence of Events."

To mask activity during Phase 1, Sujan regularly used fake, Western-sounding cover names such as "Peter Soren" and "Brian Vincer" to initiate the purchases he made.[65] While the various transactions were taking place, key members of the group used the encrypted messaging applications SureSpot and Telegram to communicate amongst themselves and avoid detection from intelligence agencies.[66]

Even though the transactions made by the network during Phase 1 appear to have been legal, a number of things about the transactions are both surprising and concerning. First is the nature of the items purchased (drone, remote-control airplane, and rocket components, as well as counter-surveillance equipment) and where many of the purchased items were shipped to, especially considering the timing and the headlines the Islamic State was making at the time.

For example, in October 2014 and December 2014, months after the Islamic State declared the creation of their caliphate in late June of that same year, Sujan—using the alias Peter Soren—purchased four antennas used for drones from Company 3 and a micro-turbine used in radio-controlled planes from Company 4.[67] At Sujan's request, these two companies shipped these items direct to Sanliurfa, Turkey[68]—a town located an hour's drive from the Syrian border town of Tal Abyad, which the Islamic State controlled, and around a two-and-half-hour drive to the group's headquarters in Raqqa, Syria. In February 2015, Company 6 shipped three GPS bug detectors to Sanliurfa.[69] Then, a month later, that same company processed an order for 10 additional GPS bug detectors, a transaction the company later cancelled "due to requirement for items to be shipped to the address for the PayPal account used for the purchase," which was the IBACS office in the United Kingdom.[70]

Just as concerning was a purchase Sujan made using the alias Brian Vincer from Company 8 in July 2015 for "ten rocket flight computer test kits," which were also shipped to Sanliurfa, Turkey.[71] Although the shipment was sent, the shipment did not arrive at its destination because the items were "detained" by Turkish authorities, who later returned them to the company.[72] These purchases, which were essentially delivered to a town right next to the Islamic State's doorstep, illustrate just how easy it was for Islamic State operatives to obtain drone components from Western retailers at the time. This dynamic—given what the group later went on to achieve with commercial drones—raises some important questions about the internal review of purchases at these specific companies and/or the policies drone, rocket, and counter-surveillance equipment retailers have in place to detect and prevent suspicious transactions, as well as the apparent lack of regulations that exist to police the distribution of these types of components, especially when the items are set to be delivered to locations immediately adjacent to active war zones.

The network's list of purchases highlights another issue that likely should have raised red flags or facilitated greater scrutiny of the purchases being made: the quantity of items being purchased or the number of transactions made within a short period of time. For example, on March 24, 2015, Sujan made an initial purchase of "various drone technology items" in the amount of $1,376.09 from Company 1 for delivery to Sanliurfa, Turkey.[73] After that initial transaction, Sujan, sometimes using different names, made 11 repeat purchases of that same batch of goods on the same day from the same company—all to be delivered to Sanliurfa, Turkey—for a total, one-day sale of more than $16,000 in

65 Ibid.

66 U.S. v. Elshinawy, "Memorandum Opinion;" U.S. v. Elshinawy, "Govt. Exhibit 4 – Conspiracy – Sequence of Events."

67 U.S. v. Elshinawy, "Govt. Exhibit 4 – Conspiracy – Sequence of Events."

68 Ibid.

69 Ibid.

70 Ibid.

71 Ibid.

72 Ibid.

73 Ibid.

drone parts.[74]

A number of aspects associated with Sujan's interactions with Company 7 might have made that company suspicious. In May 2015, Sujan purchased six pantilt mounted units "that provide real time positioning of cameras, lasers, antennas for small to medium payloads" at a cost of $18,000.[75] Those devices were shipped to the IBACS office in Cardiff, United Kingdom, but the devices were paid for from funds wire transferred from Istanbul, Turkey.[76] Then, a little more than one month later, Sujan "tells company 7 he is looking for a thermal camera and is anticipating placing a bulk order for between 20 to 50 additional pantilt devices," a sizeable order.[77]

Phase 2 – Acquisition of Commercial Drones and Other Components

As noted above, the death of Sujan in December 2015 was followed shortly by a number of related arrests in the United Kingdom and Bangladesh. While these actions almost certainly had some type of disruptive effect on the Islamic State's drone component supply chain, Sobuj and other conspirators (and likely other networks that have not yet been identified or publicly revealed) continued to make drone-related acquisitions for the Islamic State for a period after Sujan's death[78]—an event that can be loosely understood as the beginning of Phase 2. Based on available evidence, it appears the focus of the drone-related acquisitions made by Sobuj and the other individuals with whom he was connected, shifted somewhat during Phase 2 and were more focused on the purchase of commercial drones and other components that would help the Islamic State transform those remotely piloted aerial systems into weapons of war.

According to Spanish police and Bangladeshi press accounts, several months before his brother was killed in Syria, Sobuj moved to Spain where he would go on to establish another technology company called INSYNKTEL, where he served as chairman.[79] After Sujan's death, authorities disbanded the IBACS office in Dhaka, but Sobuj was reportedly still able to create a Bangladesh-based firm named WAHMI Technologies, which employed many former, local IBACS employees.[80]

For an undisclosed period of time, Sobuj and his co-conspirators used the cover of INSYNKTEL, which had an office in Seville, Spain,[81] to send drones and drone components to the Islamic State, and WAHMI to send funds that were intended to foster militancy, specifically in Bangladesh. According to Spanish police, INSYNKTEL and WAHMI were established "from the beginning" with the intent to recreate the IBACS "business network in Spain under another name so as not to be detected."[82] Leveraging these two companies, Sobuj allegedly followed an established playbook and "used the same commercial network of suppliers, contacts and customers" that were used to support the IBACS

74 Ibid.

75 Ibid.

76 Ibid.

77 U.S. v. Elshinawy, "Govt. Exhibit 4 – Conspiracy – Sequence of Events." Video material released by the Islamic State demonstrates how the group has secured and used sophisticated thermal cameras in the field. For background, see Jared Keller, "The Islamic State Might be Dying (But it Has Some of America's Best Weapons)," *National Interest*, November 18, 2017.

78 Press Release, Spanish National Police, September 22, 2017, https://www.policia.es/prensa/20170922_3.html.

79 Ibid.; Hasan; "Bangladeshi Who Adapted Drones for Military Use by ISIL Arrested in Merida," Madrid ABC.es (in Spanish), September 22, 2017; Nuruzzaman Labu; "12 Militants Arrested at Same Time; Funding Should be Stopped," *Kaler Kantho* (in Bengali), September 25, 2017.

80 Faruk, "All Members of Same Family Involved in Militant Funding"; "Fact Sheet on the Detention of Ataul Haque," Spanish National Police, September 25, 2017; "Terror Funding Thru' IT Firm," *Daily Star*, September 24, 2017.

81 "Fact Sheet on the Detention of Ataul Haque."

82 Press Release, Spanish National Police, September 22, 2017; "Fact Sheet on the Detention of Ataul Haque."

conspiracy.[83]

This activity continued until late September 2017, when another round of coordinated arrests happened in three different countries. On September 22, Sobuj was arrested in Merida, Spain.[84] (According to a Bangladeshi press account filed in August 2017, the Counter-Terrorism and Transnational Crime Unit of the Bangladesh Police "sent a letter to Spanish police via Interpol to arrest Soboj for his alleged involvement in terror financing.[85] It is not clear if an Interpol red notice was actually filed and/or if this played a role in Sobuj's arrest.) Authorities in Bangladesh also arrested 11 people, eight of whom worked at WAHMI, on that same day.[86] The day after the arrests in Spain and Bangladesh, a 28-year-old Dane—who appears to have been part of the conspiracy—was arrested in Denmark on terrorism-related charges.[87]

The justifications that the authorities provided for the arrests and the other details that are available about the alleged crimes committed by those arrested provide a more complete picture of the intent, scope, and mechanics associated with Phase 2. For example, according to Spanish authorities, Sobuj "took advantage of his scientific-technical preparation to locate and mobilize sensitive dual-use technology for the development of drones as combat weapons."[88] Sobuj's actions were "hidden behind a complex network of specialized IT firms, which financed violent actions and looked for technological material, including drones, to send it to Syria for weapons purposes."[89]

Meanwhile, authorities in Bangladesh disclosed how ISYNKTEL sent WAHMI approximately $100,000, spread across 18 installments in a calendar year.[90] According to the spokesperson for Bangladesh's Rapid Action Battalion, "47 percent of [the] total amount sent from ISYNKTEL was spent in salaries and related affairs of the officials of Wahmi."[91] The remaining "53 percent … was spent in [sic] terrorist funding" to help recruit and train members.[92] Police officials also claimed that the individuals arrested were either members of, were affiliated with, or were sympathetic to Jama'atul Mujahideen Bangladesh (JMB), a local militant group with a long history in the country.[93] The Islamic State's affiliate in Bangladesh, Dawlatul Islam Bengal, "came into operational existence in July 2015, after a merger between a renegade faction of Jama'atul Mujahideen Bangladesh (JMB) and Jund at-Tawhid wal-Khilafah."[94] Since that time, Dawlatul Islam Bengal has been tied to a number of terrorist attacks and plots in the country.[95] The group, under the name ISIS-Bangladesh, has also been formally designated by the U.S. government as a Foreign Terrorist Organization.[96]

The suspect that Danish police picked up on September 22, 2017, was arrested for "allegedly shipping

83 Ibid.

84 "Alleged Islamic IT Expert Arrested in Spain," Prensa Latina, September 22, 2017.

85 Labu, "Sadarghat 256: Bangladeshi-born IS Leader's Code for Militant Financing."

86 Faruk, "All Members of Same Family Involved in Militant Funding"; "BDT 7.8 Million Comes From Spain; Spent in Militant Activities;" Arifur Rahman Rabbi, "IT Firm Involved in Terror Financing Busted," *Dhaka Tribune*, September 23, 2017.

87 "Danes Arrest Man for Allegedly Sending Drones, Cameras to IS," Associated Press, September 23, 2017.

88 Press Release, Spanish National Police, September 22, 2017; "Alleged Islamic IT Expert Arrested in Spain."

89 Ibid.

90 "BDT 7.8 Million Comes From Spain; Spent in Militant Activities;" "Fact Sheet on the Detention of Ataul Haque."

91 "BDT 7.8 Million Comes From Spain; Spent in Militant Activities."

92 Ibid.

93 For background, see "Countering Islamist Militancy in Bangladesh," Report No. 295, International Crisis Group, February 28, 2018, pp. 7-11.

94 Khalil.

95 See Nazrul Islam, "Charge Sheet of Holey Artisan Attack This Month," *Prothom Alo*, March 10, 2018; "31 'ISIL Supporters' Killed in 10 months," *Dhaka Tribune*, September 12, 2016; "Bangladesh Militant of Neo-JMB Terror Outfit Killed in Dhaka Suicide Blast," Firstpost, August 15, 2017.

96 "U.S. Designates 7 Groups, 2 Individuals as Global Terrorists," Xinhua, February 28, 2018.

drones, components for unmanned aerial vehicles and infrared cameras that were bound for the Islamic State group in Syria and Iraq."[97] According to media accounts, this suspect sent the commercial drones and cameras that he acquired to an Islamic State intermediary in Turkey, who then smuggled them into Syria and Iraq.

From Recovered Drones to Suppliers: Retracing Islamic State Drone Purchases

Another window into the Islamic State's drone supply chain comes from the investigative work of CAR. According to Damien Spleeters, the head of CAR's regional operations in Iraq and Syria, CAR has been able to identify—and retrace—how nine Islamic State drones, which were found in the field, were procured. One of the fundamental takeaways from this sample was the complexity regarding how Islamic State drones were sourced, as seven of the nine commercial drones were purchased from different distributors located in, or websites run out of, Lebanon, Turkey, Uzbekistan, India, and Kuwait.[98] Despite the small sample size, CAR researchers were still able to identify patterns, specifically how the Islamic State used retailers "more than once over an extended period of time," which—as noted by Spleeters—showed "consistency in Islamic State chains of supply."[99]

Figure 3: Islamic State Drones Recovered by and Retraced by CAR

But there is also evidence that the Islamic State's drone and drone component supply chain was diversified. For example, there is no overlap between the seven retailers used to purchase the nine commercial drones, which were retraced by CAR, and the nine retailers that Sujan and Sobuj used to purchase drone, rocket, and counter-surveillance equipment during the October 2014-August 2015 time period. The lack of overlap between the two sets of data could be explained in a number of different ways. First, any potential overlap might not yet be visible, because at this point in time it is not publicly known if any of the nine commercial Islamic State drones retraced by CAR were purchased after August 2015 by Sobuj, the individual arrested in Denmark, or potentially other Islamic State sympathizers associated with that supply network. Second, the lack of overlap might by due to changes made to the Islamic State's drone and drone component supply network over time. These changes were perhaps made in response to changing conditions or as part of an intentional security practice, whereby Islamic State purchasers might have limited the number of transactions made through each supplier so the group could minimize its signature and avoid unwanted attention. Third, the Islamic State could have also been using multiple networks, which could have been operating in partnership with or segmented from one another, to source commercial drones and related technology.

Another interesting takeaway from the CAR sample was the layered nature of how the nine Islamic State drones were being acquired, as in a number of the cases studied the commercially available

97 "Danes Arrest Man for Allegedly Sending Drones, Cameras to IS."

98 Author interview, Damien Spleeters, October 2017.

99 Author email correspondence, Damien Spleeters, May 2018.

drone was "purchased in one country, activated[100] in a second country, and then finally used in a third country"—Iraq or Syria.[101] (It is important to note how the drone activation process could have involved the drone and its owner being physically located in a particular country or the drone and its owner being located someplace else, as it is possible that the country where activation took place could have been masked or obscured using a Virtual Private Network (VPN), a proxy server, the TOR browser, or another security protocol.) These commercial drones were being purchased from companies by third parties.[102] These transactions were apparently facilitated by an Islamic State unit, which—according to U.S. officials—purchased "drones from commercial websites and other sources in China, India and Turkey."[103] Islamic State drone acquisition lists recovered by Iraqi forces specifically referenced the popular online distributor HobbyKing, a data point which suggests, but does not prove, that the site (and/or others like it) was a source of supply for the group.[104] The specific, to-the-cent pricing found on the Islamic State drone acquisition lists also seem to indicate that drone components were being purchased directly online. Islamic State financial documents left behind by the group's fighters in Mosul showed how the group was spending "thousands of dollars a month for drone equipment."[105]

The CAR sample, as well as other data, demonstrates how the countries involved in the various stages of the purchase-activation-use process varied across cases and potentially across time. For example, one of the two drones that Islamic State operatives purchased from a Kuwaiti e-commerce site during the 2015 to 2016 period was activated in Iraq.[106] But one of the drones the Islamic State purchased through an Indian website in August 2016 was activated in the United Kingdom that November.[107] And that particular drone, which was found in Tal Afar, Iraq, was found soon after its date of activation, indicating that the period between activation and use was not long.[108]

Figure 4: Life of an Islamic State Quadcopter Drone

The details associated with the individual arrested in Denmark in September 2017 point to Turkey being a country of activation as well. As noted above, the Danish individual allegedly shipped infrared

100 The drone activation process can vary by drone manufacturer. In the case of DJI, the drone activation process functions as a form of quasi-registration, whereby before operating their drone DJI drone owners are required to "log in to their DJI accounts and activate the latest firmware for their drones." This, in turn, allows the company to "sync up each device with the specific regulations of the country where it's being operated." For quote and additional background, see Adam Clark Estes, "DJI Will Cripple Your Drone if You Don't Register It on the Company's Website," Gizmodo, May 22, 2017.

101 Author interview, Damien Spleeters, October 2017.

102 Ibid.

103 Hennigan.

104 Rassler, al-`Ubaydi, and Mironova.

105 George and Hinnant.

106 Author interview, Damien Spleeters, May 2018. As noted in the text above, it is not known if the drone and its owner were physically located in the United Kingdom when this particular drone was activated or if the drone owner used VPN or some other type of mechanism to obscure their IP address location to make it appear as though the drone was activated in the United Kingdom when the drone owner was in another location.

107 Ibid.

108 Ibid.

cameras and drones to an Islamic State intermediary based in Turkey,[109] a pattern that fits the layered model identified by CAR. These three different examples show how the group's approach to activation varied, a dynamic that could be explained by the group's use of different purchasers who were based in different places or challenges the group encountered as part of the activation process (see below).

As the first two sections of this report highlight, the Islamic State was able to innovate and surprise its enemies from the air by taking a relatively simple approach that creatively merged sophisticated commercial off-the-shelf technology with low-tech components and other technological add-ons. This cobbling together of high- and low-tech systems, and the small and easy-to-replicate enhancements that the Islamic State made helped to transform off-the-shelf drone products into unique and fairly capable weapons, which the group used for lethal and psychological gains and for other purposes. The Islamic State's high-tech/low-tech approach was underpinned and made possible by the group's ability to acquire commercial drones and related components that were used for defensive and offensive purposes through a global and layered supply chain that involved purchases being made from at least 16 different companies that were based in or run out of at least seven different countries. The supply chain leveraged front companies as well as individuals and small cells who operated as purchasing and distribution agents for the group in various countries. The individuals involved in the Islamic State's drone-related supply chain made both repeat purchases from select vendors and singular purchases from others, a dynamic that demonstrates elements of consistency and diversity in the group's supply chain. And then once the Islamic State had a sizable number of commercial drones in hand, which were likely supplied by multiple supply chain networks (in addition to the ones described above), the Islamic State's centralized and bureaucratized approach to manufacturing provided the framework needed to bring the group's drone program to scale.

The section that follows explores the nature of the drone-counter-drone competition between the Islamic State and state actors, and how the gaps and seams that are left by drone countermeasure and drone defeat solutions still provide opportunities for the Islamic State—and potentially other terror groups—to leverage or use drones in other nefarious ways.

Drone Games, Terror Drone Diffusion, and Near-Term Threats

The development and use of the Islamic State's drone fleet and the efforts by the United States and other state parties to devise solutions to mitigate the group's drone capabilities are a case study in asymmetry. The quick ramp-up of the Islamic State's drone program, and the scale and broad deployment of its small-bomb drop capable drones, took the United States and its Kurdish and Iraqi partners by surprise. The United States and other parties knew that the Islamic State's use of drones was an important and evolving threat,[110] but the group's bomb-drop capability and expanded use of the commercial devices occurred before countermeasures to defeat the group's devices could be widely implemented. This led to an intensified push by the United States and its partners to fund, develop, and broadly field a range of drone defeat devices and to create a layered strategy to manage the problem over the short term.[111]

One key component of this strategy has been the kinetic targeting of individual Islamic State drone engineers, drone operators, and drone suppliers; the facilities used by the group to enhance and manufacture drones; and the areas where Islamic State drones have been launched and/or the group's pilots trained. For example, during the summer of 2017, "U.S. warplanes … destroyed several Islamic State drone depots, machine workshops and pilot schools … [and] killed eight commanders said to

109 "Danes Arrest Man for Allegedly Sending Drones, Cameras to IS."

110 For background, see Rassler, *Remotely Piloted Innovation*, pp. 45-46.

111 For background on the drone-counter drone competition, see Rassler, "Drone-Counter Drone."

be responsible for obtaining, arming and distributing the drones" into Syria and Iraq.[112] The goal of these efforts, according to the U.S. military, has been "to remove the militants' 'tactical ability to get their systems airborne,'" and it is believed to have been effective, at least as a short-term solution.[113]

Another major line of effort has been the development of a range of drone countermeasures that aim to defeat or takeover drone devices once they are airborne. These solutions range from drone-disabling guns and lasers to nets, drone-hunting eagles, and electronic and cyber countermeasures. The cost and time required to develop and field these solutions provide a window into the economic asymmetry that is at play. As noted by *New York Times* journalist Eric Schmitt, "The Pentagon is so alarmed by this growing threat ... that it has launched a $700 million crash program overseen by two senior Army generals to draw on the collective know-how and resources of all branches of the armed services, Silicon Valley and defense industry giants like Boeing and Raytheon to devise tactics and technology to thwart the menace."[114] Now, even though the Islamic State currently remains at the forefront of the terror drone threat, the various countermeasure solutions are being designed to help the United States and its partners better manage the drone threat from other actors. This includes potential, future drone-related threats from a range of adversaries from states like Iran and China to non-state actors such as Hezbollah.[115] And while an economic comparison between what the Islamic State and the United States are spending in their drone-counterdrone competition cannot be made at this time, it is clear that the amount expended by al-Baghdadi's group pales in comparison to the hundreds of millions being spent by the United States.[116] It is hard to imagine that state and non-state actors, especially those who view the United States as either a competitor or as an enemy, have not paid attention to this dynamic.

Another challenge is that the countermeasure solutions being developed each come with their own share of limitations. For example, one family of drone countermeasure solutions involves the use of different types of hardware and software packages, or deployable nets, mounted in a gun-like format so an operator can point the system at and disable or takeover a hostile drone target.[117] While these types of systems are certainly useful, especially since they are highly portable, they are only as good or as fast as the operator using them, and that person's aerial situational awareness. In some cases, this could be a problem and lead to unknown blind spots; residents of Mosul reported not being able to hear or see commercial drones used by the Islamic State.[118] So to be more effective, these types of devices likely will need to be paired with other types of systems, which only increases the overall cost. Other drone countermeasure solutions use a variety of tools to identify, track, and disable hostile drones automatically.[119] But again, these type of systems are only effective in the areas where they are placed, an issue that creates gaps and seams in coverage and opportunities for terrorist actors to strike elsewhere. These limitations provide a comparative advantage to terrorists as they only need to find and target areas that lack counter-drone systems.

There has also been a response from the drone industry. For example, to limit misuse of their drones,

112 Hennigan.

113 Ibid.

114 Schmitt. See also Gary Sheftick, "Innovative Agencies Partner to Counter Drone Threat," Army News Service, November 17, 2015, and John Kester, "Darpa Wants Mobile Technologies to Combat Small Drones," *Foreign Policy*, October 5, 2017.

115 For background on the drone capabilities of these actors, see Rassler, *Remotely Piloted Innovation*.

116 Not much is known about how much the Islamic State has spent to develop and maintain its drone program. Islamic State files evaluated by the Associated Press in Mosul indicated that the group was spending thousands of dollars a month on drone equipment. See George and Hinnant for details.

117 Examples of this type of system include Battelle's Drone Defender and DroneShield's Drone Gun. See Marco Margaritoff, "The 7 Most Significant Anti-Drone Weapons," Drive, June 21, 2017.

118 Westcott.

119 An example of this type of system is the Counter UAV system developed by Airbus. For background, see Kelsey D. Atherton, "Airbus Introduces a System to Jam Drones Out of the Sky," *Popular Science*, January 7, 2016.

DJI has "created software-based no-fly zones [NFZs] over large parts of Iraq and Syria where ISIS fighters have been known to strap improvised bombs to commercial drones."[120] The creation of NFZs is an approach that DJI and other commercial drone manufacturers have used to prevent users from being able to fly their products over sensitive locations, such as airports and military facilities, and other areas—like stadiums—that have high threat or disruption potential. In late May 2017, DJI also made news by announcing that the company would require all DJI drone owners to log into its website to initiate a "new application activation process," which would allow DJI to push firmware updates and "to sync up each device with the specific regulations of the country where it's being operated."[121] For those DJI drone owners who do not comply, DJI will "throttle" the drone "by cutting off live camera streaming and limiting … drone flights to a 50 meter (~164 foot) radius and 30 meter (~98 foot) altitude."[122] What this means in theory is that the drone in question will not be able to "stream images or video" to a controller and its transmission range will be significantly curtailed.[123] (For context, "the maximum transmission range for the DJI Phantom 4 is over three miles."[124]) But even these types of interventions might not be foolproof. As noted by Andrew Dalton at Engadget:

> "It's unclear whether geofenced NFZs [no fly zones] will actually stop extremists from weaponizing quadcopters and other remote-controlled flying machines. In the case of DJI equipment, a knowledgeable coder could likely circumvent the geofence with a software hack, and many of the devices used by ISIS are homebrewed or cobbled together from parts to begin with. And, of course, there's also the question of whether the NFZs affect Iraqi forces' own countermeasures."

A less well-discussed component of the United States' counter-drone strategy are efforts to identify and disrupt the supply of commercial drones, and drone add-on components—so those items never reach Islamic State operatives in the first place. While the United States' drone counter-measure investments have been well-publicized, it is not known how much or how little the United States has spent on intelligence, law enforcement, and diplomatic efforts to map out and identify the suppliers that provide the Islamic State with drones and related technology. This could be a potential resource allocation problem, because, as noted by Damien Spleeters, "Unless something is done about the sourcing of the material … countries will … be stuck in this continuous cycle of targeting more and more of ISIS's inventions, locations and operators."[125]

These dynamics speak to the asymmetric competition that is at play, a cat-and-mouse game of sorts, between al-Baghdadi's group, the United States, and other parties. After catching its adversaries by surprise, the scale of the Islamic State's drone capabilities in Syria and Iraq is being rolled back. The surprise factor that contributed to the Islamic State's drone gains in those two countries has also been exposed, which will make it harder for the group to achieve, or regain, the same level of drone impact in that region. Security forces battling the group in Iraq and Syria, as well as civilians living in areas that are under siege by the Islamic State or that are being defended by the group, will now also expect and be on the lookout for Islamic State drones. The broader deployment of additional counter-drone tools will also make it harder for the Islamic State in Iraq and Syria to be as successful with its drones as it has been in the past. But the Islamic State has proven itself to be resilient, resourceful, and creative, and so the drone-counter-drone competition between states and non-state actors such as the Islamic State will evolve.

120 Andrew Dalton, "DJI Grounded its Drones and Iraq and Syria to Lock Out Extremists," Engadget, April 26, 2017.

121 Estes.

122 DL Cade, "DJI Will Severly Limit Your Drone if You Don't 'Activate' it Online," PetaPixel, May 22, 2017.

123 Estes.

124 Ibid.

125 Schmitt.

Future Terror Drone Use

Given the Islamic State's penchant for innovation, we should expect more from the group and from other actors inspired by what the Islamic State has been able to achieve in the aerial domain. The following are some possibilities about what we could see next and where the terror-drone threat might be headed. These possibilities are informed by the author's research on past instances of diffusion of this technology among terrorist groups, as well as research on new developments affecting technology and the geopolitical landscape.

Different Theaters and Different Types of Groups

The Islamic State and its affiliated groups have already tried to use commercial drones outside of Syria and Iraq. In January 2016, for example, the Islamic State released a video with an overhead view of a battle in Benghazi that was taken by a drone.[126] Multiple reports filed by journalists covering the clash between Philippine forces and the Maute group and other Islamic State-affiliated fighters in Marawi also noted the presence and use of commercial drones by these groups operating in that city.[127] Drone use by Islamic State-affiliated entities has been reported in Yemen as well.[128]

There is a large number of photos and videos available online and via social media that show what the Islamic State's bomb-capable system looks like and how it works, and the existence of this material will make it easier for other terror organizations that have already expressed an interest in, or actually used, drones to copy the approach, even if only for one-off drone operations. A useful parallel in this regard is the pressure cooker bombs that the Tsarnaev brothers constructed and used in their attack on the Boston Marathon in April 2013. The Tsarnaev brothers were able to construct those bombs thanks to an instructional, step-by-step, how-to article that was published in the first issue of al-Qa`ida in the Arabian Peninsula's English-language magazine Inspire.[129]

The nature and potential geographic and organizational scope of the terror groups that might soon follow suit is reflected by the list of terror entities that have already acquired and used drones. A previous study conducted by the author, for example, found that a range of terrorists groups, motivated by different ideologies—from jihadi to apocalyptic, right-wing and irredentist orientations—have historically sought out and tried to use commercial drones.[130] This list includes groups like Aum Shinrikyo, al-Qa`ida, the Afghan Taliban, Haqqani network, Lashkar-e-Taiba, and the FARC, as well as other incidents motivated by individual actors.[131] As of late 2016, the list of countries where these drone incidents and drone-related plots took place included Syria, Iraq, Iran, Palestine, Israel, Egypt, Colombia, Germany, Spain, the United States, Japan, Pakistan, and Afghanistan.[132]

The Islamic State's use of armed drones has already spurred copycats, so we are likely at the leading edge of this phenomenon. One of the first groups to mimic the Islamic State's approach was an unlikely one: Iraqi security force (ISF) units.[133] The ISF recognized that the Islamic State had a good, cheap, and easy-to-replicate idea on their hands, so they copied the drone bomb-tactics used by their

126 "Benghazi the Meaning of Steadfastness," Wilayat Barqah, January 16, 2016.

127 Thomas Luna, "DJI Drones are Getting Shot Down in the Battle of Marawi," WeTalkUAV.com, July 17, 2017; Tom Allard, "One week to cross a street: how IS pinned down Filipino soldiers in Marawi," Reuters, September 25, 2017; "Maute-ISIS bandits use drone in Marawi to evade pursuing soldiers," GMA News Online, June 19, 2017; Kaye Imson, "Marawi Crisis: Govt forces retake Maute's stronghold in Dansalan College," News5, July 4, 2017.

128 Hennigan.

129 For background, see Azmat Khan, "The Magazine the Inspired the Boston Bombers," PBS, April 30, 2013.

130 Rassler, *Remotely Piloted Innovation*.

131 Ibid.

132 Ibid.

133 Jim Michaels, "Iraqi Forces Now Attacking ISIS Forces With Drones in Mosul," *USA Today*, April 25, 2017.

adversary. Another potential copycat case that has already occurred took place much farther away. In late October 2017, Mexican authorities arrested four individuals in Guanajuato in Central Mexico.[134] These four individuals had in their possession an AK-47 and a commercial drone outfitted with an explosive rigged to drop from the air.[135] While the exact affiliation of the four men has not been disclosed, the city of Guanajuato "is currently contested by several drug gangs, including the Sinaloa cartel, Los Zetas, and Cártel Jalisco Nueva Generación."[136] This case is important as it demonstrates how an actor half a world away, and one likely motivated by profit and not jihadi ideology, built and apparently had plans to use an explosive-laden commercial drone. We should expect more of these type of incidents in the future.

Different Tactics, Different Targets, and Different Weapons

The Islamic State was able to achieve whatever drone successes it has had because it was able to acquire commercially available drones and creatively outfit and use them in innovative ways. Since the group is opportunistic, it will likely continue to try to use its bomb-capable drones in the same ways that it has in the past, and to strike when and where it sees opportunities and vulnerabilities. But it would also be wise to expect the group's drone program to evolve. To regain the operational element of surprise, skirt countermeasures, and maximize both body counts and publicity, it is somewhat predictable that the Islamic State will try to develop different drone tactics, seek out different drone targets, and use different types of drone weapons. It is not clear whether these potential, future changes will be effective or whether it will be other parties inspired by the Islamic State's drone actions that will implement them. But there are some indications that the potential pursuit of different targets and use of different drone weapons has the potential to be deadly and quite dangerous.

One obvious shift would be for the Islamic State to use its armed drones to target civilian or mixed targets in the West and in other locales. Imagine, for example, the added operational and psychological impact of the November 2015 Paris attacks if the Islamic State attackers who conducted that operation, also used an armed drone to target other civilians or first responders who responded to the incident, or both.[137] Even if Islamic State operatives just filmed elements of that attack from the air, the release of such footage would almost certainly have had a significant shock factor, similar to the group's beheading videos. While the Islamic State or individuals inspired by the organization have not used a drone as a weapon in the West, the group has already released propaganda material that visually shows drone attacks being conducted against symbolic targets in the United States.[138]

Terrorists face a number of choices when it comes to potential weapons, as each weapon has its own set of advantages and disadvantages. To inflict damage from the skies, the Islamic State has generally dropped 40mm grenades or other grenade-type explosives from its quadcopter drones.[139] But a few data points suggest that the Islamic State has also considered the use of chemical weapons as a potential option for its drones. Indeed, the first known, publicized discovery of an Islamic State drone occurred in June 2013 after Iraqi authorities raided "three workshops for manufacturing chemical

134 Robert J. Bunker and John P. Sullivan, "Mexican Cartel Tactical Note #35," Small Wars Journal, October 23, 2017.

135 Kyle Mizokami, "Mexican Drug Cartels are Turning Drones Into Flying Bombers," *Popular Mechanics*, November 1, 2017.

136 David Axe, "Great, Mexican Cartels Now Have Weaponized Drones," Motherboard-VICE, October 25, 2017.

137 The author gives credit to Bruce Hoffman for first mentioning the Paris attack example. See Christopher Dickey, "As ISIS Prepares its Terror Resurrection Watch Out for Drone Swarms," Daily Beast, February 28, 2017.

138 Almohammad and Speckhard.

139 Waters, "Death from Above."

agents" where "toy planes were seized on site."[140] According to local press accounts, the five men arrested were "reportedly planning to use remote-control helicopters to distribute sarin and mustard gas as part of an attack against unspecified targets in Iraq, North America and Europe."[141] Close to three years later, in the spring of 2016, U.K. Prime Minister David Cameron and other world leaders expressed concern that the Islamic State was planning to use commercially available drones to disperse toxic materials in Western cities.[142] Those leaders made specific references to the group's interest in using a radioactive "dirty bomb."[143]

Successfully carrying out a chemical drone attack is not necessarily an easy thing to do, and conducting an effective biological or radiological drone attack is even harder to pull off. The Islamic State does have a track record of chemical weapons use, however, as the group is believed to have used chemical weapons in Syria and Iraq more than 50 times.[144] The Islamic State also holds the unfortunate distinction of being "the first non-state actor to have developed a banned chemical warfare agent and combined it with a projectile delivery system."[145] Concerns about future Islamic State chemical attacks outside of Syria and Iraq were raised again in the summer of 2017 when Australian authorities arrested two brothers and "disrupted an Islamic State plot to build an "improvised chemical dispersion device" that the brothers planned to fill with hydrogen sulfide, a poisonous gas, and use in urban areas.[146] Other details of the plot, as noted by Columb Strack, are even more troubling:

> "According to the Australian police, instructions on how to construct the device came from an Islamic State 'controller' in Syria. Military-grade explosives had been shipped to the pair with air freight via Turkey for a separate aborted plot to bomb a passenger jet. The brothers had also acquired in Australia some of the precursor chemicals for the poison gas plot, although they were reportedly 'a mile and a half away' from constructing a viable chemical dispersal device. The plot illustrates how the Islamic State has the capability not only to transfer the know-how to produce toxic chemicals via secure online communications to operatives already living in target countries, but also to ship materials, including explosives, undetected."[147]

While the threat posed by the Islamic State, and the group's linked or inspired sympathizers, in this regard is real, there are other factors that limit the potential lethality and impact of any future Islamic State chemical drone attack in the West. With the loss of Mosul, the Islamic State's ability to produce and develop chemical weapons has also been degraded.[148] Further, "the generally low level of expertise the group has demonstrated" suggests "that an attack using widely available toxins or industrial chemicals would be far more likely than the use of blister or nerve agents like sulfur mustard or sarin."[149]

Even if an Islamic State chemical attack was not that sophisticated, however, or did not lead to many deaths, the propaganda and shock value of such an attack alone might make the effort worth it.

---

140 David Blair, "Iraq Foils Suspected al-Qaeda Plot to Launch Remote-Controlled Helicopters Carrying Chemical Weapons," *Telegraph*, June 3, 2013; Madeleine Morgenstern, "Iraq Says It Foiled New Al-Qaeda Plot to Use Toy Planes to Drop Chemical Weapons over North America and Europe," Blaze, June 2, 2013. For background on Abu Musab al-Zarqawi's history of experimentation with chemical and biological agents, see Joby Warrick, *Black Flags: The Rise of ISIS* (New York: Doubleday, 2015), pp. 70, 89, 139, and 144.

141 For background, see Rassler, *Remotely Piloted Innovation*, pp. 34-35.

142 Ben Riley-Smith, "ISIL Plotting to Use Drones for Nuclear Attack on West," *Telegraph*, April 1, 2016.

143 Ibid.

144 Thomas Gibbons-Neff, "Report: Islamic State has Used Chemical Weapons 52 Times in Iraq and Syria Since 2014," *Washington Post*, November 22, 2016.

145 Columb Strack, "The Evolution of the Islamic State's Chemical Weapons Efforts," *CTC Sentinel* 10:9 (2017).

146 Tim Johnson, "Something Else to Fret About: ISIS Mounting Dirty Bombs on Drones," McClatchy, September 7, 2017.

147 Strack.

148 Ibid.

149 Ibid.

More Drones: Not Just One Drone, But Multiple, and Land and Sea Drones, Too

Future attacks using not just one, but multiple aerial drones should be expected, too. The Islamic State displayed such a capability. During a speech in May 2017, the current head of U.S. Special Operations Command, General Raymond A. "Tony" Thomas III, noted how during the battle for Mosul "in the span of 24 hours there were 70 drones in the air."[150] He went on to add how "at one point … there were 12 enemy drones—'killer bees' dropping 40mm" bombs.[151] The commander of the U.S. Army's Combined Arms Center, Lieutenant General Michael D. Lundy, has also noted how the Islamic State's use of commercial drones in Iraq has "gone to almost swarm-level capability in a couple of cases."[152] So the group's use of multiple drones is no longer hypothetical, but a demonstrated capability. It is likely that the group of drones used by the Islamic State in these cases were remotely controlled by a collection of group members operating at a stand-off distance. There have been no demonstrated cases thus far of the Islamic State using autonomous or pre-programmed drones that take the human controller out of the loop.

Lastly, the concern and emphasis placed on defeating the Islamic State's aerial threats has also overshadowed the threats posed by drones that operate on land and at sea. In January 2017, for example, "Iranian-backed Houthi rebels … reportedly launched a sea-based armed drone against a Saudi warship," which killed two Saudi sailors.[153] Fighters in Syria and Iraq have also been experimenting with remotely controlled vehicles and small robots for nearly a decade.[154]

Conclusion

Terrorist organizations profit from the identification and exploitation of security gaps and seams, and the success of terror operations is also often tied—like the success of Special Operations Force missions[155]— to the perpetrators being able to maintain an element of surprise. The Islamic State was able to build and deploy a fleet of attack, bomb-drop capable drones and achieve moderate impacts because the group found gaps and seams that allowed it to source commercial drones, and related components, in the first place. The group's innovative cobbling together of commercial drones with cheap, add-on components made it easy to transform stock quadcopters into more nefarious and moderately capable devices. And while the Islamic State's drone program has been placed under pressure and the scale of the group's program has been significantly curtailed and rolled back, what the group was able to achieve with commercial drones unlocks a genie of sorts, as the group demonstrated what was possible with a little bit of sinister engineering. Not only will the Islamic State's drone tactics and approaches likely evolve—and present other threats in the future—but details about how the group was able to modify drones for operational purposes can be easily found online and copied by others.

While this report sheds new light on the nature and structure of the Islamic State's drone supply chain, there is still a lot to learn about how the group acquired its fleet of commercial drones and related technology, and how the organization's drone program developed. Given the drone and drone-related purchases revealed via the IBACS network and the investigative work of CAR, it seems likely—due to

150 Howard Altman, "Tale of Two Drones: ISIS Wreaked Havoc Cheaply, Tampa Meeting Showcases State of the Art," *Tampa Bay Times*, May 16, 2017.

151 Ibid.

152 Michaels.

153 Carol Munoz, "US Military Drone Dominance Challenged by Enemies," *Washington Times*, October 2, 2017.

154 For background, see Stuart Ramsey, "Exclusive: Inside IS Terror Weapons Lab," Sky News, January 5, 2016.

155 For background, see William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (New York: RandomHouse, 1996).

what is known about the number and frequency of Islamic State drone missions during the 2017 time period—that the organization also acquired commercial drones through other, additional channels.

The availability of commercial drones and the increasingly sophisticated technology that underpins the capabilities and performance of today's off-the-shelf drones present a challenging conundrum. These devices and others like it, which are quite affordable, relatively easy to access, and continue to become more capable and smaller in size, have revolutionized many industries and have also helped to enhance private life. The benefits of the technology and its availability are all too visible. But, as many others have noted, there is also a dark side to the commercial availability of the robotics, sensing, communication, and navigation technology that can be found in commercial-off-the-shelve drones, as this technology can be misused and repurposed to develop novel weapons of war–and at scale.

The details highlighted in this report also speak to an emerging, seemingly apparent truth: how the 'rise' of hybrid warfare, a current of which emphasizes the combination of low-cost equipment that can be used at scale with more costly systems or forms of technology, will likely require the development of new, hybrid public-private sector approaches to effectively manage, track, and degrade future hybrid threats that leverage and/or are based off of commercial systems.

Terrorist groups and hostile state actors will almost always be able to find supply chain gaps and seams. But that does not mean that efforts cannot or should not be made to tighten or better track the purchase of predictable dual-use items—such as commercial drones, rocket and counter-surveillance equipment, and other similar devices that helped the Islamic State to enhance its defensive and offensive capabilities—through creative partnerships with industry. Indeed, this report highlights how some of the purchases made by the IBACS network, and its suspicious nature, could have led investigators to those leading and acting on behalf of the IBACS network earlier if the companies involved either conducted better due diligence of transactions being shipped to the doorstep of a complicated warzone or had access to a government or neutral third-party that could have provided that type of assistance for them. Such an approach could even be automated based on keywords, common sense indicators, and questionable patterns of behavior (perhaps similar to those used in the anti-money laundering and financial compliance arenas), and be driven by a smartly designed system that would evaluate purchase data across different types of transaction management software types, which would reduce barriers to entry.

Another potential way to close the dual-use gap would be to work with industry to bolster or enhance, through cheap and cost effective approaches, how commercial drones and their associated packing can be tracked—or retraced after devices or components have been recovered in conflict areas. This would help to shorten the investigative time period and make it easier for entities like CAR to match a specific drone or device with a specific retailer after it has been recovered.

Lastly, given the large amount of funds being spent by the United States and other nations to counter hostile drones of all types, it certainly seems reasonable that more attention and resources should be spent on efforts that aim to prevent the delivery of select dual-use items to major conflict zone areas, to investigate and map out supply chain networks, and to retrace specific equipment—like drones—found in the field so existing procurement channels can be closed more rapidly.