Weapons Trafficking and the Odessa Network: How One Small Think Tank was Able to Unpack One Very Big Problem, and the Lessons It Teaches Us

David E. A. Johnson

> Oh, what a tangled web we weave, when first we practice to deceive!
> —Sir Walter Scott, *Marmion*

Today's security environment is very different from the one we faced even two decades ago. Asymmetric and hybrid threats take advantage of the industrial-age doctrine, law, and organizational and geographic boundaries that we created to fight the World Wars and manage the Cold War. Informal and illicit power structures embed themselves in licit systems to promote political violence and gain control of vital resources. Persistent security challenges, such as arms trafficking and environmental crime, feed the local conflict economies and empower the illicit networks. This expansion of mission scope provides a daunting challenge for the intelligence community. But the arrival of the information age also provides the tools necessary to understand and influence these power structures. Using these tools, a C4ADS report, *The Odessa Network,* has mapped the intricate web of entities and processes used to execute a series of illicit arms transfers.

C4ADS (www.c4ads.org), winner of the Google Chairman's 2014 "New Digital Age" Grant, is a tiny Washington, DC-based, nonpartisan, nonprofit organization dedicated to enhancing global security.[1] Leveraging unique people, unique data, and disruptive emerging technology, it does quantifiable investigative reporting on illicit networks, addressing complex threat systems that cross regional and governmental department boundaries.

In 2010, the C4ADS leadership felt that a bureaucracy-bound, sensor-driven defense and intelligence establishment, designed never to lose sight of the Japanese Fleet again, was floundering in its attempts to understand the new threats and take advantage of the opportunities inherent in the new information paradigm.[2] The C4ADS leadership team further realized that traditional academia, think tank, and contractor models could not accomplish this, either.

To address this gap, they adopted an approach advocated by one of their fellows, Dr. John W. Bodnar, in his book *Warning Analysis for the Information Age*.[3] They selected and trained a few ambitious young international-relations student-analysts who spoke more than one language fluently, had lived abroad for at least a year, and were capable of quantifiable analysis for the core team. They modified the "starfish and spider" organizational concept, creating a flat hierarchy with greater end-

[1] Reuters, "Google Executive Chairman Eric Schmidt Names 10 Recipients for the 'New Digital Age' Grants," press release, Mar. 10, 2014, www.reuters.com/article/2014/03/10/idUSnMKW16JQpa+1cc+MKW20140310.

[2] David E. A. Johnson and Newton Howard, "Network Intelligence: An Emerging Discipline" (proceedings, Intelligence and Security Informatics Conference, Istanbul, Aug. 22-24, 2012), http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6298848&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F6298753%2F6298809%2F06298848.

[3] John W Bodnar, *Warning Analysis for the Information Age: Rethinking the Intelligence Process* (Washington, DC: Joint Military Intelligence College, 2003).

point access to enhance situational awareness and still execute effective projects.[4] This change—along with the special access to sources, and the unusual freedom to focus on the problem set, that being a nonprofit organization with a donor-based business model permits—enabled rapid change and innovation. The C4ADS leadership team partnered with Google and Palantir; downloaded FOCA, NodeXL, QGIS, and other free software tools; and set out to explore the boundaries of open source intelligence.

In the winter of 2012, the chief operating officer, Farley Mesko, conceived a flagship project to examine the hypothesis that Russia was illicitly resupplying Syria's Assad regime with arms. He teamed up with analyst and Russian-language laureate Tom Wallace. In the process of their investigation, they successfully unraveled a complex web of activities that included licit and illicit organizations, multiple governments, and a social network cutting across four continents. This report had a huge effect. Pulitzer Prizewinning journalist Joby Warrick described *The Odessa Network* in a *Washington Post* article.[5] The president of Lithuania tweeted about the report. The Greek Navy seized two ships identified in the report, which were carrying 39 tons of arms. Military Sealift Command canceled large contracts with an identified shipping company. A Russian private military contractor identified in the report was found working in Syria, resulting in a change to Russian law. And the specter of corruption and Russian control raised in the report may have contributed to the downfall of the Yanukovych government in Ukraine.

The report used a wide range of open source local media reports in Arabic, Spanish, Russian, and Ukrainian; court cases and contract disputes from Russia, Ukraine, and the United States; incorporation documents made available as exhibits in those cases; and business directories from Europe, the Middle East, Africa, and elsewhere.[6] *The Odessa Network* demonstrated the utility of combining open source data, foreign language and regional expertise, and cutting-edge technology in answering complex research questions, thereby bridging the gap between tactical data and strategic insight.

The best policy-level insights are derived from tactical-level data that has been traced upward into abstraction. Deep investigation into weapons export provided political insights into the inner workings of Putin's Russia: "Abstract themes find detailed expression in the Odessa Network: reassertion of State control over strategic assets, keeping regime stakeholders loyal through sanctioned corruption, "power vertical" relationships, and fusion of public and private entities."[7] All data in the report was open source or commercially purchased. The report examined both licit and illicit weapons transfers. The authors used the term "illicit" to describe transfers perceived as contrary to international norms, not to imply violation of any international laws or agreements.

The Odessa Network is not any better or worse than other informal power structures, but its study provided some interesting lessons. In the process of discovering the details

[4] Ori Brafman and Rod Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin Books, 2006).

[5] Joby Warrick, "Ukrainian Port Eyed as Analysts Seek Syria's Arms Source, *Washington Post*, Sept. 7, 2013, www.washingtonpost.com/world/national-security/ukrainian-port-eyed-as-analysts-seek-syrias-arms-source/2013/09/07/f61b0082-1710-11e3-a2ec-b47e45e6f8ef_story.html.

[6] Tom Wallace and Farley Mesko, *The Odessa Network*, C4ADS, Sept. 2013, 10, www.globalinitiative.net/download/arms-trafficking/arms(2)/C4ads%20-%20The%20Odessa%20Network%20Mapping%20facilitators%20of%20Russian%20and%20Ukranian%20Arms%20Transfers%20-%20Sept%202013.pdf.

[7] Ibid., 11.

of Russian arms flows to Syria, the C4ADS team learned a great deal about bringing illicit power structures to light. First, they identified the C4ADS Postulates for Discovery of Illicit Networks:

1. All illicit networks touch licit networks somewhere.
2. To have an illicit capability, one must have a licit capability.
3. Human networks do not behave like mechanical networks.[8]

Using these postulates effectively will require that the government official or contractor be comfortable thinking outside the usual areas of expertise and authority. The postulates imply that publicly available data about licit activities can enable us to observe threat systems. Moreover, it is vital that the analyst understand how these commercial and consumer systems function.

As a nonprofit doing investigative reporting, C4ADS conducts legal review of its work and provides caveats with its products so that readers do not misinterpret the fully sourced, supported findings of the reports. C4ADS does this to protect those enablers of illicit networks who may be unwittingly complicit and not doing anything illegal or immoral. This is as opposed to facilitators, who knowingly support perpetrators of illicit activity through their own licit and illicit activity. Finally, the postulates imply that simple interdiction and action by any single entity or agency cannot have a useful long-term effect on the threat system. Because these networks are embedded in stable, licit systems, a sustained impact requires better understanding of illicit networks across regional and governmental department boundaries, and longitudinal study of the results of action against them. Next, the project identified some shared characteristics of illicit networks: local government acquiescence, key individual connectors, and leverage of the licit financial system.

Most importantly to our study, C4ADS also discovered a replicable process for gathering and analyzing open source information across a number of analytical methods and tools. This process highlights the need for integration across intelligence disciplines and staff functions. Other C4ADS efforts include reports on Somali Piracy (for the World Bank), on insurgency and contraband trafficking in Mali (cited by RAND), and on global ivory poaching and wildlife crime.[9] Each of these works has further reinforced the lessons taken from *The Odessa Network* project.

Use the Correct Tool for the Task

C4ADS's approach to the challenge of illuminating the complex illicit power structure involved in suspected Russian state-sponsored arms trafficking required unique people, unique data, emerging technology, and a top-down analytical direction. These were applied to create useful, credible data sets, and insightful, supported analysis.

[8] David E. A. Johnson, "Transforming Ideas into Operations" (PSOTEW WG3 presentation, National Defense University, Apr. 14, 2015).

[9] Michael Shurkin, and Stephanie Pezard, Achieving Peace in *Northern Mali: Past Agreements, Local Conflicts, and the Prospects for a Durable Settlement* (Santa Monica, CA: RAND, 2015).

Unique People

The C4ADS organization was very small and flat, consisting of a board of directors, an executive director, analyst leaders, analysts, interns, and fellows. The leadership selected project-specific analysts. They were generally recent undergraduate or graduate international-relations students from top-tier universities, who had lived at least a year in their region. They had open contacts with foreign entities, were ambitious, and were well connected, through family, peers, and professors, even up to the highest levels of industry and government. Experience was not a selection criterion. As Frederick the Great once noted, "A mule who has carried a pack for ten campaigns under Prince Eugene will be no better a tactician for it."[10] In fact, time spent isolated in a bureaucracy and learning local processes may be counterproductive. Before selection, interns attended a three-month unpaid internship and training program. The leadership encouraged analysts to bypass the "chain of command" and contact anyone in or outside the organization, regardless of title, who could assist with their problem. The young analyst was expected to develop the project, build the funding proposal, lead research, conduct on-the-ground interviews, prepare the report, coordinate with media, publish, and brief conferences and officials. One of the analysts on the Odessa Network report briefed the U.S. vice president's national security staff. While this approach may not be fully replicable in government, academic, or corporate structures, partnering with such teams is possible.

Unique Data

C4ADS used a definition of "open source" not used by the U.S. government. For C4ADS, open source data included anything legally commercially purchasable or freely available in the public domain. This included *general media, expert interview, commercial and public databases, and gray literature.*

General media contains print, video, audio, and online sources (including the current and archived websites and social media of identified organizations and individuals). For event data, C4ADS avoided U.S. outlets and preferred to examine international and local sources in the original language first. The analyst, depending on the question, may develop favorite sources based on a personal understanding of source history, bias, and credibility.

Expert interview includes not only individuals with a reputation and publications, but also anyone with the access and placement to provide useful, credible data or contacts.

Commercial and public databases contain a wide variety of data sets: telecommunications metadata, online feeds, satellite imagery, ship and aircraft transponder records, geospatial data, full-spectrum emissions data, court cases, property ownership, corporate registries, and financial data.

Finally, *gray literature* is the unpublished and published research of academic and commercial entities. Thus, open source includes access to elements of *all* the intelligence disciplines.

While the authors did travel to Ukraine for supplementary information, most of the work was done in the United States. By data foraging for readily available information and not data mining through restricted areas, the authors were able to develop

[10] Jay Luvaas, ed., trans., *Frederick the Great on the Art of War* (New York: Free Press, 1966), 47.

the product without doing anything even approaching espionage. Moreover, with all data appropriately source tagged and caveated, they were ready to build a strong argument. C4ADS holds itself to the standard of nonpartisan and credible conclusions drawn from the available data by a reasonable person. By leveraging all the open source components, the Odessa Network analysts could fill information gaps in even data-poor environments to produce data advantage and credibility.

Emerging Technology

Once the data is gathered, the analyst must apply qualitative and quantitative analytical techniques to create insight. Over 10 years, C4ADS has explored techniques ranging from dynamic, multimodal social network analysis with geospatial fusion, to simple descriptive statistics. The authors used a donated Palantir platform that included many of these tools. Another use of the term "open source" describes a business model for essentially free software. As a nonprofit, C4ADS readily adopts and tests these tools and uses donated software and hardware packages. The C4ADS team chose their bins, coded, and structured data manually. Because they were originally trained in CASOS-ORA and QGIS, the transition to Palantir was not difficult. The authors tested a number of open source and commercial data scrapers, including FOCA, and, of course, used Excel from Microsoft Office. As planners at CJSOTF-AP in 2003 in Baghdad proved, it is even possible to build a predictive analysis engine at no cost, from Microsoft Access and Falcon View.[11] The freedom to choose the tools and emerging technologies to search and process everything from Facebook photos and imagery metadata to transponder locations, Russian court documents, and corporate registries enabled the analytical team to find a way around obstacles.

Hypothesis-Driven Analysis

The C4ADS Postulates can help in identifying activities and even phenomena to observe. But without understanding the research question, it is difficult to select the appropriate analytical approach. Traditional sensor-driven approaches assume an understanding of the threat process model, and hope—mostly in vain—that data patterns will "speak" to the analyst. The analyst is frequently in danger of data overload and, most importantly, cannot define why a pattern change is important. Hope is not an analytical process. The alternative is top-down, hypothesis-driven analysis that seeks to define, instead of assume, a useful threat process model and provides data credibility and advantage. Bodnar indicates that both approaches are useful.[12] But few organizations have integrated hypothesis-driven methods effectively into their arsenal. C4ADS took a hypothesis-driven approach to the project.

The overall hybrid adaptive process is cyclic and consists of four phases: *hypothesis development, data foraging, sense making,* and *argumentation and testing*. *Hypothesis development* relies heavily on the context and the analyst's mental flexibility, general knowledge, personal history, and time spent on the problem. This requires an analyst with broad

[11] Author was chief of plans and current plans, CJSOTF-AP, when Maj. Ace Campbell and Maj. Larry Fauconet, two U.S. Army Reserve officers, developed this tool.

[12] Bodnar, *Warning Analysis for the Information Age*.

exposure to the enablers being examined. The initial research question has a tentative answer (hypothesis) that generates questions about the threat process. These questions are used to drive research.

Data foraging requires intuition and choices concerning the sources and binning of structured, unstructured, coded, uncoded, qualitative, and quantitative data.

Sense making leverages the use of appropriate analytical tools and descriptive statistics to provide evidence that supports understanding of a portion of the threat process model. The Odessa authors took particular care not to fixate on any particular tool or source, since these are entirely secondary to answering the question being asked.

The *argumentation and testing* phase builds the argument that supports the hypothesis. This argument must be structured to answer the question asked, in a way that convinces an informed audience. Moreover, at each phase there are formal and informal tests, such as analysis of competing hypotheses, that can result in reforming the hypothesis.[13] While the team continually adapted the process, this general approach was at the root of the C4ADS Odessa Network Project.

Create a Threat Process Model

At the start of the Syrian Civil War, C4ADS was looking for a project to demonstrate the power of data-driven open source analysis. Tom Wallace, a national Russian scholar laureate at the University of Michigan and a Wolcott fellow at the George Washington University, asked himself, if the Assad regime was depleting its stocks of arms, how was it being resupplied? His logical hypothesis was that Syria's longtime ally Russia was rearming the Assad regime despite international resolutions. Further, he wondered, if this was so, how would Russia do this, and how could he prove it? Farley Mesko immediately began to apply the analytical concepts used at C4ADS to support this initial hypothesis and set of research questions.

Build the Data Set

The beginning and end of the abductive inferential intelligence cycle is to create and confirm a useful threat process model.[14] The first step for C4ADS was to conduct general research into the descriptions of abstract activities surrounding arms transfers in existing literature. To do this, the team created a data set of Russian and Ukrainian weapons transfers and the ports, companies, and ships used to facilitate them: "The critical assumption was that transporting arms shipments to sensitive foreign customers requires a great deal of trust between contractors and the government suppliers. Therefore, suppliers are likely to replicate the use of companies, ships and patterns of behavior found in previous weapons exports."[15] The data set covered 12 years and 22 recipient countries, some licit and documented, others undocumented. Each shipment event had a dozen attributes, which could be used for correlation and analysis modes.

[13] CIA, Center for the Study of Intelligence, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," Mar. 2009, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf.

[14] E. L. Waltz, *Information Warfare: Principles and Operations* (Norwood, MA: Artech House, 1998).

[15] Wallace and Mesko, The Odessa Network, 9.

Countries and shipments were determined by comparing lists of recipient countries to values of arms transfers from the Stockholm International Peace Research Institute (SIPRI) Arms Transfers and Military Expenditures databases, searching for international media coverage of shipment events (for those that were of sufficient size or nature to warrant international media coverage), and native-language local media coverage of the arrivals of shipments. This C4ADS data set drew heavily on unconventional open data sources such as photos posted by local Venezuelan military bloggers or Cambodian activists, of ships unloading weapons. Ship or owner names were determined from pictures or from searching for unique International Maritime Organization ID (IMOID) identifiers.[16]

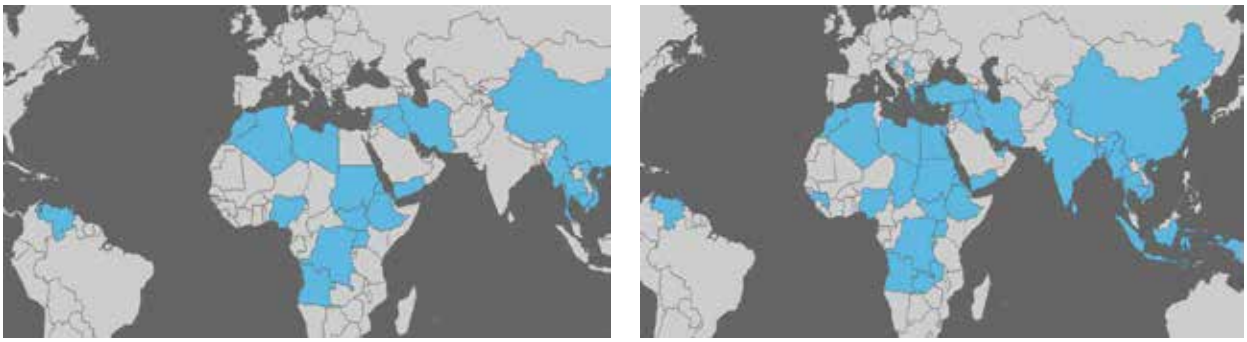
For example, some data on one shipment was obtained by locating several pictures on Phoenix Shipping's website showing various types of military equipment—including tanks and armored personnel carriers (APCs)—being loaded onto one or more unidentified ships. The tanks and APCs appeared to be loaded on the same ship. EXIF data revealed that the pictures were from October 15, 2003. The team cross-referenced SIPRI arms transfer databases for tanks and APCs delivered from Russia or Ukraine to a foreign customer for whom maritime transport would be necessary (i.e., not a landlocked neighbor such as Uzbekistan or Kazakhstan).[17]

"Out of sample" events are also analytically useful because they show the involvement of weapons transporters in moving other interesting cargoes. One event identified a ship that was also used for smuggling cigarettes into the UK.[18]

Confirm Data Set Usefulness

The next step is to determine whether the data set is useful. First, we need to determine whether the sampled data set is representative of a larger population under study. Because Russia exports to many more countries than the sample size in the report, the sample size at first appeared unrepresentative. But when the data was controlled for only those countries that would receive shipments by sea, based on geography or the type of weapons transferred, the set was acceptably representative.

Figure 11.1



Countries in our data set *All possible candidate countries*

Source: Wallace and Mesko, *The Odessa Network,* 31.

[16] Ibid., 12.
[17] Ibid., 14.
[18] Ibid., 19.

Build the Model

The data set was also examined for insights. First, the analysts looked at entities involved. This appeared to indicate direct government ownership and control of the weapons being transferred. The team cross-referenced weapons being sold with acknowledged state arms transfers. Only one event in the data set was clearly not under official control. The team also examined the possibility of selection bias. Heavy weapons of the type likely to be transferred by sea are easier for governments to monitor and likely harder to sell illicitly than small arms and light weapons (SALW). While no SALW incidents were detected, this remains a possibility.

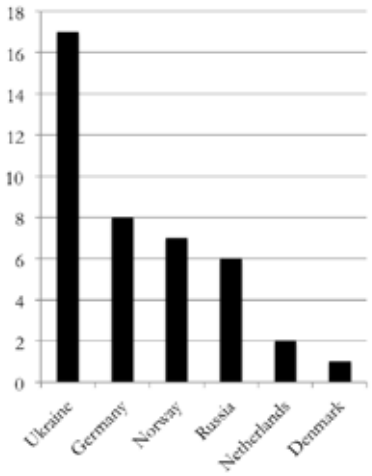
In the case of Russia, there is some ambiguity with the term "government control," which implies a unity of purpose among state agencies, and a distinction between private and public sectors, which may not exist in chaotic and corrupt political systems. The team determined that the involvement of official state weapons export agencies was the screening criterion to identify government control. With this definition, there is little evidence that private "lords of war" continue to sell major military hardware in the Putin era. In fact, examination of this alternate hypothesis uncovered draconian punishment for those who violated this norm. The Putin coalition of *siloviki* took back control of a large portion of the economy from the oligarchs after their heyday in the 1990s. And now "the facilitators of weapons exports are a critical element of domestic politics."[19] As the bridge between foreign customers and Russian producers, facilitators create the profits that are redistributed to regime stakeholders. This led the team to expect a strong connection between high-ranking Russian officials and shipment facilitators.

A small number of companies, based mostly in Ukraine and the EU, facilitate a high percentage of Russian and Ukrainian weapons exports. The chart and table below depict the salient roles played by some of these firms. This narrowing of the field led to some key research subquestions.

[19] Ibid., 33.

Figure 11.2 Shipment counts

Company	Country	Count
Kaalbye	*Ukraine*	*10*
Eide	*Norway*	*7*
Phoenix Trans-Servis	*Ukraine*	*4*
Briese	*Germany*	*4*
Westberg	*Russia*	*2*
Beluga	*Germany*	*2*
Spliethoff	*Netherlands*	*2*
Nortrop	*Ukraine*	*1*
Ukrainian Danube	*Ukraine*	*1*
Barwil Ukraine	Ukraine	1
FEMCO	Russia	1
North-Western	Russia	1
AnRussTrans	Russia	1
Balchart	Russia	1
Eckhof	Germany	1
Held Bereederungs	Germany	1
Clipper Group	Denmark	1



Source: Wallace and Mesko, *The Odessa Network,* 34.

Subquestions we answer in our discussion of the report's findings: Who are these companies and their key personnel? What qualities enable them to carry out so many arms shipments? Are these firms connected? How? Do some firms have a particular specialty?[20]

Second, the team examined location data and discovered that most shipments originated at the Ukrainian port of Oktyabrsk. This insight drove more subquestions: What is special about Oktyabrsk? What are the mechanisms for controlling and safeguarding the weapons? Since Oktyabrsk is in Ukraine, how does Russia ensure that its interests are met? These and other questions are answered in the discussion later in this chapter.

Examining the 12 or so properties of the events led not only to these insights and research subquestions, but also to insights into the more abstract activities that enabled the transfer of arms. The team grouped these into six geographic and functional clusters.

Figure 11.3 Odessa Network by location and function

Location	Entitiy	Function
Moscow and Kiev	goverment agencies	ownership of weapons
Odessa, Ukraine	shipping companies	AZ logistics integration
EU and Russia	shipping companies	specialized shipping services
Oktyabrsk, Ukraine	port and port authority	weapons loading
Africa and Middle East	private security companies	sensitive cargo protection
Latvia	banks	financial service

Source: Wallace and Mesko, *The Odessa Network,* 9.

20 Ibid., 33.

Test the Model: Syria

Since the team had now developed a threat process model for Russian arms exports, the next challenge was to apply it to a particular case for confirmation and refinement. Using the model as background knowledge, the team obtained Automatic Identification System (AIS) transponder data for all ports in Syria, Russia, and Ukraine from January1, 2012, to June 30, 2013.[21]

The team constructed a nearly complete log of commercial maritime traffic entering or leaving ports in these countries over the given time frame, complete with exact date, time, and location. Using the unique IMOID identifier for each ship, they cross-referenced the port call data set against ship registry records, allowing them to determine ship owner, manager, tonnage, flag, and so on. Given the byzantine financial and organizational arrangements used by the Odessa Network (including the use of shell, holding, and management companies that obscured ownership and control), this entailed significant investigative research. This was accomplished by using Palantir to integrate diverse data sets drawn from sources such as Ukrainian court records, SWIFT transaction receipts, Russian business directories, international shipping registries, and more. Once this combined database was complete, the team searched it for the "signature" of Former Soviet Union (FSU) arms shipments discovered through our analysis: ships owned or operated by companies with a track record of transporting Russian and Ukrainian weapons, transiting from Oktyabrsk, St. Petersburg, or Kaliningrad to Syrian ports such as Tartus, al-Ladhiqiya, and Baniyas.

The team added one more possible selection criterion: "AIS discrepancy." Ships can turn off their transponders, broadcast a false name or IMOID or Maritime Mobile Service Identity, or even "spoof" their signals to make it appear as if the ship were in an entirely different location or were an entirely different ship. Ships carrying Russian weapons to Syria, such as the MV *Katsman,* have turned off their AIS transponders, and Iranian vessels routinely spoof their signals.[22] The International Maritime Organization publishes lists of ships that are detected with these discrepancies, which were included in the database. Putting all this together, the team identified shipment events that match patterns of ownership and behavior seen in past Russian weapons shipments.

While it is impossible, using only open source and commercial data, to say exactly what cargo was contained in each of the above shipments, the key finding is that in 2012 and 2013, many ships from the Odessa Network left from known ports of origin for Russian weapons shipments and went directly to Syria or embarked on voyages that make sense only if large portions of their movements were obscured. The evidence (e.g., Syrian port calls by Odessa Network-linked ships, AIS discrepancies coinciding with known Russian seaborne arms shipments) presents a strong circumstantial case that these ships and companies are moving weapons or other sensitive cargo to the Assad regime. Bolstering this evidence is the fact that most of the interdicted and publicly reported Russian arms shipments were also carried out by members of this network.[23]

Mesko and Wallace had to address the alternate hypothesis that Syrian companies, instead of the Odessa Network, did the shipping. An assumption of their paper was that when the Russian or Ukrainian government sells weapons abroad, it (not the purchaser) coordinates the transportation of weapons, most often through the Odessa Network.

[21] Ibid., 67.
[22] Ibid., 67, fns. 344, 345.
[23] Ibid., 68.

While they believed this was the case for the vast majority of arms transfers, it was plausible that in some cases, the purchasing country itself would handle logistics. The two are not mutually exclusive. It could be that both Russia or Ukraine and the purchasing country handle different subsections of an overall arms transfer. For example, Kremlin-linked FSU facilitators might handle the highest-value (in both the military and financial senses) weapons and systems, while "native" facilitators from the purchasing country handle the lower-value weapons.

Interestingly, however, ships owned or operated by companies based in Syria or common intermediary countries (e.g., Lebanon and Egypt) made up a higher percentage of 2012 traffic at Oktyabrsk compared to other, busier Ukrainian ports, such as Odessa. The percentage of Syrian traffic at Oktyabrsk was significantly higher even compared to Nikolaev, just a few kilometers up the Bug River. Also, bulk grain carriers are, in fact, ideal for shipping large quantities of small arms; for example, court documents from the 2007 U.S. trial of legendary Syrian arms dealer Monzer al-Kassar show that he intended to use the grain carrier MV *Anastasia* to move thousands of assault rifles and grenades to the FARC in Colombia. It is, of course, possible that no correlation exists between an abnormally high percentage of Syrian ships loading cargo at a port that is the epicenter of Russian arms exports and then traveling to Tartus, and the continued flow of Russian weapons into Syria.[24]

The application of our understanding of the Odessa Network confirmed aspects of our model, brought to light additional potential indicators of illicit arms traffic, and identified alternative and competing hypotheses for exploration. The end result was a useful mapping of the Russian arms trade, in particular the Odessa Network.

The Odessa Network: An Informal Power Structure

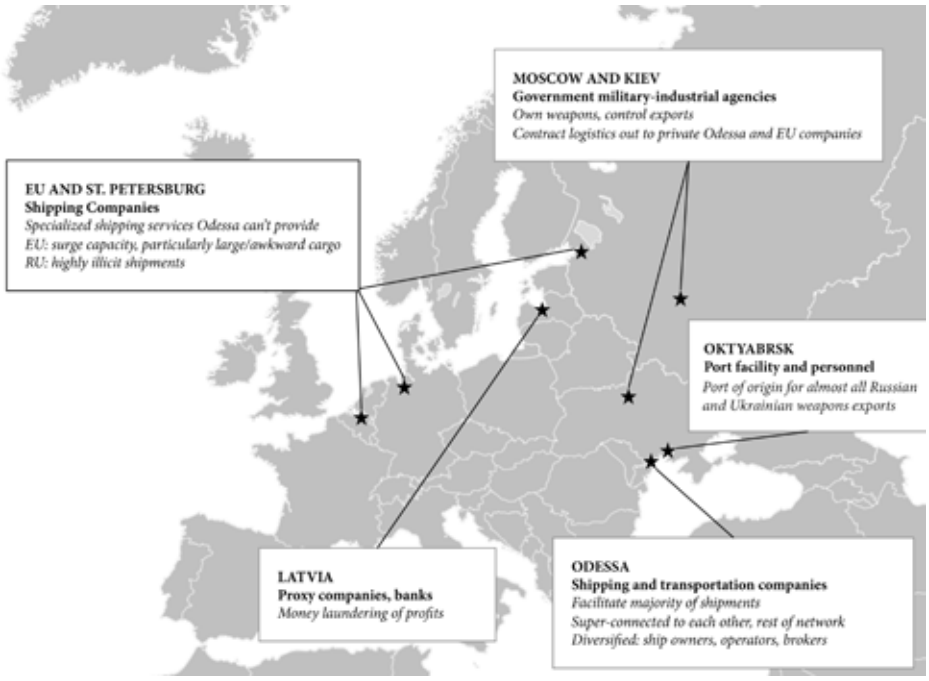
We have thus far avoided, as much as possible, the details of the report, which is readily available online at no cost. But some minimal detail is necessary to describe the utility of the report and its approach.

When we compared the number of known weapons shipments carried out by the Odessa Network facilitators and enablers to those carried out by unconnected facilitators, we could see that this network was responsible for the vast bulk of seaborne arms transfers in the data set. Thus, we can use common equipment, procedures, and locations used by these facilitators as a detectable "signature" of Russian and Ukrainian arms shipments.[25]

This signature includes logistics integration in Odessa, government connections in Moscow and Kiev, the Oktyabrsk port of origin, Russian and EU specialized services, African private security companies, and Eastern European financial services. What remained was for the team to further "pull the thread" and identify the key entities and their relationship to other facilitators and enablers. This produced the kind of detail that can enable effective interdiction, both kinetic and nonkinetic, depending on licit or illicit status of the target, strategy, available tools, and long-term objectives.[26]

[24] Ibid., 69.
[25] Ibid., 66.
[26] Sean F. Everton, *Disrupting Dark Networks* (New York: Cambridge Univ. Press, 2012).

Figure 11.4 Geographic and functional map of the Odessa Network



Source: Wallace and Mesko, *The Odessa Network,* 36.

End-to-End Logistics

One of the authors' critical insights, from which the report gets its name, was that a small group of firms based in Odessa seemed to be at the heart of the largest number of weapons exports in the data set, providing end-to-end logistics integration. This group, led by a large shipping conglomerate, was built on a bewildering set of connections between companies, family, former employees, schoolmates, and friends. Link and network analysis outlined these connections in stark relief. This network benefited from business diversification, external connectedness, and government connections.

Business diversification is a part of normal business strategies that include vertical and horizontal integration, used to expand market segment share, reduce supply chain costs, and offset local market risk. Most businesses generally have relationships with a wide variety of trusted subcontractors, and employees change jobs within the same industry and spin off other companies and suppliers. In the case of the Odessa Network, the side effect was to ensure that the network could execute sensitive contracts without routinely relying on services outside its control. And as Mesko and Wallace point out, handling expensive and sensitive cargoes bound for embargoed conflict zones or U.S. strategic competitors encouraged complexity in order to obscure the effort and reduce the chance of outside interference.[27]

In 1996, Igor Urbansky and Boris Kogan founded Kaalbye Group in Odessa. Weak governance, stockpiles of former Soviet weaponry, and foreign demand made Odessa a hub of international arms shipping in the 1990s. One trafficker, Leonid Minin, was a

[27] Wallace and Mesko, *The Odessa Network*, 36.

major broker of arms to Charles Taylor in Liberia, the RUF in Sierra Leone, and the Ivory Coast, and he even tried to sell an aircraft carrier to Turkey. While most shippers have a specific market niche, Kaalbye Group had a wide variety of subsidiaries, including Kaalbye Oil Services, Ukrainian Maritime Agency, Kaalbye Marine Service, and Kaalbye Shipping Cyprus. These companies provided crewing, chartering, freight forwarding, container and bulk shipping, project and heavy-lift work, and luxury yacht services.[28]

Shared personnel and connections across the industry indicate potential ties to a variety of external brokers and services, such as Phoenix Trans-Servis Shipping. Phoenix is a freight forwarding company specializing in defense-related cargoes. It had strong ties to government officials in Ukraine, and a work history with Kaalbye and EU ship-ping firms. Finally, Kaalbye frequently worked with companies such as Briese, a well-known German shipping company, and Tomex Team, led by Vadim Alperin.[29]

Alperin is a highly connected Ukrainian whose company managed the Kaalbye-owned MV *Faina,* which was seized by Somali pirates. His company was selected by Syrian businessman Youssef Hares, head of the Hares Group and partner to a number of FSU oligarchs. Hares recently leased a ship for trade with Libya.[30]

As the report indicates, this network was capable of taking advantage of any busi-ness opportunity, shipping both licit and illicit cargoes. While it was not within the report's purview to define any action by the network or supporting services as illegal or immoral, the report maps the links to the event data set and provides sources that support the authors' reasonable conclusions. Connections to key government officials in Moscow and Kiev were essential to making the weapons export line of business pos-sible.

[28] Ibid., 39, incl. fns. 143, 144.
[29] Ibid., 41.
[30] Ibid., 42.

Government Connections

The Odessa Network firms were not independent arms merchants. They were logistics contractors for the Russian and Ukrainian governments. State agencies such as Rosoboronexport and Ukrspetsexport owned the weapons and brokered almost all foreign sales. The Odessa Network companies played a critical role in making these arms transfers happen, but they did so only on behalf of powerful customers in Moscow and Kiev.[31] The key assumption was that there must be persistent links and contractual relationships between the Odessa Network and government officials.

Igor Levitin. Phoenix Trans-Servis is an Odessa shipping firm that has brokered multiple weapons shipments and openly advertises its connections to Russian and Ukrainian defense industrial concerns. One former Phoenix employee is Igor Levitin, who served as Russia's minister of transportation during 2004–12. He currently works as a personal adviser to Vladimir Putin and has served on the boards of directors of Sheremetyevo Airport and Aeroflot.[32]

Figure 11.5 Levitin and Putin

Igor Urbansky. Igor Urbansky, the founder of Kaalbye, served as deputy minister of transport in Ukraine from 2006 to roughly 2009. He enjoys extensive contacts among the Ukrainian defense establishment and the Party of Regions clique. Urbansky served as a captain in the Soviet cargo fleet before starting his first business, Evas, in Odessa in 1992. He went on to found Kaalbye Shipping. Urbansky was involved in the sale of Kh-55 cruise missiles to Iran and China in 2000 (in cooperation with corrupt Ukrainian and Russian intelligence officials) and in shipping military equipment to Angola in 2001. He was closely linked to military and intelligence figures in Ukraine. For example, in 2007, he personally paid for then-Minister of the Interior Vasily Tsushko, with whom he served in the Odessa Socialist Party, to be flown to Germany for medical treatment. The sophistication and quantity of weapons in deals personally attended to by Urbansky (e.g., cruise missiles) leaves little doubt of his connections to defense officials.[33]

[31] Ibid., 43.
[32] Ibid., 43, incl. fns. 190, 191.
[33] Ibid., 44, incl. fns. 199, 203, 204.

Boris Kogan. Boris Kogan was one of the cofounders of Kaalbye Shipping Ukraine and serves as a director and senior manager of the company. He was a close business partner of Kaalbye cofounder Igor Urbansky. Kogan was also on the board of directors of a Russian company, RT-Logistika. RT-Logistika is 51 percent owned by Russian Tech-nologies, the enormous state holding firm (headed by Putin's former KGB colleague and close ally Sergey Chemezov), which owns a variety of industrial companies, including Rosoboronexport and much of the Russian defense industry.

RT-Logistika is deeply involved in transporting weapons. For example, in October 2012, it arranged a cargo plane to transport sensory equipment for Syrian Pantsir SAM complexes from Moscow to Damascus, which the Turkish Air Force intercepted. Kogan was the only RT-Logistika board member who was not a senior Russian defense-indus-trial figure. Kogan personally knew and worked with some of the most senior defense-industrial figures in the Russian government. The company linking them, RT-Logistika, actively moved Russian weapons to Syria. The other company Kogan was involved with (Kaalbye) was by far the most frequent facilitator of Russian and Ukrainian weapons shipments.[34]Almost all the major Odessa-based facilitators were con-nected to organs of Russian and Ukrainian state power through personal connections. In addition to these connections, the port of Oktyabrsk in Ukraine stood out as the port of origin for the largest number of events in the data set.

Key Locations

The port of Oktyabrsk was the point of origin for almost all Russian and Ukrainian weapons exports in our data set. Located in the city of Nikolaev in Ukraine and specially

[34] Ibid., 45, incl. fns. 205, 206, 207.

built by the Soviet Union to ship weapons, Oktyabrsk possesses a number of qualities making it well suited for arms exports: advantageous geography, specialized equipment, transportation infrastructure to major FSU defense-industrial plants, and more. Russian state weapons export agencies maintain offices and personnel in Oktyabrsk. Moscow exerts significant control over the port despite its technically being in Ukraine. (The port's owner and operators had close ties to the Russian military and the Kremlin.)[35]

The economics of maritime transport make the time and distance savings of leaving from Oktyabrsk very significant. From a shipper's perspective, every extra mile and day of transit eats away profit—more fuel costs, more crew costs, and more time spent fulfilling a contract, when profitability often depends on fitting as many voyages as possible into a year.

Figure 11.6 Transit times, Oktyabrsk versus St. Petersburg

location	Algeria	Syria	India	Vietnam
St. Petersburg	19.9 days	28.2 days	36.9 days	44.6 days
Oktyabrsk	10.8 days	9.7 days	23.6 days	35.4 days

Source: Wallace and Mesko, *The Odessa Network,* 50.

Port manager Andrey Yegorov was born in Sochi (now part of Russia), served as a submarine commander in the Russian Navy Black Sea Fleet until 2000, and achieved the rank of captain. He graduated from multiple elite Soviet/Russian military academies and did not receive Ukrainian citizenship until 2000. Yegorov was reported to be a client of the Russian-Ukrainian oligarch Vadim Novinsky, the supposed owner of Oktyabrsk.[36]

The report did not identify any weapons shipments by Russian companies to Syria that did not originate in St. Petersburg or Kaliningrad. The C4ADS team suggested, as the reason for this anomaly, that perhaps both international pressure and a desire for a greater degree of control outweighed the purely economic considerations.[37] This indicates that special circumstances may lead to using companies outside the Odessa Network to transport arms.

[35] Ibid., 50.
[36] Ibid., 52, incl. fns. 233, 234.
[37] Ibid., 53.

Specialized Shipping Services

The Odessa Network could not provide all shipping services. Companies that provided recognized unique services were better suited to transport certain categories of arms due to size, port infrastructure, or political sensitivity.

Warship and submarine transportation: Eide Marine Services (Norway). Eide's distinction is functional, not political: its barge ships allow it to move large military cargoes that few others can. Eide does not need access to Odessa's political connections to find customers: given that it has moved military cargoes not just for Russia but also for the Canadian, U.S., and Swedish navies, it is fair to say that it is a service that sells itself. Thus, while Eide is an important logistics contractor for moving Russian weapons, it was not truly a part of the Odessa Network.[38]

Heavy-lift transportation: Briese, BBC, and others. A German firm, Briese Schiffahrts GmbH and Co. KG, is another transporter of Russian and Ukrainian weapons. Based in Leer, Briese is one of the largest shipping companies in Germany and among the largest heavy-lift shippers in the world, with a fleet of over 140 ships. Heavy-lift ships typically carry their own cranes and thus can move large, heavy, and unusually shaped cargo such as tanks and artillery. (Bulk carriers and normal cargo ships cannot.) Briese and other EU heavy-lift firms had an important functional role in the Odessa Network: heavy-weapons shipments to countries with poor infrastructure. The report outlined potential connections to a Kaalbye Shipping shell company, Primetransport Ltd. Briese's corporate structure highlights the complexities of this analysis.[39]

Figure 11.7 Briese corporate structure

Source: Wallace and Mesko, *The Odessa Network*, 56.

[38] Ibid., 54, incl. fns. 248, 249, 250.
[39] Ibid., 55.

Highly sensitive shipments: Balchart, Westberg, FEMCO, et al. Russian shipping companies appeared to play a small but significant role in the maritime export of FSU weapons. The data set showed only four arms transfers facilitated by Russian companies: three to Syria, and one to an unknown customer of sufficient interest that the U.S. State Department formally complained about the transfer. The C4ADS team found no weapons transfers facilitated by any Russian shipping company that were not highly illicit, whereas the Ukrainian and EU elements of the Odessa Network had plenty of licit shipments (e.g., to Vietnam and Venezuela). The second common feature among Russian companies shipping weapons was deep involvement by the Russian government. The authors postulated two tentative hypotheses: One, Russian shipping companies were more likely than non-Russian companies to be contracted by state weapons export agencies for illicit shipments. Two, they had particularly strong connections to the Russian government, including through the Odessa Network.[40]

Private Security

Odessa shipping companies appeared to own or employ multiple private maritime security companies (PMSCs), including Moran Security Group, Muse Professional Group, Helicon Security, Changsuk Security Group, and Al Mina Security Group. These companies' business model revolved around staffing ships passing through dangerous areas (particularly the Gulf of Aden and the Gulf of Guinea) with heavily armed FSU military veterans, who provided protection from pirates. Though hijacking is a threat for any shipowner, it is particularly troubling when the cargo is sensitive military equipment, as happened in 2008 when Somali pirates hijacked the MV *Faina,* a Kaalbye ship carrying Ukrainian weapons to South Sudan.[41]

Foreign observers, local media, and on-the-ground contacts have reported a growing number of Russian and Ukrainian private military security companies and arms dealers operating in war zones such as Somalia and the Democratic Republic of the Congo. FSU entities offer a wide range of services, acting as a one-stop shop for governments and militant groups alike to purchase weapons, mercenary services, trained pilots, and so on. Muse was active in Somalia, where a Somalia Monitoring Group report listed it as guarding ships entering and leaving Bosaso Port. Muse also worked with the Yemeni coast guard to contract services out to the highest bidder.[42] All these entities shared a need to transfer cash.

Financial Services

Russian and Ukrainian weapons are big business, both for the governments that export them and for the Odessa Network companies contracted as transporters. Russia exported over $17.6 billion in weapons in 2012, and Ukraine exported $1.3 billion worth in the same year. The Odessa Network company leaders facilitating these weapons flows

[40] Ibid., 58.
[41] Ibid., 60, incl. fn. 286.
[42] Ibid., 61, incl. fns. 306, 307.

earned significant profits. There was evidence that some of the Odessa Network companies employed Eastern European banks known for, or accused of, money laundering, and a series of Panamanian companies run by Eastern European nationals who acted as proxy directors. The analytical team found salient connections and "pulled the thread" to see what unraveled.[43]

The Odessa Network operated in a region of the world where financial crime is endemic, large-scale, and persistent. Russian and Ukrainian arms exports occurred in this context of massive and systemic financial evasion. There are functional reasons to launder money in arms shipping, particularly in concealing illicit arms transfers. Even licit transfers are sensitive to early disclosure, and many agencies are adept at "following the money" once they know where to look.[44] Illicit redistribution of national wealth to regime stakeholders was how United Russia and the Party of Regions maintained stability: they made collaborating with the state more profitable than challenging it. Money laundering also plays an important role in Russian foreign policy. A small but well-documented example is the Sluzhba Vneshney Razvedki's (Foreign Intelligence Service's) funding the election of a pro-Russian candidate in a Latvian mayoral election. The funds for this type of operation are not licit.[45]

Some FSU money laundering relies on proxy directors and shell companies. In this scheme, companies recruit people with no business qualifications to lend their names as directors to businesses located in offshore havens such as Panama, allowing the "real" owners to conduct business in virtual anonymity. One shell company can then be named a director of yet another new company, creating a daisy chain of shell companies facilitating anonymous financial transactions and obscuring ownership.[46]

The international banking system can be used to facilitate laundering and transfer of illicit income, even with reasonable compliance measures in place. A well-known bank in one country may have a correspondent relationship with a bank in another country, which shares an unknown relationship with a sanctioned bank in a third country, allowing ill-gotten gains to be accessed in the original country from a reputable financial-services provider. Banks and other financial-services providers expend significant effort seeking to avoid compliance challenges, and their due-diligence efforts can act as a form of early warning. Government agencies (while recognizing banks' need for legal certainty before sharing information) may want to investigate why a financial-services provider decides to sever a correspondent relationship. Even the most well-run and licit banks cannot share information with government agencies unless they are first immunized against legal action by customers, foreign governments, and even other government agencies due to privacy regulations. When they have such certainty, they could warn government regulators of the compliance risks that caused them to terminate a relationship with another financial services provider. The ability to prevent illicit gains from being transferred thru licit correspondent relationships is especially important since financial relationships are the glue that binds the network and its facilitators and enablers together.

[43] Ibid., 62, incl. fns. 308, 309.
[44] Ibid., 62, incl. fn. 317.
[45] Ibid., 63, fn. 320.
[46] Ibid., fn. 322.

Conclusion: The Need for a Comprehensive Approach

From the study of the Odessa Network, C4ADS identified postulates that enable the discovery of other illicit power structures. The research process is replicable and produces credible, useful insights. Finally, the insights provided in the Odessa Network report improve our understanding of the challenge of informal or illicit power.

The team derived the C4ADS postulates for discovery of illicit networks by examining the agents within the Odessa Network.

1. All illicit networks touch licit networks somewhere. The Odessa Network had a web of perpetrators conducting illicit activity, facilitators knowingly supporting that activity through licit and illicit activity of their own, and enablers unwittingly conducting licit activity that supported the perpetrators' and facilitators' actions. There is nothing inherently wrong with relationships forged in school, government service, business, or even prison. And yet, these bonds can create the trust necessary to bind an illicit or informal power structure.

2. To have an illicit capability, one must have a licit capability. In the Odessa Network case, the standard business motivations, processes, and assets involved in licit transportation of goods were mirrored and sometimes co-opted for illicit transport.

3. Human networks do not behave like mechanical networks. Human networks are resilient and cannot be broken. They are influenced and disrupted, but because they are biological and have unbounded connections to licit entities and activities, disruption is more difficult than with a minimum connected cut problem, such as efficient Allied interdiction of German rail networks during the Second World War.[47]

C4ADS created the right tool for conducting the kind of research required to understand an illicit power structure. The team then asked a research question that was relevant and built an event data set across a large enough time span to provide useful volume and variety. They examined the event properties for correlations, commonalities, and insight using descriptive statistics, geospatial analysis, and social network analysis. These insights were clustered into activity and location functions to describe a threat process model. The model was tested and further refined against a salient, related, current research subquestion. Throughout the process, alternative and competing hypotheses were examined for each of the relationships observed. C4ADS then presented the model in publication as a signature for a particular illicit power structure. This process, a variation on net-chain analysis, avoids the cultural-mirroring challenges that generally come from sensor-driven approaches that assume known functions. C4ADS has continued to refine the approach, build a larger data set of entities and relationships, train successive intern/analyst classes, and build best known practices with more interesting and useful open source and commercial databases in each new report.

[47] Alexander Gutfraind, Los Alamos National Laboratory, "New Models of Interdiction in Networked Systems," *MORS Phalanx 44*, no.2 (June 2011): 25-27. http://mmsengineering.ca/sasha-web/docs/gutfraind.phalanx.scan.pdf.

The Odessa Network highlights three key aspects of an illicit or informal power structure: government connection, key individual connectors, and financial services support. First, the network must have a relationship with local government. This can be a function of official sanction, poor governance, or official corruption. Next, key individuals act as super bridges connecting perpetrators, facilitators, and enablers, because illicit activity travels at the speed of trust. Finally, illicit activity generates significant income to sustain itself and requires the use of licit financial systems and regular business processes to hide, launder, and transfer resources.

Influencing or disrupting these informal and illicit power structures requires a sustained and comprehensive approach. Because of the unbounded nature of a human network, no single agency can have lasting impact. In *Disrupting Dark Networks,* Sean Everton provides a strategic matrix that includes kinetic and nonkinetic activities targeting the basic functional elements of an illicit power structure.[48] To take the strategic framework approach a step further will require a lead agency to identify outside agencies with the capacity, capability, and authority to act on the licit and illicit components, and provide those agencies with the information and motivation to address their portion of the problem set. Profit-motivated facilitators or enablers may be influenced through both kinetic and nonkinetic approaches. This will require analytical capability that recognizes more than geographic areas of responsibility, influence, and interest. For example, the Department of Defense would have to gather intelligence on domains of influence and interest, such as media, business, or finance, during times of peace. Informal and illicit power structures leverage these licit systems, thereby influencing diplomatic, informational, military, economic, and political elements of national power.

After publication of *The Odessa Network,* C4ADS was sued in U.S. court by a Ukrainian shipping conglomerate and, more recently, an Eastern European bank. The prestigious Washington law firms these companies chose as enablers, containing well-known American lawyers and politicians, have represented other affiliated known and allegedly illicit international clients. In this case, under the Washington, DC, Anti-Strategic Lawsuits Against Public Participation statute, the decision, with prejudice, in favor of C4ADS set several precedents and resulted in yet more illicit activity being read into the public record.[49] Rather than having the intended chilling effect, this effort at "lawfare" has highlighted just what a threat today's open source intelligence is to these illicit power structures. Once chided in intelligence circles as being static, irrelevant background information that produced no data advantage and could easily be deception, open source is fast becoming the main source of credible and useful intelligence. While Naval analysts have long thrown away the classified red book in favor of *Jane's Fighting Ships,* the use of now readily available and searchable public records, appropriate data sets and analytical approaches, and emerging data management tools throws the classified intelligence community on its ear, making old priorities, techniques, and access

[48] Sean F. Everton, *Disrupting Dark Networks* (New York: Cambridge Univ. Press, 2012).

[49] Superior Court District of Columbia, *Center for Advanced Defense Studies v. Kaalbye Shipping International et al.,* 2014 CA 002273, Apr. 7, 2015, http://dcslapplaw.com/files/2015/04/C4ADS_Superior_Court_Opinion.pdf.

controls obsolete and even counterproductive.[50] We should, however, expect bureaucratic resistance to real reform. Cramming effective responses to this paradigm shift into the same old organizational and personnel frameworks would not be easy, since our own networked power structures are also resilient. But the intelligence community can emphasize exploitation of open source data over classified approaches, integrate hypothesis-driven analytical methodologies, and support a network of strategic partnerships with innovative nonprofit organizations.

[50] Author interview with Capt. (Ret.) Peter O'Brien, USN, former director of fleet intelligence, DIA, Mar. 2015, Washington, DC; HIS, *Jane's Fighting Ships,* Aug. 13, 2015, https://www.ihs.com/products/janes-fighting-ships.html.