Data As Light on the Gray: Mitigating FOCI in the Supply Chain

By

J.A Sheppard, Justin Olmstead, Blake Howald, Matt Machado

In most everyday contexts, 'gray zone' means 'in between' or 'almost but not quite'. When the term, 'gray zone' is applied to interstate conflict, however, things get weird. Gray zone warfare popularly refers to hostility that is below the threshold of armed conflict. Others simply prefer to put it under the flag of ambiguity. These views are nevertheless odd because they amount to saying that gray zone warfare is in between war and peace. It is like trying to imagine a boxing match where the fighters are almost punched in the nose but not quite. Among the more pragmatic analysts who realize that there is nothing ambiguous about things like stolen intellectual property, gray zone warfare is really a problem of antiquated laws that are ill-suited to the crimes, *e.g.* almost but not quite prosecutable transgressions. Finally, gray zone warfare may have less to do with an adversary's genius for aggression and relate more to structural problems in societies that are slowed by consensus building and bureaucratic boundaries that separate different national instruments of power. In other words, almost military, not quite law but somewhere in between those and diplomacy. All of this has amounted to a lot of time and money being spent on how to detect and

deter an elusive kind of conflict that is almost war but not quite. It is a nice academic exercise. What is weird about it is that it is probably overkill. Designing effective deterrence for an almost but not quite hostile actor seems unduly complicated compared to simply removing the real potential for gain, *i.e.* denial. In the softer world of gray zone warfare, one way to do this is to use the emerging tools that can shine a light on a network and identify the relationships that contribute to gray zone activity. Since qualitative and quantitative analysis can provide consensus about whether a threat exists, and how sever it might be, it makes sense to use those tools to identify likely targets and then harden them before they fall under foreign influence and control.

The Fog of War

Stripped of all of its mystery, gray zone warfare is little more than activity by which a nation tries to achieve its goals through incremental gains and usually in ways that are underhanded and not physically violent. This basic gist is what led Dr. Frank Hoffman sometime ago to describe gray zone warfare to the House Armed Services Committee as 'salami slicing' strategies. It was a perfectly apt illustration but presumably the image of hospitably preparing a snack led some to conclude that the intent behind gray zone warfare activity is not tied to the

project of regime change. Rather, as often expressed, the gray zone is filled with strategic competitors who seek to change the *status quo*. That does sound nicer but it glosses the reality that the imposition of political will is still at the heart of the struggle. So, at the risk of being a bit gruesome, perhaps thinking of gray zone warfare as akin to *Lingchi*, 'death by a thousand cuts' solidifies the point. Indeed, the main components of humiliation, dismemberment over a long period of time, and ultimately the death of an enemy tracks well with traditional elements of warfare that include enmity, infliction of damage, and the submission of an adversary. Rather than slice away the flesh of a condemned prisoner, however, gray zone warfare whittles away at the body politic using covert, often illicit, means that are present in most any war.

In the world of economic espionage, the cuts and slices often look like normal business transactions. For instance, the scuttled attempt by a group of Chinese investors to take over the chipmaker, Lattice Semiconductor Corporation, is well-known. On the surface, that deal had the appearance of a straightforward acquisition. Through a federal review, however, the buyer was found to have backing from the Chinese government-controlled China Venture Capital Fund Corporation. The implication was that the proposed buyer, Canyon Bridge Capital Partners, was essentially a front organization for the Chinese government to both

acquire intellectual property and assert more control over the U.S. supply chain for computer chip technology. Gray zone warfare can also involve non-state actors who may not fully grasp the larger goal for engagement with an adversary. Chong Sik Yu, the President of America Techma, Inc., who was arrested for exporting prohibited electronic components that were listed on the U.S. Commerce Control List may fit that profile. Indeed, he may have been driven more by profit and/or a general sense of Chinese nationalism than a desire to displace the U.S. in the global technology market. The point is that these events, and many others like them, can be viewed in isolation as discrete criminal activity but, at the same time, they also fit neatly into a picture in which sensitive material is acquired in order to benefit a foreign government. Before giving into the notion that such instances are acts of economic espionage but not quite, it is perhaps prudent to abstract from the examples and simply dial into the concern that they suggest that China, and other countries that use similar means, seek to gain control of goods in order to undermine reliable access to the supply chains that ensure the U.S.'s strategic advantage.

To address that concern, a number of recent publications, including the most recently released National Defense Strategy, call for deterrence as the best route for 'reducing a competitor's perception of the benefits of aggression

relative to restraint'. Such an approach is misguided. To be sure, at a minimum, deterrence requires at least some shared understanding about the use of force in order to compel an adversary to change course. It also requires that such force be delivered swiftly and with certainty. Yet, most of the literature related to gray zone warfare clearly implies that that gray zone warfare depends on the stability of that shared understanding in order to operate below it. Moreover, since effective deterrence demands a firm and speedy response, aggressors deliberately undermine those elements through actions that cause risk confusion and provide deniability. Simply put, gray zone warfare works precisely because its activities are performed with the limitations of deterrence in mind.

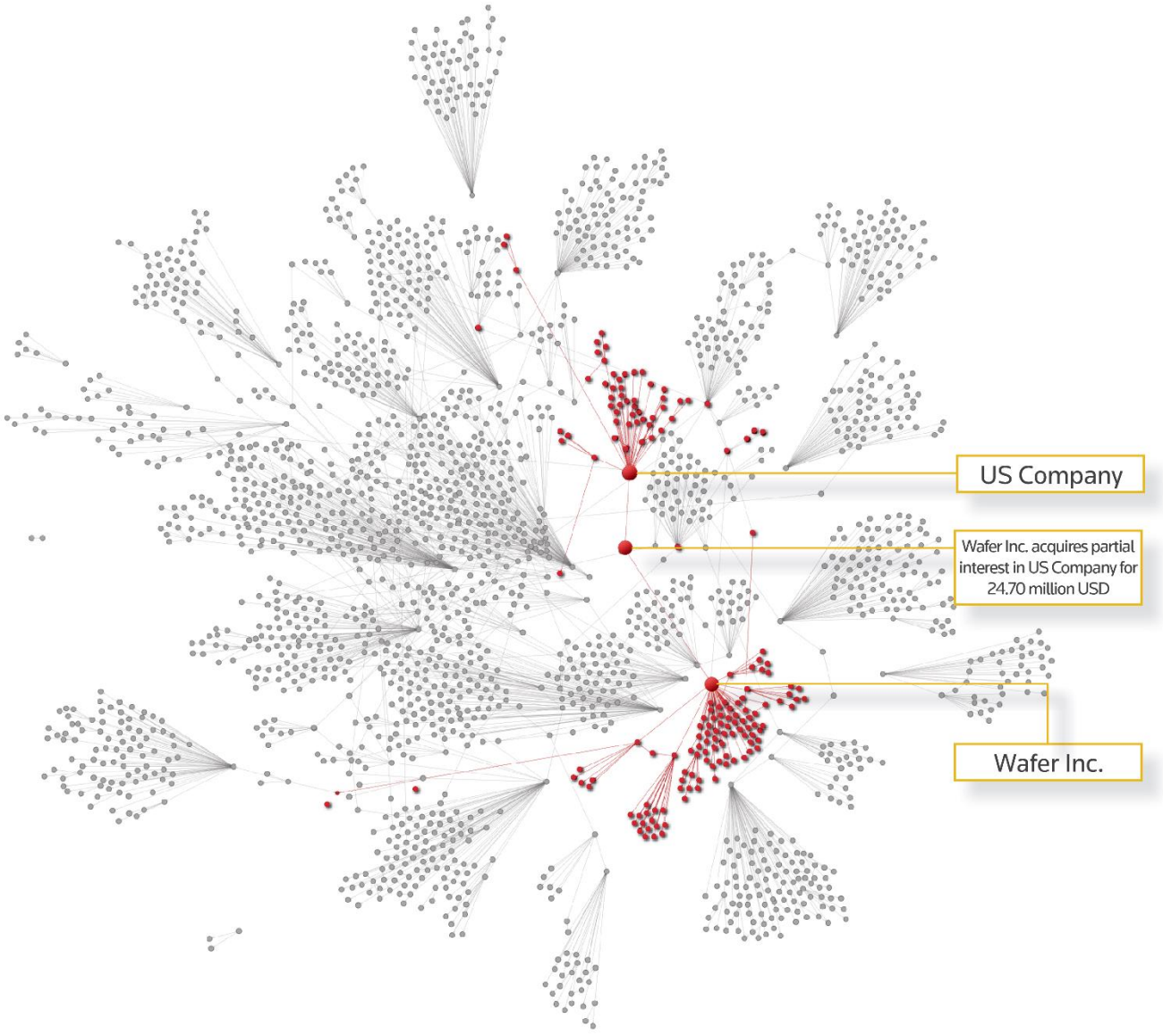
Anti-Access

Although the activity that is commonly associated with gray zone warfare is mismatched to deterrence, it can be curtailed by anticipating the threats. Put more concretely, from a gray zone aggressor's point of view the intention behind dodgy activity is to induce misperception and, at the same time, prevent a target nation from discovering the true objectives (*maskirovka*, for the Soviet historians). This is the basic anatomy of what is known as deception and denial and, as students of the late and greatly esteemed Barton Whaley know, countries engage in it because it works. An effective antidote to such practices, however, is

anti-access. That is to say, stopping a foreign aggressor is often a matter of anticipating the threats and then engaging in activities and programs that neutralize the effectiveness of the nefarious efforts. Putting the required obstacles in place to protect things like trade secrets, IP, and the links and nodes within a supply chain is tricky business, however. On the one hand, the attacks are instigated by civilians who are often state-supported and/or state-encouraged which makes the agenda for gray zone warfare especially difficult to detect. Indeed, like a well-written computer virus, the attacks often bear the signatures of legitimate business deals but the events prove otherwise. On the other hand, the onus for anticipating and blocking attacks falls on industry which, usually as a matter of resources, does not actualize counter-measures with the speed that the threat demands. Nonetheless, there are ways to share that burden while continuously monitoring the business environment for potential gray zone activity. Forewarned is forearmed, as the old adage goes, and a good threat assessment can deliver the necessary information for stopping potential operations that could lead to the foreign influence and control of a company or a supply chain.

A Light in the Fog

One way to get ahead of gray zone warfare type aggression is to understand and analyze a wide scope of empirically based potential threats. Indeed, a data-based network can provide a temporally static canvas for seeing what entities and relationships exist in data relative to entities and relationships of interest and a given threat. So, for example, an illustration of the proximate threats to a company in the defense industrial base would look like this:



This network visualization is comprised of points, or nodes, which represent *entities* (e.g. people, companies, places, etc.) and lines, or arcs, which represent *relationships* between two points, *e.g.* headquartered in, supplied by, ships to, *etc*. Both the entities and the relationships are extracted from multiple data sets such as SEC filings, disclosures, news articles, proprietary and open source data sets and is a partial representation of the semi-conductor industry. The engineering that is required to build such networks with precision is a subject for a different article. Suffice to say here, however, that quite a bit of care is devoted to data quality and confidence and, when overlapped with expert analysis, the picture provides a good sense of the way that things really are.

The above picture does contain just over 2,000 entities comprised of corporations, corporate offices, economic deals, and their relationships in the semi-conductor industry. Both that number and type of entities and relationships can be adjusted to any industry and to any kind of threat that needs to be analyzed. For purposes of this discussion, however, what is represented is an actual company in the US semi-conductor industry and the number of entities is enough for illustrative purposes. Also, it is worth noting that within the data graph is a foreign corporation that is labeled, “Wafer Inc.” It too is a real company but that label should be a fairly obvious signal that all company names

have been changed to protect their corporate identities which, perhaps ironically is a wee bit of deception on our part. Nevertheless, changing the names does not hide the salient fact that Wafer, Inc. has a relationship to US company through a roughly $25 million-dollar, partial acquisition.

The size of Wafer's stake in the U.S. Company is significant but the question is whether or not the investment is an instance of an attempt at foreign influence and control in the semi-conductor industry. That is a hard question to answer because a cursory exploration of the foreign company shows that it deals in more than just semiconductors. Indeed, Wafer Inc.'s previous financial investments Include everything from UK-based virtual reality companies to European audio technology firms. Wafer had also completed multiple domestic financial transactions in Chinese electronics and robotics firms. To complicate things further, it is also associated with more than 35 corporate individuals, mostly foreign nationals, with little known about their other corporate affiliations or influence. Simply put, the broad nature of Wafer's business activity and its expanding industry portfolio makes it difficult for US authorities to easily assess the risk Wafer Inc. could pose to the broader US Semiconductor industry. Turning a blind eye to the complexity of that company, however, is not an option because waiting for an unfriendly agenda to reveal itself at the end of what appeared to be

otherwise normal business practices is equal to a failure to identify a harmful technology acquisition within the cloud of greater industry activity.

There is one more complication to note: business isn't static. Put more fully, making risk assessments while keeping pace with greater industry activity is challenging. In a three-month period, an additional 43 new companies, people, and corporate financial transactions, along with an additional 52 new identified relationships, were observed in our China-US Semiconductor industry graph. Each of these new nodes would need to be analyzed for risk of influence or technology transfer to the US Semiconductor industry in order to get ahead of a potential gray zone threat. Data Science and technology can assist with the collection, processing, and prioritization of the information but, as suggested above, human expertise is ultimately needed for distinguishing between benign and possibly malignant business activities. Presumably, that is where US Authorities step in to make the risk determinations. For example, the appropriate agencies would need to assess the nature and degree of influence a company like Wafer Inc. would have over US Company; whether it is potentially disruptive to US Company's operations, market share, and price; whether it is potentially disruptive to the semi-conductor supply chain in general and whether there are any other

connections that are further removed that are nonetheless potentially, albeit indirectly, disruptive.

Access Control

It is always easier to spot the difference between normal, above-board acquisition and potential economic espionage after the fact. The ideal, however, is to see the activity in a number of spheres prior to the espionage occurring and then taking the right action ahead of time in order to deny improper access in the operational area. Through data analysis, it is possible to identify what is a threat and what is not. By looking at an adjudicated case, *i.e.*, a case that is known to be dodgy, and breaking down its elements, it is possible to see what is true across most business activities and then use that as a kind of barometer that can indicate the severity of potential threats. Additionally, a balanced, well-executed, combination of qualitative and quantitative analysis can lead to a quick consensus about what to do about any threating activities that emerge.

Effective denial through the use of data is one means to shining a light on FOCI in the gray zone. Better information provides corporations, and in particular those working with the US government, a level of assurance that their business partnerships fit within the parameters of normal commerce. Strategically, it also makes more sense to deny adversaries the opportunity to insert themselves in

the US defense supply chain than it does to give them the freedom to act on their own levels of risk aversion. To be blunt, being ready to deny an adversary's hostile entry into a business transaction is better than trying to persuade that adversary not to engage economic espionage. Continual monitoring of the business environment allows for the early identification of potential vulnerabilities that aggressors seek to exploit and it offers a better platform from which to blunt the detrimental, albeit incremental, gains that come from waging gray zone warfare.