A Resilience Framework for Understanding Illicit Nuclear Procurement Networks

AARON ARNOLD[1]

Abstract

Current approaches to global supply-side controls to curb the proliferation of nuclear dual-use goods and technologies fail to consider the mechanisms that drive non-state actors to adapt and innovate. Consequently, policymakers are left reacting to, rather than anticipating, new illicit procurement techniques and methods. This article proposes a new analytical framework based on the concept of resilience, which considers how illicit procurement networks change and adapt within environments characterized by risk and uncertainty. That is, how do internal and external drivers help to insulate or create vulnerabilities for procurement networks? Focusing on the causes and consequences of resilience offers a more dynamic and comprehensive picture of illicit procurement because the concept can account for how networks adapt to supply-side policies and vice versa. To further illustrate this framework, this article explores three cases of illicit nuclear procurement. Finally, the conclusion examines the possible implications for future global supply-side policies to control the spread of nuclear dual-use goods and technologies.

Keywords:

Counter-proliferation, illicit procurement, resilience, nuclear

1 Aaron Arnold is an Assistant Professor at Curry College in Milton, MA. He is also an Associate at the Project on Managing the Atom, at Harvard University's Kennedy School of Government. Aaron spent ten years as a nonproliferation and counter-proliferation consultant to the United States Department of Defense, Department of Homeland Security, and the Department of Justice. His work primarily focuses on nuclear proliferation, threat finance, and sanctions evasion.

Introduction

Despite the successful conclusion of a nuclear agreement with Iran in late 2015—a deal that limits Iran's nuclear program in exchange for sanctions relief—the illicit global trade in nuclear and missile technology remains an active and ongoing concern. Globalized commerce, increased access to dual-use goods, growing indigenous manufacturing capabilities, and persistent demand for missile and nuclear technology have produced a niche market for middlemen to act as conduits between supplier and proliferator states.[2] Yet, despite global efforts to control the spread of dual-use goods and technologies, procurement networks are often able to operate under the radar of intelligence and law enforcement organizations. Iranian procurement networks, for example, were largely able to evade global efforts to limit Iran's nuclear enrichment program to increase its number of gas centrifuges, all while under strict international economic sanctions and virtually cut-off from the global financial system.[3] It should be noted, however, that while Iran was able to increase its number of gas centrifuges, the country was not able to make significant scientific progress on improving its uranium enrichment program, and generally continued to use the outdated IR-1 centrifuge design. Nonetheless, what explains the apparent persistence and success of nuclear procurement networks to continue operations given the increased attention to strengthening global supply-side controls?

The overall strategy of nuclear supply-side controls is to curb the transfer of "difficult-to-produce technology and equipment that is essential for making nuclear weapons and intended by the purchaser for that purpose."[4] This includes limiting trade in materials with both nuclear and non-nuclear applications, the timely detection of proliferation-related activities, dissuading proliferating-related activities, and disrupting or denying proliferation-related activities when

---

2 Bruno Gruselle, "Proliferation Networks and Financing," Fondation pour la Recherche Stratégique, Paris, 2007, p. 7, <http://www.stanleyfoundation.org/publications/working_papers/Delory5.pdf>. See also Matthew Bunn, Marty Malin, William Potter and Sandy Spector, *Preventing Black Market Trade in Nuclear Technology* (Cambridge: Cambridge University Press, forthcoming).

3 In 2006, the UN Security Council adopted resolution 1737, which banned exports to Iran of "all items, materials, equipment, goods, and technology" related to nuclear activities. The Security Council expanded this ban in March 2008 to include travel sanctions on specific individuals, as well as nuclear-related sanctions on entities affiliated with Iran's nuclear program. Finally, in June 2010, the Council imposed its most restrictive sanctions against Iran with resolution 1929, which prohibited Iran from investing in foreign nuclear activities, banned weapons exports to Iran, called on member states to inspect all cargo to and from Iran, expanded the list of sanctioned entities, and finally, called for states to implement additional financial-related sanctions. Despite these restrictions, Iran made progress on its nuclear enrichment program. In 2003, for example, Iran maintained a few hundred centrifuges, but by 2013, experts believed Iran's number of centrifuges had grown to over 19,000. Many of the items Iran procured, like carbon fiber, valves, and aluminum tended to be below-threshold items, which made it difficult for authorities to "identify links between below-threshold items and prohibited end-users and end uses in Iran." See, "Final Report of the Panel of Experts Established Pursuant to resolution 1929 (2010)," United Nations Security Council, June 2014, pp. 14–15, <http://www.un.org/ga/search/view_doc.asp?symbol=S/2014/394>; "Visualizing Centrifuge Limits Under the Iran Deal," *Nuclear Threat Initiative*, June 25, 2015, <http://www.nti.org/analysis/articles/visualizing-centrifuge-limits-under-iran-deal/>.

4 Matthew Bunn, Marty Malin, William Potter and Sandy Spector, *Preventing Black Market Trade in Nuclear Technology* (Cambridge: Cambridge University Press, forthcoming).

they occur.[5] These approaches, however, fail to account for the ability of procurement agents and networks to adapt. A motivated network will find ways to circumvent even the most rigorous controls. For the purposes of this article, a procurement network is taken to mean the networks of middlemen that either wittingly or unwittingly illicitly procure nuclear dual-use goods and technologies on behalf of a state. These networks can vary in size, scope, and sophistication; may be comprised of one or more members; and organized as a formal, business-like partnership, such as the A.Q. Khan network, or more informally, based on familial relationships. Iran, for example, has tended towards de-centralization with respect to procurement activities.[6] North Korea, on the other hand, has generally maintained a strong, centrally-directed network of procurement operations.[7] This definition is somewhat broader in scope than other definitions, which tend to focus on the state, its intentions, and its direct interactions with other proliferation aspirants.[8]

Interestingly, while supply-side controls make up a significant portion of the global nuclear nonproliferation regime, relatively little attention is given to the inner-workings of the procurement networks. Consequently, supply-side controls have trouble anticipating how procurement networks will adapt. This is not to imply that the controls are static. On the contrary, there is a clear evolution of global supply-side controls that has adapted to changes in the spread of nuclear goods and technologies. In response to India's 1974 nuclear weapons test, for example, nuclear supplier countries formed the Nuclear Suppliers Group (NSG) to develop and issue guidance on limiting the export of sensitive nuclear materials and technologies. Although the NSG is an informal multilateral export control arrangement between nuclear suppliers, with no legal authority or formal enforcement mechanisms, its participating governments have implemented its guidelines through national laws and practices. During the 1980s and 1990s, the United States called attention to the NSG's lack of specific guidance on controlling the exports of dual-use goods and technology (i.e., goods that have both nuclear and non-nuclear applications).[9] It was eventually the revelations of Iraq's covert nuclear program that helped

---

5 Andrew C. Winner, "The Proliferation Security Initiative: The New Face of Interdiction," *The Washington Quarterly* 28:2 (March 1, 2005), pp. 129–43; Frederick McGoldrick, "Nuclear Trade Controls: Minding the Gaps," CSIS, Washington, DC, January 2013, <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130122_McGoldrick_NuclearTradeControls_Web.pdf>.

6 For a short history of Iran's procurement activities, see, "Final Report of the UN Panel of Experts Established Pursuant to Resolution 1929 (2010)," S/2014/394, Annex II, June 2014, <http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2014_394.pdf>.

7 For a recent discussion on the scale and scope of North Korea's procurement operations, see John Park and Jim Walsh, "Stopping North Korea, Inc.: Sanctions Effectiveness and Unintended Consequences," MIT Security Studies Program, August 2016, <http://web.mit.edu/ssp/people/walsh/Stopping%20North%20Korea%20Inc_Park%20%20Walsh_FINAL.pdf>.

8 Chaim Braun and Christopher F. Chyba, "Proliferation Rings: New Challenges to the Nuclear Nonproliferation Regime," *International Security* 29:2 (October 1, 2004), pp. 5–49; Alexander H. Montgomery, "Ringing in Proliferation: How to Dismantle an Atomic Bomb Network," *International Security* 30:2 (October 1, 2005), pp. 153–87.

9 For further discussion of dual-use goods and technologies, see, "Communication Received from the Permanent Mission of the Republic of Korea to the International Atomic Energy Agency Regarding Certain Member States' Guidelines for Transfers of Nuclear-Related Dual-Use Equipment, Materials, Software and Related Technology," Information Circular, International Atomic Energy Agency, October 24, 2016.

usher in new NSG guidance on controlling dual-use technology.[10]

Later, responding to the threat of potential nuclear terrorism, the UN Security Council unanimously adopted resolution 1540 in 2004, which requires UN Member States to prohibit any support to non-state actors seeking WMDs, adopt and enforce laws that criminalize the proliferation of WMDs to non-state actors, and establish domestic controls over nuclear-related technologies, goods, and services.[11] While some states moved quickly to adopt and implement new supply-side controls, others still lag.[12]

The picture of global supply-side controls that begins to emerge is one that is left reacting to, rather than anticipating, nuclear procurement. Moreover, as export controls change and enforcement tightens, procurement networks iteratively change and adapt. That is, even as states moved to strengthen these controls globally, whether through interdictions, export control regimes, or sanctions, procurement channels and networks adapted. Middlemen have adopted a range of techniques and methods to hide their illicit activities, including transshipment through a third-party country, targeting countries with lax export controls to set up operations,

---

10 Fred McGoldrick, "Nuclear Trade Controls: Minding the Gaps," A Report of the CSIS Proliferation Prevention Program (Washington, DC: Center for Strategic and International Studies, January 2013). One of the key issues with dual-use technologies is its ubiquity among both nuclear and non-nuclear states. This, of course, is quite problematic for supply-side controls that mainly focus on controlling goods and technologies from supplier states. R. Scott Kemp argues, for example, that technology once thought to be "exotic" is now commonplace and accessible to even the most unsophisticated proliferation aspirants—either through indigenous capability or clandestine procurement. The implication, of course, is that policymakers should look beyond supply-side controls to the "cultural, normative, and political organization of the world" in order to reduce demand. Yet, despite Kemp's compelling argument, some proliferation aspirants, like Iran and North Korea, relied heavily on procuring complicated foreign technology, even when they had the capability (and opportunity) to indigenize. In the case of Iran, for example, Kemp argues that A.Q. Khan's contributions to Iran's gas centrifuge program in the late 1980s was insignificant. Interestingly, although Iran mastered the P-1 gas centrifuge design, the country continued to covertly procure foreign materials and parts. This, despite relatively sophisticated indigenous manufacturing. In other words, Iran may have viewed supply-side controls (including economic and financial sanctions) as so weak and incapable, that they posed no real threat to the advancement of its nuclear enrichment program. See, R. Scott Kemp, "The Nonproliferation Emperor Has No Clothes," *International Security* 38:4 (April 1, 2014), pp. 40–41.

11 In May 2003, then President George W. Bush announced the Proliferation Security Initiative (PSI), which seeks to enhance global coordination and collaboration with respect to WMD trafficking. More specifically, the initiative focuses on ensuring that participating countries have the national legal authorities to prohibit and prevent WMD proliferation, the ability to inspect and identify proliferation-related cargo, the ability to seize and dispose of interdicted materials and technologies, and the mechanisms in to ensure swift decision-making. Less than five months after its launch, in October 2003, the PSI had its first successful interdiction of a German-owned cargo ship carrying components for 1,000 centrifuges destined for Libya. It was this interdiction that began to unravel the extent of A.Q. Khan's network, and put into question the efficacy of global export controls. See "Chronology: A.Q. Khan," *The New York Times*, April 16, 2006, <http://www.nytimes.com/2006/04/16/world/asia/16chron-khan.html>.

12 "2016 Comprehensive Review: Background Paper for the Formal Open Consultations by the 1540 Committee," United Nations, New York, NY, June 22, 2016, p. 4, <http://www.un.org/en/sc/1540/pdf/CR-June-Consultation-Background-Paper.pdf>. Although the prevailing wisdom was that compliance with nonproliferation norms was a function of cost and the unequal distribution of benefits, Stinnett et al., for example, explain that states' non-compliance with UNSCR 1540 is more closely related to bureaucratic and economic capabilities, rather than national security interests. See, Douglas M. Stinnett et al., "Complying by Denying: Explaining Why States Develop Nonproliferation Export Controls," *International Studies Perspectives* 12:3 (August 1, 2011), p. 323.

obfuscating payments, forging end-user certificates and export licenses, and procuring "below threshold" components that may suffice or be upgraded by the recipient.[13] Part of A.Q. Khan's success, for example, was his ability to adapt procurement methods to evade scrutiny from both law enforcement and intelligence agencies worldwide. This included compartmentalization of key activities, the use of front companies, increasing the number of intermediaries, creating fraudulent end-user certificates, and conducting business through corrupted banks to obscure payments. For at least a while, Khan's nimble and adaptable network proved to be quite an obstacle for global export controls meant to curb illicit nuclear procurement.[14]

Counter-proliferation policies have evolved in such a way as to emphasize procurement *modus operandi* rather than underlying processes that may influence the *way* a network adapts and changes. Interestingly, the techniques and tactics that nuclear procurement networks use have changed very little. In fact, a 1984 de-classified US intelligence assessment on gray market nuclear materials highlights the frequent use of front companies, falsification of end-user certificates, alteration of information listed on export applications, and transshipment through third-party countries with lax export controls.[15] These methods are nearly identical to those described by the UN Panel of Experts' report on the implementation and violations of UN Security Council resolution 1929, which imposed stiff sanctions and embargoes on Iran.

This is not to suggest that addressing procurement methods is unimportant. On the contrary, a deep understanding of illicit procurement methods and techniques is necessary to close gaps in global export controls and strengthen enforcement mechanisms. Consider, however, the problem of proliferation financing—that is, the financing of illicit nuclear procurement. Unlike terrorist financing or money laundering associated with narcotics trafficking, proliferation financing often resembles normal trade finance—practically undetectable from the perspective of the financial industry.[16]

---

13 David Albright, Paul Brannan, and Andrea Stricker, "Detecting and Disrupting Illicit Nuclear Trade after A.Q. Khan," *The Washington Quarterly* 33:2 (April 1, 2010), pp. 85–106.

14 It is important to note that the Khan network was an outlier of sorts when compared to other states' entrenched procurement networks. Iran, for example, has demonstrated a keen ability to take a distributed approach, where its procurement agents rely extensively on middlemen located overseas—mostly in China. In these networks, illicit procurement revolves primarily around evading export controls, with little actual nuclear know-how. North Korea, on the other hand, uses an approach that more closely resembles a version of the A.Q. Khan network in terms of scale and complexity. In a recent study, John Park and Jim Walsh describe the complex and tangled system of "state trading companies," which the North Korean regime uses to conduct both licit and illicit procurement. See John Park and Jim Walsh, "Stopping North Korea, Inc.: Sanctions Effectiveness and Unintended Consequences," MIT Security Studies Program, August 2016, <http://web.mit.edu/ssp/people/walsh/Stopping%20North%20Korea%20Inc_Park%20%20Walsh_FINAL.pdf>.

15 "The Gray Market in Nuclear Materials: A Growing Proliferation Danger," An Intelligence Assessment, Washington, DC: Central Intelligence Agency, Directorate of Intelligence, July 1984, <https://www.cia.gov/library/readingroom/document/cia-rdp85t00287r000600940003-2>.

16 For a discussion of proliferation financing, see Sonia Ben Ouagrham-Gormley, "Banking on Nonproliferation," *The Nonproliferation Review* 19:2 (July 1, 2012), pp. 241–65; For an industry perspective of proliferation financing, and analysis of current issues with global counter-proliferation financing policies, see Emil Dall, Andrea Berger, and Tom Keatinge, "Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance," Royal United Services Institute, June 2016, <https://rusi.org/publication/whitehall-reports/out-sight-out-mind-review-efforts-counter-proliferation-finance>.

Of course, one of the primary reasons for the gap in analysis is a lack of information on the internal workings of illicit procurement networks. Procurement is a secretive, covert activity, and the information that is available tends to be limited in scope. Although nuclear procurement networks share similar properties, they have varied in scope, scale, structure, and purpose.[17] This article takes a different approach. Rather than identifying new procurement techniques and tactics, this article proposes a new analytic framework, which uses the concept of resilience to explain illicit procurement networks' processes of innovation and adaptation within environments characterized by risk and uncertainty. That is, what are the mechanisms that allow networks to bounce back from some type of shock such as an enforcement action?

Resilience, within this context, is the product of underlying environmental, organizational, and individual-level factors. In other words, the ability of a procurement network to adapt or innovate is influenced by some basket of variables, like individual learning and level of street sense, organizational structure and access to resources, and understanding changes in external legal, political, social, or economic influences.

Understanding these interactions can provide fresh insights into difficult questions. How dedicated, for example, are illicit procurement channels and what is their degree of specialization? More specifically, how connected are middlemen to states' proliferation interests, or is it merely a case of opportunity and arbitrage? Is there crossover between legitimate and illicit markets and if so, to what extent? Is there competition within illicit procurement channels? If so, what are the consequences? What is the role, if any, of criminal deterrence? How do network members learn to defend against enforcement? How do middlemen interpret and understand export laws? How does enforcement influence decision-making within networks? From a policy perspective, resilience may help to enable policies that specifically target and inhibit the ability of procurement networks to bounce-back.

The next section describes the key parameters of resilience. Then, to illustrate how the framework may provide useful insights, three cases of illicit procurement are presented which help to illustrate the interplay between internal and external drivers and identify the attributes or qualities that enable a network to respond to external shocks. Alternatively, what attributes tend to neutralize enforcement actions? By no means are the cases representative of all types of illicit nuclear procurement, but they nonetheless provide an intuitive benchmark. It is also important to reiterate that the objective of this article is to provide an analytical framework that moves beyond a general discussion of *modus operandi* to a more nuanced understanding of internal network dynamics. In other words, the cases and subsequent discussion only demonstrate what amounts to a proof of concept and does not suggest confirmation of a causal mechanism.

Resilience: A New Approach to Understanding Illicit Procurement

The concept of resilience can have multiple meanings depending on the context and unit of analysis. On one hand, resilience is the ability of a system to bounce back to its original state.

---

17 Bruno Gruselle, "Proliferation Networks and Financing," Fondation pour la Recherche Stratégique, Paris, 2007, p. 7, <http://www.stanleyfoundation.org/publications/working_papers/Delory5.pdf>; Alexander H. Montgomery, "Ringing in Proliferation: How to Dismantle an Atomic Bomb Network," International Security 30:2 (October 1, 2005), pp. 153–87.

At the other end of the spectrum, resilience is the ability of a system to adapt and evolve into a new state in response to unforeseen external shocks.[18]

Originally used to describe phenomena within ecological systems, resilience has gained popularity in recent decades to understand the capacity of social systems to deal with uncertainty and risk.[19] After the 9/11 terrorist attacks, the organizational sciences and consequence management fields found resilience to be a useful construct to describe the ways organizations bounce back from low probability, high impact events. Practitioners and scholars have also applied similar frameworks to describe how criminal and terrorist networks adapt to disruptions stemming from enforcement or regulatory actions, changes in network dynamics, or changes in market dynamics.[20] Others have even suggested resilience as a way to strengthen global nonproliferation norms.[21]

Resilience is defined in this article as the general capacity of a network to evade or bounce back from external or internal disruptions. External disruptions may be environmental disruptions, such as increased enforcement actions, or changes in domestic law. Internal disruptions, on the other hand, might include breakdowns in communications or loss of operating revenue. In other words, it is a foolhardy task to assume that a procurement network's success or failure is determined solely on the success or failure of supply-side controls. This is true in part, but discounts the persistence of nuclear procurement networks in the face of counter-proliferation efforts aimed at shutting them down. The ability of a procurement network to evade and adapt to government enforcement and supply-side controls is a sign of its resilience. However, resilience is not constant, and not all networks bounce back or succeed in evading efforts to disrupt their operations.

Identifying sources of resilience within networks, let alone illicit networks, is a relatively nascent field. In a study on illicit drug networks, however, Martin Bouchard provides a useful definition of resiliency as a function of three key attributes: vulnerability, elasticity, and adaptability.[22]

Vulnerability is a network's relative exposure to internal or external threats. For example, how compartmentalized are the network's activities compared to the relative level of enforcement? Reducing vulnerability, however, is not necessarily an intrinsic or an automatic process. It requires forethought and critical evaluation of potential and likely threats. Take, for example, organization and logistics, which are oftentimes points of vulnerability for illicit procurement. A

---

18 Karl Weick, "Introductory Essay: Improvisation as a Mindset for Organizational Analysis," *Organization Science* 9:5 (October 1, 1998) pp. 543–55; Louise K. Comfort, Arjen Boin, and Chris C. Demchak, eds., *Designing Resilience: Preparing for Extreme Events* (Pittsburgh, Pa: University of Pittsburgh Press, 2010), p. 8.

19 Aaron B. Wildavsky, *Searching for Safety* (New Brunswick, USA: Transaction Books, 1988).

20 Julie Ayling, "Criminal Organizations and Resilience," *International Journal of Law, Crime and Justice* 37:4 (December 2009), pp. 182–96; Martin Bouchard, "On the Resilience of Illegal Drug Markets," *Global Crime* 8:4 (November 1, 2007), pp. 325–44.

21 Arian Leigh Pregenzer, "Systems Resilience: A New Analytical Framework for Nuclear Nonproliferation," Sandia National Laboratories, December 1, 2011, <http://www.osti.gov/scitech/biblio/1034890/>.

22 Martin Bouchard, "On the Resilience of Illegal Drug Markets," *Global Crime* 8:4 (November 1, 2007), pp. 325–44.

network that is reliant on a single mode of shipping is more vulnerable than a network that uses multi-modal transport systems. It is important to note, however, that vulnerability is contextual, and often dependent on other environmental factors. Whereas using multi-modal logistics and shipping systems may reduce vulnerability in regions where export enforcement is high, it may have no effect in areas where export enforcement is low—thus, an inefficient use of resources. Alternatively, a network that employs several shipping partners and routes simultaneously where enforcement is high may also increase its risk of detection and interdiction. Therefore, reducing vulnerability consists of an interplay between external forces and internal network responses.

Whereas vulnerability characterizes overall exposure to threats, elasticity characterizes the network's ability to "bounce back" from unforeseen shocks and return to its original state. If a key member is extricated from the network, how does the network recover functionality? Redundancy, for example, is a key component to elasticity. Duplicate communications systems can help mitigate against a shock that may neutralize one or more channels. However, redundancy, in and of itself, may not be entirely sufficient to ensure elasticity. In a centralized network that lacks compartmentalization, for example, redundant communication networks may offer no protection against external surveillance. Under this scenario, redundancy may provide law enforcement and intelligence agencies even greater access to the inner workings of the network.

It is important to note, however, that elasticity does not necessarily imply that the network is easily able to adapt. If the shock is too great, and the network cannot bounce back, it must either adapt or perish. Bouchard defines this capacity to adapt as, "…the extent to which [the network] can modify its circumstances to make its components less vulnerable."[23] Of course, adaptation can be a complex process and over time requires a great deal more resources to be successfully achieved. In the case of illicit procurement, adaptation may mean using new smuggling routes, finding alternate suppliers, changing corporate identities, substituting goods, or moving operations to a new location altogether. It is also important to note that an adaptation may involve something entirely new and yet to be discovered by intelligence, law enforcement, or regulatory authorities.

Vulnerability, elasticity, and adaptability are not mutually exclusive elements of resilience. A resilient network can, and oftentimes does, display properties of each element. Sometimes they are complementary, and sometimes they are competing. Reducing vulnerability by compartmentalizing information, for example, may decrease overall elasticity or even the capacity to adapt. Restricting access to information or people may demonstrate a keen awareness of a need for greater security, but it can also inhibit information flows during periods of crisis. Likewise, a network may be able to increase its elasticity by increasing its number of members or modalities, but it is quite possible that in doing so, the network increases its vulnerability to outside scrutiny by offering more access points.

The next sections will describe how organizational, individual, and environmental factors affect resilience. To better illustrate the proposed relationship between resilience and environmental, organizational, and individual factors, Figure 1 illustrates a notional path diagram, which shows how exogenous factors (organizational, environmental, and individual) affect endogenous factors of resilience (vulnerability, elasticity, and adaptability).

23 Ibid, 330.

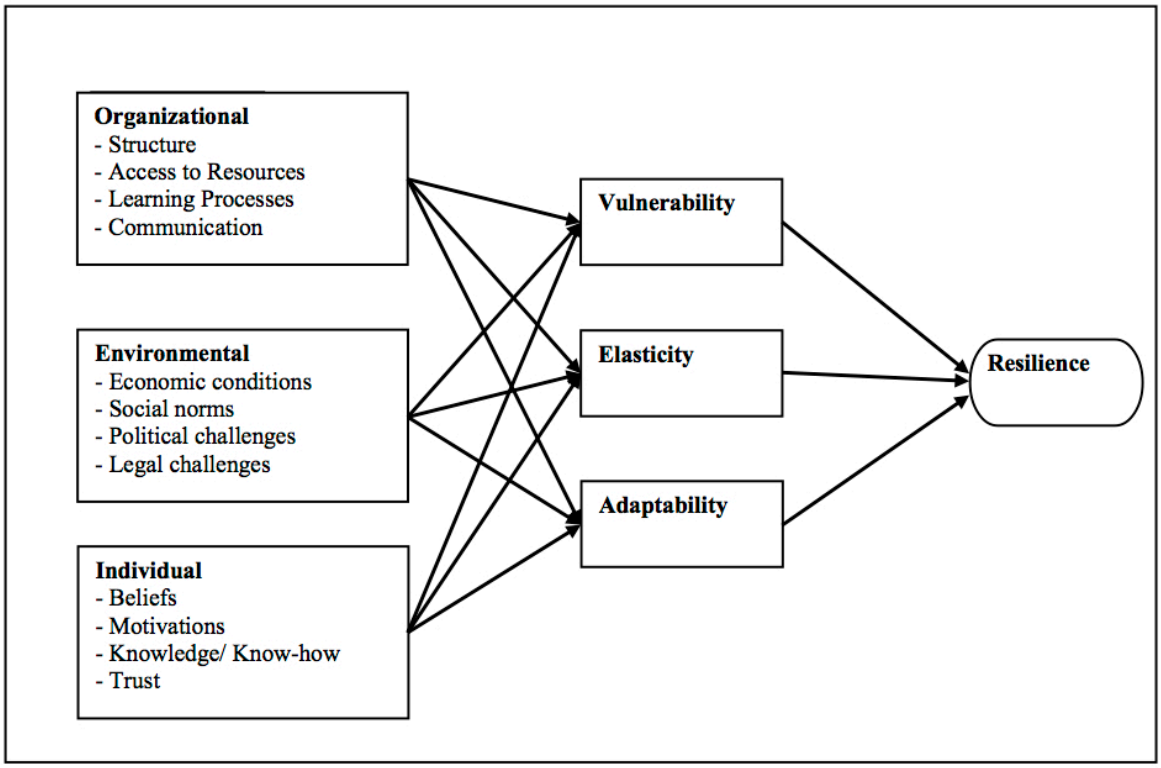

Figure 1. Notional Path Diagram of the Relationship between Resilience and Organizational, Environmental, and Individual Factors

Organizational and Individual Factors

Generally, organizational and individual level factors are the intrinsic characteristics of the network. At the organizational level, structure, access to resources and learning processes can all affect the elasticity, vulnerability, and adaptability of a network. Likewise, individual level factors, such as communication, beliefs, and motives can also affect resilience in similar ways.[24]

Take technical expertise, for example. Within illicit procurement networks, technical expertise, which is a function of information availability and learning, can play an integral role in guarding against shocks and maintaining core functionality. The degree to which procurement agents understand the technology they are dealing with has the potential to either mitigate or exacerbate external threats. On one hand, if members of the network have a strong technical background, they may be better suited to identify relevant suppliers. If a supplier is cutoff, technical expertise may prove useful in finding not only alternative suppliers, but alternative materials. Technical expertise may also insulate against certain types of law enforcement actions, like undercover operations, where fake or dummy materials are used.

Interestingly, trust dynamics—an individual level factor comprised of belief systems and motives—between network members may also play an important role for resilient networks. A

24 Diane L. Coutu, "How Resilience Works," *Harvard Business Review* 80:5 (May 2002), pp. 46–55; Arjen Boin and Michel J. G. van Eeten, "The Resilient Organization," *Public Management Review* 15:3 (March 1, 2013), pp. 429–45.

network that enjoys a high degree of trust is able to adjust quickly to external or internal threats, as information is more easily transferred among members.[25] In a recent study on trust dynamics within a nuclear smuggling network, Egle Murauskaite described the process within a loosely connected network.[26] The author suggests that the overall lack of deep trust, either based on familial bonds or repeated transactions, may have increased the network's susceptibility to infiltration—thus reducing resiliency.[27]

Likewise, A.Q. Khan's eventual undoing was the CIA recruitment of key network members. In 2003, intelligence agencies pressured Friedrich Tinner and his sons—key members of the Khan network who helped transfer material and know-how to Libya—to turn against Khan.[28] In this case, the breakdown in trust and loyalty among key members was too much for the network to recover from. It may also indicate that Khan himself was not fully aware of the security concerns his network faced from intelligence agencies, and therefore did not think to address those vulnerabilities.

Learning and sense-making is also a critical driver within resilient networks. In general terms, learning and sense-making are the processes that organizations and organizational members use to accumulate and synthesize information.[29] It is important to realize, however, that organizational and individual level factors may have different effects (or roles to play) within illicit networks than they do in legitimate networks. Traditional notions of organizational learning, for example, present peculiar problems for illicit networks. Take for example learning through trial and error. While the opportunity costs of trial and error are high for any organization, it may be impossibly high for illicit networks. Illicit networks always run the risk of erring on the first trial, which may have catastrophic consequences. Secrecy presents another challenge, as the accumulation of tacit knowledge may be tempered by the need for greater secrecy and compartmentalization within procurement networks.

Flexible organizational structures may also promote the ability to act creatively and innovate under ambiguous or uncertain conditions—further contributing to resilience. In illicit networks, redundancy, de-centralization, and loose-coupling between nodes are all factors

---

25 Cynthia Stohl and Michael Stohl, "Networks of Terror: Theoretical Assumptions and Pragmatic Consequences," *Communication Theory* 17:2 (May 1, 2007), pp. 93–124.

26 Egle Murauskaite, "The Trust Paradox in Nuclear Smuggling," *The Nonproliferation Review* 22:3–4 (October 2, 2015), pp. 321–39.

27 Ibid, 333–34.

28 David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free Press, 2010), p. 10.

29 Although complex, there are three general processes that describe how organizations learn: experience accumulation, knowledge articulation, and knowledge codification. The first, experiential accumulation, occurs through a process of environmental interactions, whereby the interactions lead to the accumulation of tacit knowledge. Learning by doing and learning through trial and error are simple examples. Knowledge articulation occurs when organizations figure out what works and what does not work through sharing and communication among organizational members or groups within an organization. Finally, knowledge codification happens when the organization formalizes what it learned through the creation of blueprints, manuals, and standard operating procedures. See, for example, Chris Argyris and Donald Schon, *Organizational Learning: A Theory of Action Perspective* (Reading, MA: Addison-Wesley, 1978); James G. March, "Exploration and Exploitation in Organizational Learning," *Organization Science* 2:1 (February 1991), pp. 71–87. Maurizio Zollo and Sidney G. Winter, "Deliberate Learning and the Evolution of Dynamic Capabilities," *Organization Science* 13:3 (June 1, 2002), p. 341.

that can minimize the impact of external disruptions.[30] The need for secrecy, however, tends to promote compartmentalized structures. While compartmentalization may create obstacles for efficient legitimate organizations, it can reduce the impact of a compromised or damaged node within an illicit network by reducing the probability of catastrophic cascading effects. The A.Q. Khan network, for example, effectively compartmentalized sensitive activities and used redundant structures through a complex network of shell and front companies.[31] Therefore, taking out a single intermediary generally did not have profound consequences throughout the rest of the system.

Finally, access to economic resources affects the capacity to innovate and pursue creative solutions. A recent report by C4ADS and the Asian Institute for Policy Studies notes that North Korea's overseas procurement networks are largely successful due to their access to significant State resources.[32] In particular, the report highlights the case of Dandong Hongxiang Industrial Development Co. Ltd., which is a North Korean procurement front that conducts over $500 million in trade annually, including trade in dual-use goods with military and nuclear applications.[33] Greater access to working capital ensures that illicit networks are able to easily change identities or shift operations to new locations when under threat.

Environmental Factors

Illicit procurement networks must also contend with environmental drivers, such as competition from other illicit networks, local policies and laws, enforcement actions, social and political conditions, market structure, and changes in demand.[34] These factors, of course, can impose significant costs or benefits, either forcing the network to adapt or insulating the network against vulnerability. In some respects, these are all responses to increased risk and uncertainty within the network's operating environment such as increased global awareness of proliferation risks and implementation of supply-side controls.[35]

---

30 Julie Ayling, "Criminal Organizations and Resilience," *International Journal of Law Crime and Justice* 37:4 (December 2009); Jacqueline Brewer and Michael Miklaucic, *Convergence: Illicit Networks and National Security in the Age of Globalization* (Washington, DC: National Defense University Press, 2013), pp. 213–33; Mark S. Granovetter, "The Strength of Weak Ties," *American Journal of Sociology* 78:6 (May 1, 1973), pp. 1360–80; Cynthia Stohl and Michael Stohl, "Networks of Terror: Theoretical Assumptions," Communication Theory 17:2 (May 2007); Arjen Boin and Michel J. G. van Eeten, "The Resilient Organization," *Public Management Review* 15:3 (March 1, 2013), pp. 429–45.

31 David Albright, Paul Brannan, and Andrea Stricker, "Detecting and Disrupting Illicit Nuclear Trade after A.Q. Khan," *The Washington Quarterly* 33:2 (April 1, 2010), pp. 85–106.

32 "In China's Shadow: Exposing North Korean Overseas Networks," Asian Institute for Policy Studies, Washington, DC, August 2016, <http://en.asaninst.org/contents/in-chinas-shadow/>.

33 Ibid, 34.

34 Julie Ayling, "Criminal Organizations and Resilience," *International Journal of Law Crime and Justice* 37:4 (December 2009).

35 Many of Iran's procurement activities highlight this phenomenon. Consider the case of the Islamic Republic of Iran Shipping Lines (IRISL)—an entity subjected to US and EU sanctions since 2008 and 2010, respectively, due to its role in supporting Iran's nuclear and ballistic missile programs. IRISL illustrates how financial and insurance sanctions, for example, can induce adaptation and result in system resilience. As sanctions increased, IRSL adapted by re-flagging and renaming its shipping vessels, tampering with end-user certificates, and adjusting information to conceal financial transactions in order to maintain access to global financial systems. See "Update on the Continuing Illicit Finance Threat Emanating from Iran," Department of the Treasury Financial Crimes Enforcement Network, Washington, DC, June 2010.

Enforcement actions can be a strong motivating factor in promoting illicit procurement networks to adapt. In fact, as Michael Kenney points out, the interaction between enforcement and internal forces can lead to a process of "competitive adaptation," whereby networks adapt to external forces and vice-versa.[36] As "players" are eliminated and enforcement strategies change, the net result is a more efficient system with a higher state of resiliency.

Changes within the networks' political, social, or economic environment may also enable success or failure by bolstering or hindering resiliency. Although US and international sanctions against Iran exacted significant economic damage, the sanctions also bolstered its resilience to external shocks. A recent report by John Park and Jim Walsh on the efficacy of sanctions against North Korea found that they were largely ineffective at stopping North Korean procurement. In fact, the report goes on to claim that sanctions may have even increased Pyongyang's procurement capabilities.[37] According to the authors, North Korean procurement firms were able to successfully monetize risk as sanctions drove up transaction costs.

In Iran's case, it is quite clear that international sanctions fomented social and political acceptance of sanctions-busting networks, which enforced resiliency in two ways. First, acceptance provides a sense of security. The efficacy of Iran's procurement networks was, in part, bolstered a widespread belief in the illegality of international sanctions, which led to the legitimization of illicit procurement networks. "Of course we bypass sanctions. We are proud that we bypass sanctions because the sanctions are illegal," commented Iranian President Hasan Rouhani about US and international sanctions.[38] Evading sanctions, then, became a patriotic duty of sorts.[39]

In 2016, a prominent Iranian-Turkish businessman—Reza Zarrab—was implicated in a fraudulent scheme of bribery and corruption to control a gold smuggling operation that provided Iran access to foreign currency. According to a criminal indictment filed in the Southern District of New York, from about 2010 to 2015, Reza Zarrab operated multiple money service businesses located in the United Arab Emirates and Turkey which he knowingly allowed Iranian banks to use in order to evade US sanctions.[40] In 2011, for example, Zarrab instructed Al Nafees Exchange, which is a UAE-based exchange house, to make international payments on

---

36 Michael Kenney, *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (University Park, Pa: Pennsylvania State University Press, 2007), p. 108.

37 John Park and Jim Walsh, "Stopping North Korea, Inc.: Sanctions Effectiveness and Unintended Consequences," MIT Security Studies Program, August 2016, <http://web.mit.edu/ssp/people/walsh/Stopping%20North%20Korea%20Inc_Park%20%20Walsh_FINAL.pdf>.

38 "Iran President Rouhani Hits out at US Sanctions," *BBC News*, August 30, 2014, sec. Middle East, <http://www.bbc.com/news/world-middle-east-28997452>; "Iran President Condemns US Sanctions 'Invasion,'" *The Associated Press*, August 2014.

39 See for example Peter Andreas, "Criminalizing Consequences of Sanctions: Embargo Busting and Its Legacy," *International Studies Quarterly* 49:2 (June 1, 2005), pp. 335–60; R. T. Naylor, *Patriots and Profiteers: Economic Warfare, Embargo Busting, and State-Sponsored Crime* (Montreal: McGill-Queen's University Press, 2008).

40 USA v. Rezza Zarrab, Indictment S1 15 Cr. 857 (US District Court, Southern District of New York May 2016).

behalf of Mellat Exchange—a subsidiary company of the Iranian Bank Mellat.[41] In a December 2011 letter to the general manager of Iran's central bank, Zarrab wrote that, "The role of the Supreme Leader and the esteemed officials and employees of Markazi Bank play [*sic*] against the sanctions, wisely neutralizes the sanctions and even turns them into opportunities by using specialized methods."[42] He then goes on to suggest that it is his "national and moral duty" to evade global sanctions.

In March 2012, for example, the European Union cut off Iran's access to the Society for Worldwide Interbank Financial Telecommunications (SWIFT).[43] The SWIFT-ban, coupled with the US financial sanctions, ousted Iran from the global financial system, and almost overnight, Iranian firms found themselves without a means to access global markets. Iranian firms, however, could adapt and eventually return to normal operations—albeit with higher transactions costs—in part by displacing operations to new locations and finding new payments routes. In some cases, these payment routes moved into less regulated and opaque financial centers, such as the United Arab Emirates. Ultimately, Iranian businesses began to normalize smuggling techniques such as using transshipment points in Dubai, falsifying end-use certificates, exploiting loopholes in remittance regulations, and co-opting regional neighbors.

In fact, it is likely that this level of normalization and legitimization of smuggling provided redundancy and increased resilience for Iran's nuclear procurement operations. As international sanctions increasingly cut Iran off from global trade and commerce, nuclear and ballistic missile procurement and sanctions evasion became increasingly interlinked—relying on the same logistic and financial intermediaries.

Finally, state demand for dual-use goods and technology may play a significant role. One of the more significant unaddressed questions regarding illicit nuclear procurement is the role and effect of market competition. How much, if any, competition exists between illicit procurement networks? If so, how do networks manage this competition? This dynamic creates somewhat of a paradox in nuclear procurement. From one angle, proliferator states may want to increase the chances of successful procurement by promoting multiple supply networks. While this may increase the resiliency of procurement operations from the perspective of the proliferator state, the added competition may increase the vulnerability of the individual procurement agent. How, then, do procurement agents deal with this inherent tension?

The next section describes three recent cases of illicit nuclear procurement. By no means are these cases representative of every type of illicit nuclear procurement network, but each

---

41 The US Department of the Treasury, Office of Foreign Assets Control (OFAC) added Bank Mellat to the Specially Designated Nationals list in October 2007, pursuant to Executive Order 13382—an executive order that targets proliferators of WMDs. According to the Treasury Department, Bank Mellat provided banking and other financial services to entities involved in Iran's nuclear program, such as the Atomic Energy Organization of Iran. As part of the Joint Comprehensive Plan of Action, the United States removed its sanctions against Bank Mellat in January 2016.

42 USA v. Rezza Zarrab, Indictment at 10, S1 15 Cr. 857 (US District Court, Southern District of New York May 2016). Bank Markazi is Iran's central bank.

43 Headquartered in Belgium, SWIFT provides a secure network infrastructure for banks to send transaction-related information, is the world's largest global financial messaging service.

offers unique perspectives that help illustrate the dynamics of using a resilience framework—specifically the interplay between internal and external drivers. The data for each case is primarily derived from court transcripts, as well as other public records, including government reports and periodicals.

Case I: Nicholas Kaiga

Between September 2007 and June 2013, Belgian national Nicholas Kaiga worked as an intermediary to procure and transship dual-use and nuclear export controlled materials to Iran. According to the criminal indictment against Kaiga, an unnamed co-conspirator located in Iran submitted multiple orders to a named US company for aluminum tubing, which listed the end-user as *Super Alloys*—a company located in the United Arab Emirates.[44] A short investigation by a US export control officer found that an Iranian company with ties to sanctioned entities owned *Super Alloys*. Shortly thereafter, the US Bureau of Industry and Security denied the export license for the aluminum.

To avoid export licensing requirements, *Super Alloys* requested that the US company begin shipping non-export controlled materials to a purported customer in Belgium—*Industrial Metals & Commodities SPRL* (IMC), which listed Nicholas Kaiga as the owner and operator of the company. By 2009, US Immigration and Customs Enforcement began an undercover operation against *Super Alloys*. As the investigation continued, it became evident that Kaiga was re-shipping materials to a front company in Malaysia, which the unnamed Iranian co-conspirator also owned. From Malaysia, the materials were forwarded on to the UAE and then re-exported to Iran.

To determine the ultimate end-user, undercover agents shipped sham aluminum to Kaiga in December 2011, which Kaiga then forwarded to Malaysia and eventually on to Iran in February 2012.[45] Eventually, Kaiga contacted the undercover agent to inquire about the authenticity of the materials. ICE arrested Kaiga in July 2013. He was found guilty of committing violations of the International Economic Emergency Powers Act and sentenced to 27 months in prison. In July 2015, the United States deported Nicholas Kaiga back to Belgium.

Although successful in his procurement, at least initially, Kaiga is at best characterized as an unsophisticated middleman who took advantage of export control gaps. One notable feature about Kaiga's network is its structure. It was the simplicity of his network, at least in part, which reduced his overall vulnerability. In a sense, by keeping its membership low, he could reduce his vulnerability to enforcement actions. In fact, according to court records, the undercover agent made several overtures to Kaiga, asking to join his operations—which Kaiga refused.

---

44 The aluminum tubing in this case, which was 7075 T6 aluminum, has aerospace and nuclear applications. The specialized aluminum can be used to manufacture gas centrifuges, and is therefore export controlled. See, USA v. Nicholas Kaiga, Criminal Complaint (US District Court, Northern District of Illinois, Eastern Division 2013).

45 Although it is clear from the indictment that Kaiga and the co-conspirator had a business relationship, it is not clear whether or not Kaiga was aware of the ultimate destination of the materials that he was transshipping to Malaysia. It is clear, however, that Kaiga was aware that he was violating export control laws by transshipping the restricted goods to Malaysia.

Although it is possible that he balked at this offer out of an abundance of caution, it is more likely that Kaiga did not see a legitimate business need to expand his operations. In other words, business was slow for Kaiga.

Although he lacked technical expertise regarding the parts he was acquiring, Kaiga was a skilled businessman with a strong background in international financing and banking. He understood European Union export laws, which he could leverage in order to re-export controlled goods to Malaysia. Unfortunately for Kaiga, his lack of technical expertise ultimately left him vulnerable to an undercover operation led by US Immigration and Customs Enforcement.

During the undercover operation, ICE agents sent Kaiga dummy aluminum tubes. Believing the parts were genuine, Kaiga then forwarded the tubes on to Malaysia, where they were re-exported to Iran. It was only after they reached Iran when Kaiga learned that the order did not meet the correct specifications. Interestingly, even when he did find out they were dummy tubes, he thought the US manufacturer was at fault—he did not once consider that he may be the subject of an undercover operation. Had Kaiga identified the dummy tubes, he could have cut his losses and displaced his activities elsewhere. Of course, Kaiga had no reason to believe that he was under investigation. Unlike other cases, however, the United States did not add Kaiga to its sanctions list. If it had, perhaps he would have been more cautious—even seeking alternative methods to obscure his identity.

At best, Kaiga's network could be characterized as inelastic and vulnerable to external enforcement. Most notably, Kaiga's lack of redundant systems left his operations open to infiltration. Furthermore, if Kaiga had a better technical understanding of the materials he was dealing in, he might have become aware of US interest in his operations much sooner—giving him time to find alternative suppliers.

Case II: Sihai "Alex" Cheng

In January 2016, Sihai "Alex" Cheng was sentenced to nine years in prison for violating US export control laws. According to the criminal indictment, between 2009 and 2012, Cheng—a Chinese citizen—worked with Iranian national Seyed Jamili to procure and transship thousands of export controlled pressure transducers, worth almost $2 million, to Iran.[46] Cheng and Jamili met at a trade show in Guangzhou, China. It was at this meeting where an enterprising Cheng agreed to work with Jamili to acquire sensitive components that would ultimately end up in Iran's gas centrifuge program. In fact, without Cheng's involvement, it is quite unlikely that Jamili could procure the parts.[47] Shortly after Cheng's indictment, the United States and European Union sanctioned Jamili's company, *Eyvaz Technic*, for its involvement with Iran's nuclear program.

---

46 Pressure transducers are sensors with multiple applications, but can be used to measure pressure during uranium enrichment processes. Indictment in the case of the United States of America v. Sihai Cheng, No. 13CR10332 (n.d.).

47 USA v. Sihai Cheng, Sentencing Hearing Transcript (US District Court for the District of Massachusetts 2016).

Cheng's network appears to have been quite unique in that it is one of the few known recent cases where corrupted employees of a supplier took part in the illicit activity. Employees at a Shanghai-based subsidiary of MKS Instruments, which is a parts supplier based in Andover, Massachusetts, worked with Cheng to obtain fraudulent export licenses.[48]

One of the keys to Cheng's early success was his ability to compartmentalize information and thus maintain at least some degree of secrecy. Email records from Cheng's sentencing hearing suggest that he kept most of his co-conspirators in the dark about the most sensitive aspects of his operations. In fact, in an email to Jamili, Cheng wrote, "I must tell you again, the goods are supplied to us secretly. MKS doesn't know it's supplied to me. They think it's supplied to the Shanghai agent and used for some Chinese solar energy and semiconductor industry…"[49] Hu Johnson—another co-conspirator—believed that the items were being re-exported to Singapore—genuinely unaware that the parts were ultimately destined for Iran.[50]

Cheng's degree of technical expertise was quite low. In fact, even though it was clear that Cheng knew he was committing export violations, it is unclear whether he knew the parts were intended for Iran's nuclear program. Not only did Cheng not have a solid understanding of the technical aspects of the parts he was procuring, but his international business acumen was lacking as well.[51] His attorney, however, notes that while Cheng is quite intelligent, his knowledge of international business is quite naive.[52] This lack of expertise may have contributed to an inability to guard against external shocks. A superficial understanding of international business can limit an actor's ability to find alternative payment schemes, new logistic routes, or substitute suppliers. It also means the actor may not be attuned to changes in demand or regulatory and legal requirements. Ultimately, then, the lack of business acumen puts Cheng's illicit operations in jeopardy and reduces overall resiliency. It is important to note, however, that although Cheng may not have been an international trade expert, it is not possible to measure the direct effect of his inexperience on his overall success or failure with illicit trade.

One aspect of Cheng's operations that clearly impacted his network's vulnerability and elasticity was his belief that he would not be caught (i.e., sense-making). Cheng maintained that he

---

48 Indictment in the case of the United States of America v. Sihai Cheng; David Albright and Andrea Stricker, "Case Study - Chinese Salesman Arrested in Pressure Transducer Case," Institute for Science and International Security, Washington DC, January 18, 2013, <http://isis-online.org/isis-reports/detail/case-study-chinese-salesman-arrested-in-pressure-transducer-case/>.

49 "Sentencing Memorandum in the Case of the United States v. Sihai Cheng" (US District Court of Massachusetts, February 1, 2016), p. 45.

50 In a statement before the court, Cheng provides a different account, noting that he did in fact tell the MKS employees that the pressure transducers were for an end-user in Iran. See, USA v. Sihai Cheng, Sentencing Hearing Transcript at 145. In a related case, however, the US Government noted that there is no evidence that Qiang Hu knowingly caused export controlled parts to be shipped to Iran. See, USA v. Qiang Hu, Government Sentencing Memorandum (United States District Court, District of Massachusetts 2014).

51 Cheng graduated with an English degree from Shandong University, and shortly thereafter began working in international trading, which was lucrative and provided income for his family, who are farmers rural provinces of Goungzhou.

52 USA v. Sihai Cheng, Sentencing Hearing Transcript at 163. While profit was a strong motivator for Cheng, his attorney noted that it was more the excitement of being involved in a global business and the corresponding prestige. Nonetheless, Cheng himself admits that his motivations were based on greed.

perceived the risk of getting caught to be low and that he did not fully realize the severity of his export violations.[53] Although some evidence suggests that Cheng at least partially understood the severity of his export violations, he nonetheless openly traveled to London, where he was arrested and eventually extradited to the United States. This suggests that Cheng was not aware of impending law enforcement actions against him and his network.[54]

Finally, Cheng's access to resources, specifically working capital, was quite limited. In fact, for most of his procurement, Jamili fronted Cheng the cash to complete each transaction. While the US prosecutors contend that Cheng worked to procure almost $2 million worth of parts for Iran's nuclear program, Cheng's profit margin was quite narrow. Although the exact amount is unknown, he likely split about $450,000 between 13 co-conspirators over a five-year period. In other words, Cheng was taking a significant risk for what amounted to a few thousand dollars a year. Thus, without significant proceeds, Cheng did not have the resources to reduce his network's vulnerability by maintaining multiple front companies, bank accounts, and logistic routes. Had his operations been more lucrative, perhaps Cheng would have taken greater precautions to insulate his network from external threats.

Overall, Cheng's resiliency was rather low. Low working capital, no back-up systems, and no expectation of getting caught meant that Cheng was not prepared when the United States decide to enforce export controls.

Case III: Li Fang Wei

Li Fang Wei, better known as Karl Lee, controls one of the most enigmatic procurement networks since A.Q. Khan. For more than a decade, Li—a Chinese procurement agent—has been a "principal supplier" to both Iran's ballistic missile and nuclear programs.[55] Unfortunately, other than information obtained from US criminal indictments, as well as a blurry picture on a FBI Wanted poster, not much is known about Li. What is known, however, is that Li runs one of the largest procurement channels since the Khan network and yet enforcement agencies have been unable to shut his operations down. In fact, he is currently the only procurement agent with a $5 million bounty for information leading to his arrest. Unlike the two previous cases, however, Li is known not just for his ability to act as a middleman, but also as a manufacturer. In fact, a recent analysis of his network suggests that Li may be manufacturing and exporting sensitive guidance components, which have ballistic missile applications.[56]

---

53 Emails between Cheng and Jamili seem to indicate that Cheng knew of the risks he was taking by transshipping the export controlled items to Iran. In one email Cheng wrote, "Time is important, not only for you, for me, for your end-user, but also for your nation. I personally believe the war will break out in two years, and that will be the start of World War III." It should be noted, however, that during the sentencing hearing, Cheng offered a different explanation for this exchange, suggesting this was merely "bravado" meant to entice and keep Jamili as a customer. In fact, other evidence does suggest that Cheng became increasingly concerned that Jamili would cut him out of the procurement operations.

54 According to a person familiar with the case, the Chinese government may have tipped-off Cheng to the United States' interest in his business operations. Despite this warning, however, Cheng continued his procurement operations.

55 David Albright, Andrea Stricker, and Donald Stewart, "Serial Proliferator Karl Li," Institute for Science and International Security, Washington DC, May 8, 2014, <http://isis-online.org/isis-reports/detail/serial-proliferator-karl-li-chinas-continued-refusal-to-act/20>; Daniel Salisbury and Ian Stewart, "Wanted: Karl Lee" Project Alpha, King's College, London, UK, May 19, 2014, <http://projectalpha.eu/wanted-karl-lee/>.

56 Ibid.

The internal workings of Li's network are largely a mystery to outsiders. But, over the last decade, Li has made extensive use of front companies and circuitous financial transactions in order to obscure his illicit dealings—techniques that go well beyond what Kaiga and Cheng employed. In 1998, Li first established *LIMMT Economic and Trading*—a company Li used to transfer relatively large quantities of high-end carbon fiber and aluminum alloys to Iran. In 2006, the US Treasury Department added *LIMMT* to its sanctions list, and later, in 2009, added Li himself.[57]

To evade sanctions, Li established a complex network of front companies and aliases. Between 2004 and 2014, Li used over a dozen fronts and even more aliases. In fact, Li would often use family members or business associates to obscure his true identity from banks.[58] Unlike the other networks, however, Li has been able to quickly bounce back from external shocks and even adopt new methods. In fact, one of the major drivers of Li's adaption were US law enforcement and regulatory actions. When the US added Li's front companies to the Treasury Department's sanctions list, he changed his corporate identities. When the FBI seized Li's assets through his Chinese bank's US correspondent accounts, he simply moved his remaining assets into financial institutions with no US correspondent accounts.

Another factor bolstering Li's resilience is that his expectation of interference from Chinese enforcement is quite low. In fact, some evidence suggests that the Chinese government had warned Li about possible impending US sanctions. Not surprisingly, the Chinese have refused multiple extradition requests, despite multiple dèmarches from the US State Department.[59]

Clearly, Li's operations are far more resilient than Kaiga and Cheng. Two significant factors likely helped bolster this resilience. First, US sanctions against Li and his companies provided a signal to Li that he needed to adapt or else face possible criminal or economic penalties. In other words, it was the US designation that tipped-off Li, and then Li's ability to interpret—or make sense of—this signal to come up with clever evasion methods. Second, Li has a large pool of capital at his disposal. Thus, he can afford maintenance costs associated with running multiple front companies.

Discussion and Implications

The Nicholas Kaiga, Alex Cheng, and Karl Li cases each illustrate that resilience within procurement networks is a varied process, influenced—at least in part—by internal and external drivers. It is important to note, however, that these cases only demonstrate what amounts to a proof of concept, and does not suggest evidence of causal mechanism. That is, while many of the findings are quite intuitive, the cases are rather narrow and will require additional analysis using further cases. Moreover, these cases focused specifically on Iranian nuclear procurement. North Korea, for example, uses very different methods. Nonetheless, even as a proof of concept,

57 In Rem Complaint against Karl Lee, No. 14 CIV (Southern District of New York April 29, 2014).

58 Daniel Salisbury and Ian Stewart, "Wanted: Karl Lee" Project Alpha, King's College, London, UK, May 19, 2014, <http://projectalpha.eu/wanted-karl-lee/>.

59 "NIAG 8233: Transfer of Maraging Steel from China to Iran," Wikileaks Public Library of US Diplomacy, Secretary of State, January 14, 2009, <https://wikileaks.org/plusd/cables/09STATE3943_a.html>.

these findings do have implications for global supply-side controls from both a policy and enforcement perspective.

First, it is important to note that the model, as described in this article, cannot, with any degree of certainty, make the claim that some controls are better able detect or dissuade a network in a specific resilient state. Clearly, this is a logical conclusion, which might lead one to believe that enforcement of supply-side controls should consider ways to reduce a network's overall resilience or prevent a network from achieving a higher state of resilience. Yet, the research is not yet at a point to make this determination. To make this determination, a more thorough analysis of the covariation between successful operations and factors of resilience is needed.

Some of the findings, however, do suggest that access to resources may play an important role in network resilience. In April 2014, a federal grand jury indicted Li, *in absentia*, for sanctions violations and money laundering. Instead of attempting to shut him out of the global financial system by imposing sanctions, the Justice Department targeted Li's assets. Interestingly, the Justice Department employed a seldom used tactic against Li entailing the filing of a civil complaint against Li's assets. In doing so, the US Government could seize his assets which were held in overseas accounts at Bank of China and Shanghai Pudong Development Bank by seizing funds from the banks' accounts in the US.[60] In doing so, the US Government was able to seize almost $7 million of Li's assets. It is important to note, however, that the process of competitive adaptation ensures that Li, and others like him, will work to insulate themselves against this type of enforcement in the future. Thus, agencies must be willing to innovate and seek out new strategies.

A resilience framework may also offer recommendations to improve policy approaches to global export control regimes. Take, for example, the illicit financing of nuclear procurement. One of the key challenges for banks and government agencies in detecting financial transactions relating to nuclear procurement is the inability to identify specific patterns of behavior—also "activity-based" proliferation finance. The financial industry is quite adept at conducting name and entity checks against international sanctions and export-control lists, but less so at detecting patterns. A recent report on proliferation financing by the Royal United Services Institute found that banks need a better understanding of the underlying "behavioral signatures of the illicit procurement."[61] Understanding the persistent ability of nuclear procurement networks to adapt—its resilience—might be able to help bridge this problem. Of course, to do so, US intelligence and enforcement agencies must overcome obstacles that prevent efficient and transparent information sharing with the private sector.

A new area of research with significant implications for export control policy is on non-state proliferator motivations. Why would an intermediary in China be willing to transship export controlled materials to Iran and risk potential fines, or even worse, arrest and incarceration? Conventional wisdom assumes that middlemen are largely profit-motivated and weigh these incentives against the costs of getting caught. Although the risk versus reward calculus can be

60 In Rem Complaint against Karl Lee, No. 14 CIV (Southern District of New York April 29, 2014).

61 Emil Dall, Andrea Berger, and Tom Keatinge, "Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance," Royal United Services Institute, June 2016, <https://rusi.org/publication/whitehall-reports/out-sight-out-mind-review-efforts-counter-proliferation-finance>, p. 26.

rather parsimonious for policy makers, the evidence available tends to demonstrate that profits are quite low and the risks of detection by law enforcement and intelligence agencies is not trivial. In fact, it seemed to be the case that in the Cheng and Kaiga cases, each viewed the risk of getting caught as so low that even minimal profits were worth the risk. While perhaps counterintuitive, this is consistent with some of the criminological literature on why people commit crimes.[62] To be sure, however, a much deeper analysis is necessary to determine these causal mechanisms.

Of course, understanding these motivations is important when considering possible deterrent effects. In sentencing Alex Cheng, for example, it was quite clear that the judge was interested in sending a deterrent message to potential export violators. In justifying the lengthy prison sentence, the judge noted that, "…there are a lot of people there who are trying to get our stuff out of the country into other countries. So it's not so much him [Cheng]. You have to have a serious deterrent."[63] Here, the judge assumed—perhaps wrongly—that a lengthy sentence imposed against Cheng would send a deterrent signal to other would-be procurement agents.

In a new article by Ian Stewart and Daniel Salisbury, which explores non-state actor motivation, the authors state that, "For an actor to be deterred, the potential perceived cost of the action must outweigh the benefit."[64] This, of course, implies that certainty over severity can be a de-motivator for procurement agents. But, a resilience framework would suggest some level of adaptation. When enforcement does increase, for example, the net result is likely a more lucrative market for proliferators. In other words, risk can be monetized within illicit procurement, which may in turn attract new procurement actors.[65]

Conclusion

Nuclear weapons aspirants, historically, have at least partially relied on acquiring foreign materials and technology to support enrichment programs. Given this trend, coupled with a

---

62 Take, for example, the routine activities theory of crime, which postulates that motivation, abundance of opportunity, and the lack of some type of macro-level control leads to criminal activity. While contentious, it nonetheless explains certain crimes, such as intellectual property theft and other types of occupational crimes. Recent work by Bichler and Malm applies routine activities theory of crime to explain motivation in transnational criminal activity—such as import/export violations. The authors explain how the lack of macro-level economic, social, political, and legal controls—especially in areas of jurisdictional asymmetry—coupled with globalized commerce and increased access to communications creates opportunity ripe for exploitation regardless of reward. For a discussion of the routine activities theory of crime, see Derek B. Cornish and Ronald V. Clarke, *The Reasoning Criminal: Rational Choice Perspectives on Offending* (New York, NY: Springer New York, 1986), pp. 1–16; see, also Gisela Bichler and Aili Malm, "The Routine Nature of Transnational Crime," in *The Criminal Act: The Role and Influence of Routine Activity Theory*, ed. Martin Andresen and Graham Farrell (New York, NY: Palgrave Macmillan, 2015), pp. 33–58.

63 "Sentencing Memorandum in the Case of the United States v. Sihai Cheng,", p. 167.

64 Ian Stewart and Daniel Salisbury, "Non-State Actors as Proliferators: Preventing Their Involvement," *Strategic Trade Review* 2:3 (Autumn 2016), p. 12.

65 For a discussion of the monetization of risk within illicit procurement see John Park and Jim Walsh, "Stopping North Korea, Inc.: Sanctions Effectiveness and Unintended Consequences," MIT Security Studies Program, August 2016, <http://web.mit.edu/ssp/people/walsh/Stopping%20North%20Korea%20Inc_Park%20%20Walsh_FINAL.pdf>.

long-held belief that the acquisition of complex technology remains the primary challenge for states seeking nuclear weapons, policymakers have focused much attention on controlling the spread of nuclear-related materials and technologies.[66] Unfortunately, this attention has come at the cost of ignoring other dimensions of illicit procurement.

The mesh of treaties, national laws, sanctions, embargoes, and non-binding political commitments tends to fall short of a seamless and integrated system capable of detecting and stopping illicit nuclear procurement. Ubiquitous technology and indigenization of manufacturing present significant challenges for global export regimes. Moreover, implementation gaps in United Nations Security Council resolution 1540 still present obstacles for transparency and capacity-building efforts. This article proposes a new framework based on the concept of resilience to better understand the core drivers that affect and promote illicit procurement. That is, despite efforts to stem the global trade in dual-use goods and technology, how are illicit procurement networks able to defend themselves, bounce-back, and adapt?

The three case studies presented help to paint a picture of how resilience can be used to analyze illicit procurement networks. What is clear is that knowledge acquisition, structure, learning, sense-making, innovation, and access to resources—in addition to external forces—can all influence the network's ability to adapt. Consequently, enforcement and policy must take proactive, rather than reactive, approaches to countering non-state proliferation of dual-use goods and technologies.

Acknowledgments

Special thanks to Martin Malin, Daniel Salisbury, Matt Bunn, and Robert Shaw for their guidance and comments on earlier versions of this paper.

66 R. Scott Kemp, "The Nonproliferation Emperor Has No Clothes," *International Security* 38:4 (April 1, 2014), pp. 39–78; Douglas M. Stinnett et al., "Complying by Denying: Explaining Why States Develop Nonproliferation Export Controls," *International Studies Perspectives* 12:3 (August 1, 2011), pp. 308–26; Frederick McGoldrick, "Nuclear Trade Controls: Minding the Gaps," CSIS, Washington, DC, January 2013, <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130122_McGoldrick_NuclearTradeControls_Web.pdf>; Matthew Kroenig, *Exporting the Bomb: Technology Transfer and the Spread of Nuclear Weapons* (Ithaca: Cornell University Press, 2010).