ISN
ETH Zurich

23 June 2014

Converging Threats Yield New Opportunities

If the global security environment is so interconnected now, what do states need to do in response? According to Brian Finlay, it's high time for government agencies to link up with NGOs and the private sector. The latter have innovative approaches that are just waiting to be used.

By Brian Finlay for ISN

Last July, a North Korean-flagged bulk carrier steamed through the Caribbean Sea en route to Wonson, DPRK, via the Panama Canal. Queuing at the Manzanillo International Terminal, Panamanian officials seized the ship on reports that it was transporting illegal drugs. They found much more than that. Buried under a cargo of 250,000 bags of sugar—and in contravention of UN Security Council sanctions—they discovered two anti-aircraft missile batteries, nine air defense missiles, two Mikoyan-Gurevich MiG-21 fighter planes and other prohibited items. It was not the first time this vessel was transporting illicit goods to and from North Korea. In the three years prior to this seizure, the same ship had been caught conveying a wide variety of contraband from heroin substitutes, to counterfeited alcohol and cigarettes, and large caches of ammunition for AK-47s through various ports around the globe.

While the July operation was a clear law enforcement success, the incident is indicative of a wider dilemma facing governments today: a growing array of interconnected security challenges, facilitated by transnational organized criminals, exploiting a global supply chain that does not respect national borders or stove-piped policy responses. The numbers speak for themselves:

· For decades, governments have tried to manage the negative impacts of both the licit and the illicit conventional arms trade, yet, according to the US Department of Commerce, the arms trade currently accounts for approximately 50 per cent of all corrupt transactions worldwide. The illicit arms trade is a $4 billion annual industry that drives violence across the planet and is estimated to cost Africa approximately $18 billion per year.

· You will not be hard pressed to find a politician that wants to end modern day slavery. Yet of the 27 million men, women, and children that are victims of human trafficking each year, the international community has identified only about 40,000 of them in the last few years.

· In 2009, U.S. President Barack Obama vowed to work with international partners to "secure all vulnerable nuclear material around the world within four years." Yet in 2013 alone, four years after this promise was made, the IAEA's Nuclear Incident and Trafficking Database (ITDB) confirmed 146 incidents involving nuclear and radioactive materials. That figure included 6 incidents involving possession and related criminal activities, 47 involving theft or loss of material, and 95 involving other

unauthorized activities—and these are the incidents about which we are aware.

Even worse than these individual threats is the growing interconnectivity between once isolated criminal and terrorist acts. We now know for instance that the 2004 Madrid train bombings that killed 191 people and wounded another 1,800 were financed in part by the Moroccan hashish trade. Likewise, the resources Hezbollah uses to fund its attacks—such as the Bulgarian bus bombing in 2012—are partly derived from the Latin American drug trade. In Africa, al Shabaab's attack on the Westgate shopping center in Nairobi was facilitated in part by wildlife trafficking, and the attack on an Algerian gas plant that same year was financed by cigarette smugglers.

These graphic anecdotes demonstrate that a widening gyre of security threats is interwoven in the era of globalization. Regrettably, what we have not yet done is to learn from the innovations of these illicit traders, break down our own outmoded, stove-piped responses, and develop a workable strategy to combat this menace. In 2000, the United Nations General Assembly adopted the Convention against Transnational Organized Crime. That agreement is the central international instrument in the fight against widening criminal activity around the globe. Responding to a growing recognition of international criminality, many national strategies have subsequently been developed. Yet these good efforts seem to have had little impact on disrupting a growing convergence of transnational threats.

The ongoing conflict in Syria presents an illustrative case study of the novel security dynamics of the 21st century. The current conflict is being sustained by multiple actors: government forces bankrolled and equipped by the licit and illicit arms trade, as well as various forms of illegal financing; terrorist organizations and insurgent groups that leverage a wide range of criminal activities, and moderate opposition groups receiving military assistance through backchannels or by hiding in plain sight. Each of these groups takes advantage of Syria's porous borders and global and national security strategies that were set up to manage 20th century state-centric threats. In their current form, these approaches do little to respond to the 21st century dynamism that is transnational crime today.

Consider, for example, the smuggling routes in Turkey's southeast, which now present refuge to those fleeing the Syrian conflict but have also been exploited by foreign fighters that want to participate in the conflict. The conflict has helped to fine-tune these illicit paths and strengthen the networks that run them. Today, non-state actors funneloil out of Syria and arms into the country. Increased transnational criminal activity throughout the region as a result of the Syrian conflict threatens armed violence in neighboring countries, most notably Lebanon. There are now worries of a renewed civil war in that country, instigated by Syria's own conflict.

Also troubling is the added presence of the Syrian regime's chemical weapons. The networks used by the Syrian government to procure the chemical precursors needed to produce its weapons, such as sarin, further demonstrate the interwoven nature of global security threats. While Syria has possessed the technological capability to manufacture chemical weapons for decades, it does not currently make all of the dual-use chemicals needed to produce the sarin nerve agent used outside of Damascus in August of last year. Rather, the regime relies upon an array of outside sources to obtain the needed precursor chemicals for its current chemical weapons production. Although many point to Russia and North Korea as possible suppliers, we now know that the source of these chemicals includes a variety of different actors, including private manufacturers and chemical brokerages in the United States, the Netherlands, Switzerland, France, Austria, Germany, and other well intentioned countries around the globe. One British company sought to sell precursors to sarin — sodium fluoride and potassium fluoride — to a Syrian firm as recently as January 2012. Ultimately, these front firms funnel the precursors they buy to the Syrian chemical weapons program.

The ever-evolving convergence between transnational crime and global security threats present

challenges of such vast size and scope that they threaten to overwhelm the capabilities of even well-intentioned governments to contain them. Today, traditional responses by governments are proving increasingly incapable of meeting these interconnected threats. Yet while security analysts more often lament the new challenges these networked threats present, they also present opportunities to meet these threats at critical nodes in the global supply chain. By exploiting the nexus between these threats, new opportunities have emerged to engage a wider spectrum of impacted constituencies, to better leverage limited resources, and to meaningfully and sustainably address these interconnected challenges.

A robust response starts with governments beginning to work more seamlessly across the traditional boundaries that have hampered efforts to alleviate these transnational threats. These boundaries include: (i) agency and mission stovepipes within governments, (ii) barriers to collaboration across national borders, and (iii) a reluctance to engage sub-state (industry) actors in the national security and global development dialogues. Indeed, many of the transnational threats mentioned above have common solutions and afford new opportunities for partnerships. The same container transiting the Port of Kingston and containing rotor tube cylinders or magnetic suspension bearings might also contain cocaine, counterfeit Viagra, or humans. That container is carried on the same shipping vessel. Its movement may be underwritten by the same insurer. And it transits the same ports of debarkation and entry. Each of these nodes presents the opportunities to better identify and choke off the illicit flow of contraband. Each also affords the opportunity to build new alliances among like-minded governments and industry collaborators who may share common goals even when their motivations differ.

A second major rethink concerns the private sector, which increasingly owns the means of innovation, production, and distribution of both legitimate and, knowingly or not, illegitimate goods. Although no well-meaning company would willingly involve itself in criminal activities, it is true that industry is motivated primarily by profit, not by security. More often than not, industry could do more to promote the latter without trading on the former, but lack sufficient incentive or business rationale to do so. By establishing win-win partnerships between the public and private sectors in the national security domain that rightly encourage profit while yielding a security dividend, industry can become the not-so-secret weapon in our global struggle against illicit trafficking. Unless the public sector can retool its engagement strategies with corporations, the dark side of globalization will continue to gain ground and potentially outstrip the benefits of our expanding global connectedness.

Global commerce is stretching the traditional tools of security governance to their limits. As production and trade networks become increasingly complex and geographically far-flung, the challenges of preventing illicit transshipment and other misappropriations of sensitive items add urgency to the search for more innovative solutions. Nonetheless, the first recourse of most regulatory authorities remains traditional, top-down controls—particularly in the aftermath of disruptive global security events and technological developments. As a result, exporters today must comply with an increasingly complex array of controls, imposed by multiple governments and international organizations, to address many different security and policy objectives. At the company level, this regulatory burden has increased compliance costs and elevated compliance risk. Moreover, exporters vary greatly in size, organization, operational practices, and maturity, and these differences often compound the toll brought by regulatory changes.

In short, it is clear that the existing toolkit is inefficient – and ultimately, insufficient – in combating modern and evolving threats. The private exporting community largely remains a passive target of legal requirements, not a willing participant in the global control regime. Supporting exporters' ability to recognize and avoid those transactions that ultimately could support proliferation and related transnational crimes should be an overarching objective of policymakers around the globe. This

approach would reinforce sound regulations and more systemically discourage and impede illicit, careless, and otherwise problematic industry activities in global value chains—all while supporting legitimate industry's ability to compete.

A third step for both governments and the private sector is to develop a holistic characterization of the global spectrum of transnational threats. The threats must be quantified – the illicit arms trade, human trafficking, WMD proliferation, international property crime, money laundering and the drug trade—and better matched to available national, international, and non-governmental responses to these challenges. Such a "networked" approach to better coordinating our responses to transnational criminal activity would encourage improved leveraging of limited resources to build more sustainable solutions.

In addition to government and private sector efforts, turning the tide against transnational organized criminals will require active participation from the multilateral and NGO community, which can provide a forum for information sharing and the development of innovative partnerships between these self-interested constituencies. Civil society has the capacity to serve as an information broker between occasionally mistrustful constituencies in government and industry.

Each of these efforts would contribute to the process of building a network of innovative and pragmatic solutions to address interconnected threats. To have the best chance at preventing a descent into violence orchestrated by interconnected security threats, the international community must build up a holistic body of work founded on a collaborative synthesis of identified lessons learned, as well as demonstrated best practices between governments, nongovernmental organizations, and the private sector.

For more information on issues and events that shape our world, please visit the ISN Blog and browse our resources.

Brian Finlay is a senior associate and director of the Managing Across Boundaries program at the Stimson Center.

Publisher

International Relations and Security Network (ISN)

---

http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=181068&lng=en

---