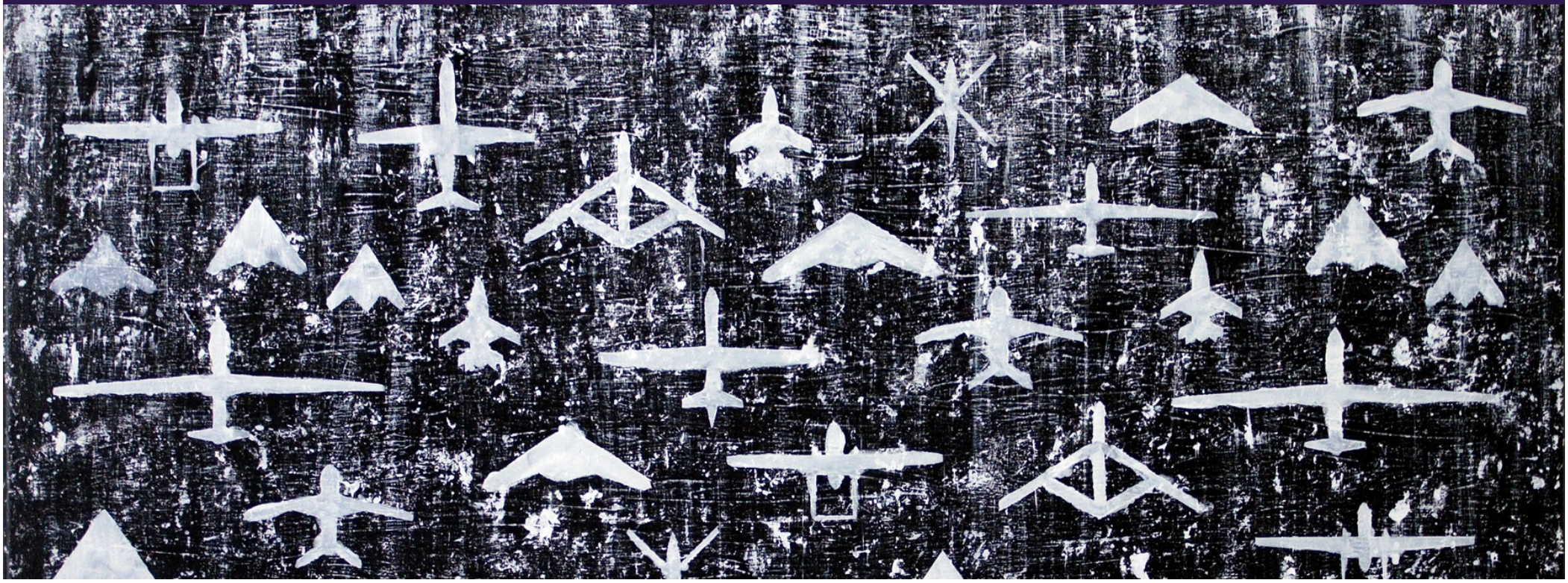

Drugs and Drones: The Crime Empire Strikes Back

Vanda Felbab-Brown

24 February 2016

This article is part of the Remote Control Warfare series, a collaboration with Remote Control, a project of the Network for Social Change hosted by Oxford Research Group.

Editor's note: *Remote Warfare and the War on Drugs mini-series: This series of articles explores how remote warfare is being used in the war on drugs. To date, much of the debate on remote warfare has focused on its use in the war on terror. However, the use of drones, private military and security companies (PMSCs), special forces and mass surveillance are all emerging trends found in the US's other long standing war, the War on Drugs. The articles in this series seek to explore these methods in more depth, looking at what impact and long term consequences they may have on the theatre in which they're being used. Read other articles in the series.*

Latest

An Update on the Security Policy Change Programme

Chances for Peace in the Third Decade

A Story of ORG: Oliver Ramsbotham

A Story of ORG: Gabrielle Rifkind

Most read

The Role of Youth in Peacebuilding: Challenges and Opportunities

Making Bad Economies: The Poverty of Mexican Drug

> **“ Ever advancing remote warfare technology is being increasingly used by law enforcement agencies to counter drug trafficking. In response, drug cartels are also adopting new technology to smuggle and distribute drugs. However, the technological superiority of law enforcement-military actors is also causing criminal and militant groups to adapt by employing the very opposite tactic, by resorting to highly primitive technology and methods. In turn, society is doing the same thing, adopting its own back-to-the-past response to drug trafficking and crime. ”**

Cartels

ORG's Vision

Remote Warfare: Lessons Learned from Contemporary Theatres

The history of drug trafficking and crime more broadly is a history of adaptation on the part of criminal groups in response to advances in methods and technology on the part of law enforcement agencies, and vice versa. Sometimes, technology trumps crime: The spread of anti-theft devices in cars radically reduced car theft. The adoption of citadels (essentially saferooms) aboard ships, combined with intense naval patrolling, radically reduced the incidence of piracy off Somalia. Often, however, certainly in the case of many transactional crimes such as drug trafficking, law enforcement efforts have

tended to weed out the least competent traffickers, and to leave behind the toughest, meanest, leanest, and most adaptable organized crime groups.

Increasingly, organized crime actors have adopted advanced technologies, such as semi-submersible and fully-submersible vehicles to carry drugs and other contraband, and cybercrime and virtual currencies for money-laundering. Adaptations in the technology of smuggling by criminal groups in turn lead to further evolution and improvement of methods by law enforcement agencies. However, the use of ever fancier-technology is only a part of the story. The future lies as much behind as ahead (to paraphrase J.P. Wodehouse), with the asymmetric use of primitive technologies and methods by criminal groups to counter the advanced technologies used by law enforcement.

The Seduction of SIGINT and HVT

The improvements in signal intelligence (SIGINT) (information gained by the collection and analysis of the electronic signals and communications of a given target) and big-data mining (the extracting of useful information from large datasets or streams of data) over the past two decades have dramatically increased tactical intelligence flows to law enforcement agencies and military actors, creating a more transparent anti-crime, anti-terrorism, and counterinsurgency battlefield than before. The bonanza of communications intercepts of targeted criminals and militants that SIGINT has come to provide over the past decades in Colombia, Mexico, Iraq, Pakistan, Afghanistan, and other parts of the world has also strongly privileged high-value targeting (HVT) and decapitation policies-i.e., principally targeting the presumed leaders of criminal and militant organizations.

The proliferation of SIGINT and advances in big-data trawling, combined with some highly visible successes of HVT, has come with significant downsides. Although high-value targeting has been effective, this has only occurred under certain circumstances. In many contexts, such as in Mexico, HVT has been counterproductive, fragmenting criminal groups without reducing their proclivity to violence; in fact, exacerbating violence in the market. Other interdiction (the targeting of opponent's organizational structures or disrupting their logistical chains) patterns and postures, such as middle-level targeting and focused-deterrence, would be more effective policy choices.

A large part of the problem is that the allure of signal intelligence has led to the discounting of other key intelligence techniques, including developing a strategic understanding of criminal groups' decision-making in order to anticipate the responses of targeted nonstate actors to law enforcement actions (here Mexico provides a disturbing example). It also requires the cultivation of human intelligence assets (sorely lacking in Somalia, for example) and obtaining a broad and comprehensive understanding of the motivations and interests of local populations that interact with criminal and insurgent groups (notably deficient in Iraq, Afghanistan, and Pakistan). Finally, establishing good relationships with local populations to advance anti-crime and counterinsurgency policies is essential. In Colombia, for example, drug eradication policy antagonized local populations from national government and strengthened the bonds between them and rebel groups.

In other words, the tactical tool, technology – in the form of signal intelligence and big-data mining – has trumped strategic analysis. Instead, strategic intelligence analysis needs to be brought back, to drive interdiction targeting patterns, instead of letting the seduction of signal data drive intelligence,

analysis and targeting action. Indeed, the political effects, as well as the anticipated responses by criminal and militant groups, and any other outcomes of targeting patterns, need to be incorporated into the strategic analysis. Questions to be assessed need to include: Can interdiction hope to incapacitate – arrest and kill – all of the enemy or should it seek to shape the enemy? What kind of criminals and militants, such as how fractured or unified, how radicalized or restrained in their ambitions, and how closely aligned with local populations against the state, does interdiction want to produce?

Dogs Fights or Drone Fights: Remote Lethal Action by Criminals

Criminal groups have used technology not merely to foil law enforcement actions, but also to fight each other and dominate the criminal markets and control local populations. In response to the so-called Pacification (UPP) policy in Rio de Janeiro through which the Rio government has sought to wrestle control over slums from violent criminal gangs, the Comando Vermelho (one of such gangs), for example, claimed to deploy remote-sensor cameras in the Complexo do Alemão slum to identify police collaborators, defined as those who went into newly-established police stations. Whether this specific threat was credible or not, the UPP police units have struggled to establish a good working relationship with the locals in Alemão.

The new radical remote-warfare development on the horizon is for criminal groups to start using drones and other remote platforms not merely to smuggle and distribute contraband, as they are starting to do already, but to deliver lethal action against their enemies – whether government officials, law enforcement forces, or rival crime groups.

Eventually, both law enforcement and rival groups will develop defenses against such remote lethal action, perhaps also employing remote platforms (drones to attack the drones). Even so, the proliferation of lethal remote warfare capabilities among criminal groups will undermine deterrence, including deterrence among criminal groups themselves over the division of the criminal market and its turfs. This is because remotely delivered hits will complicate the attribution problem – i.e., who authorized the lethal action — and hence the certainty of sufficiently painful retaliation against the source and thus a stable equilibrium.

More than before, criminal groups will be tempted to instigate wars over the criminal market with the hope that they will emerge as the most powerful criminal actors and able to exercise even greater power over the criminal market – the way the Sinaloa Cartel has attempted to do in Mexico even without the use of fancy technology. Stabilizing a highly violent and contested – dysfunctional – criminal market will become all the more difficult the more remote lethal platforms have proliferated among criminal groups.

Back to the Past: The Ewoks of Crime and Anti-Crime

In addition to adopting ever-advancing technologies, criminal and militant groups also adapt to the technological superiority of law enforcement-military actors by the very opposite tactic — resorting asymmetrically to highly primitive deception and smuggling measures. Thus, both militant and criminal groups have adapted to signal intelligence not just by using better encryption, but also by not using cell phones and electronic communications at all, relying instead on personal couriers, for example, or by flooding the e-waves with a lot of white noise. Similarly, in addition to loading drugs on drones, airplanes, and submersibles, drug trafficking groups are going back to very old-methods such

as smuggling by boats (including through the Gulf of Mexico), by human couriers, or through tunnels.

Conversely, society sometimes adapts to the presence of criminal groups and intense, particularly highly violent criminality by adopting its own back-to-the-past response – i.e., by standing up militias (which in a developed state should have been supplanted by state law enforcement forces). The rise of anti-crime militias in Mexico, in places such as Michoacán and Guerrero, provides a rich example of such populist responses and the profound collapse of official law enforcement. The inability of law enforcement there to stop violent criminality – and in fact, the inadvertent exacerbation of violence by criminal groups as a result of HVT – and the distrust of citizens toward highly corrupt law enforcement agencies and state administrations led to the emergence of citizens' anti-crime militias. The militias originally sought to fight extortion, robberies, theft, kidnapping, and homicides by criminal groups and provide public safety to communities. Rapidly, however, most of the militias resorted to the very same criminal behavior they purported to fight – including extortion, kidnapping, robberies, and homicides. The militias were also appropriated by criminal groups themselves: the criminal groups stood up their own militias claiming to fight crime, where in fact, they were merely fighting the rival criminals. Just as when external or internal military forces resort to using extralegal militias, citizens' militias fundamentally weaken the rule of law and the authority and legitimacy of the state. They may be the ewoks' response to the crime empire, but they represent a dangerous and slippery slope to greater breakdown of order.

In short, technology, including remote warfare, and innovations in smuggling and enforcement methods are malleable and can be appropriated by both

criminal and militant groups as well as law enforcement actors. Often, however, such adoption and adaptation produces outcomes that neither criminal groups nor law enforcement actors have anticipated and can fully control. Technology cannot fix defecting anti-crime and anti-drug policies, such as preoccupation with drug seizures , or absent rule of law and culture of lawfulness. Advances in technology do not obviate the need to strengthen bonds between citizens and the state and to create law enforcement and socio-economic conditions which allow citizens to internalize laws. Nonetheless, crime and some illegal economies will always persist and law enforcements and criminals will compete with each other in adopting improving technologies and finding measures to counter them, including most primitive but effective ones. The criminal landscape and military battlefields will thus increasingly resemble the Star Wars moon of Endor: drone and remote platforms battling it out with sticks, stones, and ropes.

Artwork of drone warfare by JJprojegts.

Dr. Vanda Felbab-Brown ***is a senior fellow in Foreign Policy at the Brookings Institution and co-director of the Brookings projects on Improving Global Drug Policy: Comparative Perspectives and UNGASS 2016 and Reconstituting Local Orders. Dr. Felbab-Brown is an expert on illicit economies and organized crime and international and internal conflicts and their management, including counterinsurgency and statebuilding. Her research focuses particularly on South Asia, Burma, the Andean region, Mexico, and Somalia, and she has conducted fieldwork in some of the most dangerous parts of the world. Dr. Felbab-Brown has an extensive publication list of books, policy reports, academic articles, and opinion pieces, including Poached: Combating Wildlife Trafficking, with***

Lessons from the War on Drugs (forthcoming 2016); Narco Noir: Mexico's Cartels, Cops, and Corruption (forthcoming 2016); Aspiration and Ambivalence: Strategies and Realities of Counterinsurgency and State-building in Afghanistan (2013); and Shooting Up: Counterinsurgency and the War on Drugs (2010). Dr. Felbab-Brown is a frequent consultant for national, multilateral, and non-governmental organizations and a frequent commentator in U.S. and international media. She also regularly provides expert testimony to the US Congress. Prior to joining the Brookings Institution, Dr. Felbab-Brown was an Assistant Professor at the Georgetown University School for Foreign Service. She received her PhD in political science from MIT and her BA from Harvard University.

020 3559 6745