Home Made, Printed, and Remote Controlled Firearms—Terrorism and Insurgency Implications

Robert J. Bunker
Claremont Graduate University

Recommended Citation
Home Made, Printed, and Remote Controlled Firearms— Terrorism and Insurgency Implications

This essay in the TRENDS terrorism futures series focuses on trends in the manufacturing of homemade and printed firearms along with the emergence of remote (teleoperated) firearms. Each of these trends is discussed in turn in this short essay, as are the implications of their cumulative effects on terrorism and insurgency. Ultimately, as will be highlighted in this piece, both physical and cyber forms of terrorism are increasingly merging as a result of firearm and computer components becoming more closely integrated [1].

Home Made Firearms

In October 2014, Jalisco’s Attorney General stated that two clandestine arms factories in Guadalajara, Mexico linked to the Cártel de Jalisco Nueva Generación (CJNG) were raided by Mexican authorities in cooperation with the US government [2]. This is the same violent cartel responsible for ambushing scores of Mexican police officers, closing down entire cities with burning car and bus roadblocks and mass building arson, and even, in May 2015, shooting down a Mexican military helicopter with rocket propelled grenades (RPGs).

Two converted residences—the first of their kind ever discovered in Mexico—were used to assemble AR-15 assault rifle components purchased legally online with no background checks in the United States. Parts of homemade guns can be purchased in this manner as long as the receivers—the mechanical part which cycles, fires, and ejects the bullets—are only about 80% partially built. Such unfinished receivers were then completed in these underground weapons factories by specialized milling machines and fitted to other AR-15 components to create well over a hundred finished firearms prior to their being shutdown [3]. Such an off-the-books firearm has no production serial
number or original registered owner to trace it back to and, for all intents and purposes, thus really
does not even exist.

The emerging trend towards the production of homemade assault rifles, derived from unfinished
parts, has until recently been largely unrecognized. A particular gun parts seller with one store in
California and another in Florida estimated that they would sell about 75,000 unfinished receivers in
2014 alone. Such clean—that is non-serialized and unregistered—weapons are increasingly being
used by gang members in the United States and by criminal organizations and the cartels
throughout parts of Latin America including Mexico and Colombia. To date, hundreds of such
finished AR-15 and AK-47 style weapons have been recovered by the US ATF alone [4]. Such
weapons, however, do not appear to have as of yet proliferated to more traditional terrorist and
insurgent groups such as Al Qaeda and Islamic State. This is likely the case because those groups
tend to operate in conflict environments in which black market arms are relatively easy to obtain.
Further, they are also able to readily engage in outright governmental arsenal seizures as has taken
place in Iraq, Syria, and Yemen whenever the opportunity presents itself.

Still, the severity of this homemade guns assembly issue has now resulted in the release of ATF Rul.
2015-1 in January 2015 that addresses the ‘80% receivers’ legal loophole [5]. Whether this ruling will
also help to facilitate the eventual shutdown of online sales of such receivers and gun kits from non-
US online sellers is unknown. However, 3D printing technology is rapidly advancing to the point that
purchasing gun parts online for home assembly will one day become obsolete anyway. Such
trending operates in much the same way that internet music downloads have replaced earlier sales
of physically based compact disk (CD) music.

Printed Firearms
The first 3D plastic printed gun—‘The Liberator’—was created in May 2013. It was a single shot
pistol design with a very limited operational lifespan [6]. Soon after that gun was printed—with
100,000 online printing files downloaded by the general public prior to the computer schematics
being taken down by the US government—a long series of printed guns were produced that were
cheaper to create and more durable and functional in their design. In July 2013, the first printed
plastic rifle was produced [7] and, by November 2013, a metal 1911 .45 Caliber pistol was printed
[8]. In 2014, special bullets designed for 3D printed guns were then created, and, in 2015, a much
heavier Colt Cm901 7.62mm assault rifle had been printed along with a metal silencer [9]. Additional
3D printing breakthroughs are expected to continue to take place.

Printed gun advances—along with the initial printing of plastic AR-15 receivers as has already taken
place—may soon create a synergy with CNC milling technology. As early as September 2014,
computer milling allowed for finished aluminum AR-15 receivers to be produced in sizeable quantities by a $1,200.00 CNC mill known as the ‘Ghost Gunner’ [10]. While no mention of the 3D metal printing of AR-15 receivers has been noted, it is only a matter of time before this capability is achieved. Combined with cheap CNC mills and the ability to print all AR-15 components in metal, the new ATF Rul. 2015-1 will pretty much become meaningless.

As would be expected, 3D printing had caught the attention of ‘early adaptor’ criminals as early as 2011 with designs on printing plastic car and handcuff keys and high capacity assault rifle magazines [11]. It was initially thought that the first illicit 3D printed gun factory had been raided in Manchester, United Kingdom in October 2013, but this turned out to be unfounded [12]. An illicit 3D firearm printing operation was actually discovered in May 2014 in Japan belonging to an individual subsequently charged with criminal possession of multiple firearms [13]. More incidents have taken place with what appear to be plastic 3D printed gun parts belonging to a drug dealer being seized in Australia in 2015 [14].

While concerns over potentials for terrorists printing weapons have been made known by governmental and police officials in multiple countries and many 3D weapons printing bans have been enacted, no known incidents in which terrorists or insurgents have printed firearms have as of yet have been identified [15]. This is likely due to the same reasons that such groups are not yet assembling home made firearms—it is presently much simpler and easier to either purchase them on the black market or raid police and military weapons depots and steal them. Still, the trending potentials are clear, as is the rapidly evolving nature of these weapons. In fact, the next frontier for 3D printing will be that of remote operated systems where by gun parts will be printed with integrated computer circuits to create hybrid firearm-computer systems. This leads us to our next firearms technology use trend.

**Remote Controlled Firearms**

Concerns over terrorist use of teleoperated (remote) firearms that can be physically fired in one location while the operator is in another location have existed for over well over a decade now. Initially these were notional and science fiction derived perceptions, however, contemporary advances in technology and actual incidents in which they have been used have now made these viable concerns. While a remotely fired sniper rifle set up in a bell tower mimicking the August 1966 University of Texas massacre sans the physical presence of the shooter may seem a stretch of the imagination, this is now easily achievable for terrorist utilization.

The initial indication of the possibility of remote firearm use potentials by terrorists took place with the development of the Live-Shot virtual hunting system. The system was marketed by a Texas
company so that disabled hunters could shoot Whitetail Deer. Conceived as early as 2003 and created in 2005 after an investment of about $15,000, the system consisted of a rifle mounted on a motorized platform controlled by a computer linked to the internet. A remote user, utilizing their own computer system via the internet in another location, could control the operation of the rifle—the aiming and firing of it—in real time via a camera link [16]. Immediate backlash against the system took place due to public outrage, with a resulting widespread ban on internet hunting in the United States since being enacted [17].

While the Live-Shot system turned out to be a failed business venture, conceptually the ability to aim and shoot a firearm via an internet linked computer was proven beyond a doubt. All that was then required was to change the intended target from a deer to a human. This took place by at least 2013 with the TRAP T192 Remote Sniper Kit being commercially offered by a security products company for both ambush and counter-sniper applications. The kit comes with solar-powered battery charging that allows for weapons system placement loitering capability [18]. That same year, a Wi-Fi capable precision guided firearm (PGF) was also offered commercially by a different company. It allowed a user with a smart phone or tablet to activate, via a unique PIN system, a computer guided aiming system that offers trained sniper equivalent targeting capabilities [19]. No actual instances of the use of these systems in media reports have been noted [20].

Actual battlefield use did take place in March 2013 and July 2014 by FSA (Free Syrian Army) fighters utilizing remote controlled sniper rifles. This fielding of two improvised systems occurred in Syria with videos of their use placed on online social media. In both instances, a short control cable from the weapon is connected to a user with a small tablet/controller around an interior corner of a building so that counter-sniper fires will not target them. In the latter video, the weapon is being fired unlike in the initial video [21]. A video posting in June 2013 of a FSA remote controlled machine gun being fired has also surfaced [22]. Purported Islamic State affinity chats have since taken place in January 2015 related to the ‘remote control technique’ (translated from Arabic) for firing weapons [23]. Combined with a recent discussion of the Ansar al-Islam use of a remote controlled truck with a machine gun bed mount [24], this would suggest that both terrorist and insurgent organizations are beginning to become well aware that remote control firearm technologies exist and offer unique tactical battlefield applications.

**Terrorism and Insurgency Implications**

The above firearms trends can be viewed as a compliment to homemade IED manufacturing and remote detonation that have existed for decades now. Basically, a more discriminate point—and to some extent area—firearms targeting capability is emerging to compliment the earlier non-
discriminate area targeting capability that has long existed with smaller IED and larger VBIED use. This will result in new terrorist and insurgent capabilities eventually being gained in the areas of:

- **Remote Sniping**—the shooter is both protected from harm (has removed himself or herself from the battlefield) and, via a stabilized platform and computerized aiming system, is able to engage in the precision engagement of point targets like a sniper.

- **Virtual Targeting Presence**—that is, having the ability to threaten potential targets in a specific area for long durations by means of remote sensing overwatch. Additionally, proximity and motion detector alerts that notify the remote firearm user of any human activity 24/7 can be utilized for longer extended periods of time.

- **Remote Combined Arms**—creating interlocking remote controlled fields of fire with remote detonated IEDs for both offensive terrorist targeting purposes and defensive channeling and urban kill zone utilization by insurgent forces.

These homemade, printed, and remote controlled trends are also resulting in firearm and computer integration for both weapon manufacturing and utilization needs. This experimental merging of firearm and computer has been progressing in fits and starts for a while now. It can be seen in the initial next generation U.S. conventional military systems attempt via the OICW (Objective Individual Combat Weapon)—with its onboard computer utilized for grenade round air bursting solution calculations—that would have engaged opposing forces in defilade positions that are protected from direct fires.

As described in the earlier sections, terrorist and insurgent organizations will also benefit from the self-manufacturing of firearms as a means to bypass black market weapons constraints—especially in states with strong anti-arms smuggling regimes—as well as in the repair of broken firearms with the metal printing of precision replacement parts.

While none of these implications will significantly alter the ‘disruptive’ and ‘terror’ generating components of terrorism itself, they may alter some of its weapons procurement logistical requirements and potentially even allow for the generation of greater numbers of casualties during a specific terrorist incident while at the same time greatly reducing terrorist casualties in return. Additionally, such incidents would likely help to blur our understanding of both physical and cyber forms of terrorism, as they presently exist. This would result in unique counterterrorism dilemmas being created that would ultimately require new and innovative response and intelligence protocols being developed by police and state security forces.

*Notes*


While it is assumed that only legitimate governmental, law enforcement, and associated entities may purchase these remote controlled systems, the actual vetting process has not been determined.

[22] “Raw Video FSA Machine Gun.” *YouTube*. 2 June 2013, [https://www.youtube.com/watch?v=k6O98j3z9so#t=19](https://www.youtube.com/watch?v=k6O98j3z9so#t=19).


Tags: Firearms Homemade firearms insurgency remote controlled firearms terrorism