EVALUATING THE IED THREAT IN UKRAINE THROUGH THE USE OF SOCIAL MEDIA

OPEN SOURCE INTELLIGENCE (OSINT)

The rapid development of the internet and the ability of the user to access, store and disseminate vast quantities of electronic data from anywhere in the world, has provided a new means for militant groups to expand their recruitment, training and propaganda efforts to reach a global audience. It has also provided a rich seam of open source (overt and publicly available) data of increasing value to intelligence agencies in their efforts to understand and counter the terrorist threat.

List-X Company, Allen Vanguard Counter-Threat Solutions (AVCTS), specialising in open source intelligence (OSINT) and counter improvised explosive devices (IEDs), has seized upon this opportunity, and today its team of researchers and analysts use OSINT to monitor IED activity around the world.

SOCIAL MEDIA

Of all the open source materials available interactive social media has recently risen to the fore as one of the most valuable and underexploited resources. Militant groups, always fast to adapt to new technologies, have been quick to harness the reach and potential of this resource using it to spread videos of their campaigns, recruitment materials and instructional videos to a global audience.

Whilst at first restricted to basic and often obscure blogs and forums the rapid growth of social networking sites, and an influx of young media savvy recruits has increased the capability and reach of these groups exponentially. The move from heavily moderated forums to the ubiquitous social media platforms brought with it potential audiences of tens of millions of users. Content can be spread across prominent global sites such as Facebook, YouTube and Twitter as well as lesser known, region specific and up and coming networks not widely utilised in the West or by the English speaking community, such as the Russian site VKontakte or Chinese blogging site Weibo. In this manner groups are able to directly contact potential recruiters and financers rather than going through traditional channels such as direct contact.

... OF ALL THE OPEN SOURCE MATERIALS AVAILABLE INTERACTIVE SOCIAL MEDIA HAS RECENTLY RISEN TO THE FORE AS ONE OF THE MOST VALUABLE AND UNDEREXPLOITED RESOURCES ...

Each of these resources typically competes for a share of the market by presenting the user with a unique means of sharing data. For example, whilst

Twitter limits its users to concise messages linked to hashtags searchable by the network's entire user base, other sites such as Facebook offer a wider range of content shared to pre-approved contacts. Militant groups are likely to operate across a range of platforms, selecting the one whose features best fit their purpose. Somalia based Al-Shabaab for example used Twitter to provide a running commentary on its attack on the Westgate mall in Nairobi before security forces could comment, thus controlling the narrative from the beginning. Alternatively, far-right groups have utilised sites such as Facebook to provide a monitored platform for their supporters to share their views, organise events and conduct recruitment campaigns.

Perhaps the most prominent group to utilise social media has been Islamic State (IS). The group has been impressive in its ability to discover and exploit new social media platforms and information sharing websites. It uses these sites as part of a coordinated media strategy imitating and surpassing the campaigns of even multinational corporations.

> ...THE ISLAMIC STATE GROUP USES SOCIAL MEDIA PLATFORMS AND INFORMATION SHARING WEBSITES AS PART OF A COORDINATED MEDIA STRATEGY...

However, there are limitations to their capabilities; the majority of these organisations have existed in regions in which internet usage is limited to location, affluence or state controls. Some militant organisations are able to provide sporadic cover whilst others have been able to tightly control their output, presenting a problem for the OSINT researcher concerning the reliability of the source.

UKRAINE

An exception to the above issue is the recent separatist conflict in Ukraine. The population hosts a level of internet connectivity equivalent to that of a Western European nation. The vast majority of its citizens have experience interacting with social media and access to a variety of platforms for uploading content. For the first time both militant groups, security forces and perhaps most importantly civilians have been able to document the conflict around them from its opening days.

This provides a unique opportunity to witness conflict in an area largely closed off to the independent media and foreign observers. Through the monitoring of social media it is possible to chart the development of IED use throughout the conflict. Invaluable information to any force which finds itself operating in the affected regions or involved in demining or other disarmament roles.

BACKGROUND TO THE CONFLICT

Ostensibly a separatist conflict between the so called 'Novorossiya' region, a consolidation of the 'Donetsk and Lugansk Peoples' Republics of Eastern Ukraine and the remainder of the country, the fighting is a microcosm of a wider conflict between Russian and Western interests. The separatist militants are financed, equipped and possibly even supplemented by Russian forces, whilst a number of nationalist volunteer militias locally known as 'battalions' operate alongside Ukrainian security forces. These militias are also believed to have the backing of private individuals outside of the Ukrainian government and often operate outside of existing command structures.

IED usage to date has almost entirely consisted of adapted munitions, partially due to the large amounts of conventional weaponry readily available to both sides. Throughout the course of the range of these adaptations the purpose of these weapons has undergone a number of developments.

In the initial days of the conflict IEDs were used to secure or deny routes into or from the main cities within Eastern Ukraine. From 07 July 2014 to 21 July 2014 at least ten road and rail bridges were demolished through the use of explosives. Both sides were believed to be responsible for the destruction.

Figure 1. Image of AT mines adapted to function against the stanchions of a road bridge.
(VKontakte, 12 September 2014)

An image widely shared on social media site VKontakte by separatist sources (Figure 1) shows a bridge located near the government held south eastern city of Mairupol, prepared for demolition by nationalist militias.

The image features 18 AT mines, likely TM-62Ms, secured to the upper and lower sections of nine bridge stanchions, with the upper side of the mine facing the pillar. The mines are placed flat against the stanchions suggesting that the fuze has been removed or adapted in some way. It is likely that the crossed fabric or rubber strips which are visible on the back of the mines are there to hold some form of improvised fuze in place on the face of the device. The devices are linked, likely by detonating cord, seemingly so that they can be functioned simultaneously.

Additional concrete slabs, have been placed against the lower mines, likely in order to further secure them in place as well as attempting to further direct the charge toward the stanchion. If functioned the devices would cause significant damage to these supports and in all probability collapse the structure; however, a set-up involving the placing of devices on each side of the stanchion, to create a sheering moment, would likely be more effective.

CACHE FINDS

On 07 August 2014 a Russian supplied weapons cache was found to include 12 IEDs (Figure 2).

Figure 2. A cache find containing timed IEDs.
(Twitter, 07 August 2014)

Figure 3. Damage to Separatist leader Denis Pushilin's vehicle in Donetsk.
(Twitter, 12 June 2014)

The devices appear to be improvised grenades constructed using cast iron water heating pipes as an outer casing. Grooves have been cut into the casing, as evidenced by the lack of rust apparent in these sections, likely in an attempt to improve the fragmentation and a welded hexnut on the top acting as an entrance hole for a burning fuze. The fuzes themselves are short and probably give approximately five or so seconds of delay. They are likely filled with black powder or some other form of improvised igniferous mixture such as sodium chlorate or potassium nitrate and sugar.

The design has several shortcomings. The use of grooves in the outside of the casing will slightly improve the fragmentation effect; however, this would be more efficient if cut on the inside of the device, although this is admittedly much more difficult to accomplish. The tops of the burning fuzes are open; in handling, some powder may fall out and alter the burn rate of the fuze itself. A simple measure such as tape or a wax seal over the end would prevent this. One of the devices has a wider diameter than its counterparts suggesting construction using a varying or limited supply of piping.

A question raised by the presence of these devices is why they are needed in an area which ostensibly has access to a range of conventional Russian supplied weapons, including conventional grenades. The discovery suggests two possible likely scenarios. Either Russian supplies are not as far reaching or plentiful as previously reported or that the separatists require the use of IEDs for purposes of deniability.

TARGETED KILLINGS

One of the primary roles IEDs have played in the conflict has been their role in targeted killings.

On 12 June 2014 there were reports of a possible IED attack targeting the vehicle of Denis Pushilin, the self-proclaimed leader of the People's Republic of Donetsk (DNR). Three people were killed including one of Pushilin's security detail, an aide and an unidentified civilian whilst the driver and three other civilians were injured. Pushilin himself was not in the vehicle at the time.

Post-incident imagery (Figure 3) shows significant fire damage to the vehicle which appears to be relatively intact. No fragmentation or significant blast

Figure 4. (Left) a UAV adapted to carry an RGO grenade and its payload (Right).
(VKontakte, 27 October 2014)

damage to the vehicle panels or crater is visible. The imagery is consistent with a device of a low Net Explosive Quantity (NEQ) being placed inside or possibly underneath the vehicle.

It is probable that the device was placed underneath or near the passenger section of the vehicle.

Separatist militants claimed that Ukrainian security forces were responsible; however, there was no official comment on the incident.

Separatist militants have also extended their reach outside of the conflict area and into the rest of Ukraine. A number of militant cells have been discovered and detained in major cities.

On 09 November 2014 a timed IED, placed inside a bag, functioned inside the Stena (Wall) bar in Kharkiv, Kharkiv Oblast, injuring up to 11 people. The device had been left near the bar and utilised nails as additional fragmentation

Witness accounts and post-attack imagery indicate that the device was placed inside the building near the bar. It was contained in a bag of an unknown type and utilised nails as additional fragmentation.

UNMANNED AERIAL VEHICLES (UAV)

Ukraine, with its ready access to commercially available materials, has also become a testing ground for new IED concepts. On 27 October 2014 a VKontakte account associated with separatist militant forces released images of a commercially available UAV adapted as a delivery system for an IED (Figure 4).

The device itself consists of an RGO hand grenade, containing a main charge of 0.5kg of TNT, with metal bolts to provide additional fragmentation. The device is contained and secured to the UAV by duct tape which is in turn connected to a metal cable suspended below the UAV. No method of initiation is apparent; however, the RGO grenade differs from the far more widely available RGD variant in that it can be fitted with an impact fuze. It is possible the operator intended to utilise this function by either disconnecting the cable letting the device fall, or by flying the UAV itself directly into the target. In the images, the grenade pin is still in place lending credence to the theory that the device still utilises its original fuze and safety features.

Although the UAV cannot be identified, similar sized models have a flight time of approximately 18 minutes, without the addition of a payload. The maximum operational range and flight ceiling are typically cited as 1.5km but are likely determined by flight time, particularly if the operator intends to recover the UAV. A number of these models are able to carry cameras underneath the device with a payload capacity of up to 0.7kg.

Whilst no footage of the device in action has been made available, and the weight of the device is approaching the upper limits of the UAVs capacity the concept is assessed as being achievable.

CONCLUSION

IED use in Ukraine is heavily based on the adaptation of conventional explosives and weapons readily available in the country. To date this activity has largely been contained to the separatist held regions; however, a key concern for the future is that the failure to find a diplomatic solution increases the risk of IED attacks occurring elsewhere in the country.

Separatist militants have already demonstrated a willingness to target civilian areas with a known connection to nationalist forces. They are also known to have cells active in these cities and in cities of interest to separatist forces. It is likely that further IED attacks are planned and that Ukraine will see an increase in such activity targeted at prominent individuals, government and civil structures and pro-Ukrainian events or meetings.

A second risk is that nationalist militias, who although linked to the Ukrainian security forces, exist outside any military or political command structures may carry out retaliatory attacks of their own in separatist held regions.

More alarmingly, militants have demonstrated a willingness to experiment with new technologies, which are readily available in the region. By posting their finds on social networking sites these groups can readily share images of new devices, their operational capabilities and their construction with allied groups as well as those with whom they have no direct connection.

The above article demonstrates that the use of social media as primary source, combined with high quality analytical reporting, makes it possible to chart the development of IED use in an area which would have otherwise remained inaccessible. At the same time these images exist as both a propaganda source and a means of sharing technical and operational information with other militant organisations.

Although Western intelligence agencies have access to classified sources, these are not always readily available and may not be timely. OSINT is widely available and through the use of social media sites material can potentially be available within minutes of an IED event occurring. This data can be used to chart both the development of the conflict as it occurs as well as corroborating intelligence gained through other sources. As such, continued monitoring of open source data is critical to any counter-IED, demining or humanitarian agency with plans to operate in Ukraine. ■