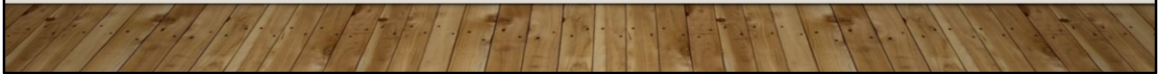


COMMUNICATIONS TECHNOLOGY IN CT



DR ROBERT DOVER – UNIVERSITY OF LEICESTER – PREPARED 11 MAY 2016
FOR: TERRORISM AND COUNTER TERRORISM: A PAKISTANI PERSPECTIVE
AT IMPERIAL COLLEGE OF BUSINESS STUDIES (ICBS), LAHORE



ICT AS RADICALISATION

- Self-starters have been seen to radicalise via deep web content
- Training has been delivered via dark web, so removing the need to travel.
- Countermeasures are restricted to technical interventions (eg electronic surveillance), human intelligence or community relations.



CROWDSOURCING OPERATIONALART?



The January and November 2015 attacks on Paris demonstrated a good level of military training amongst the attackers (they all fired and maneuvered in the style of trained soldiers). In European standards they were also very well armed.

The attacks (including the Brussels attack) demonstrated a high degree of learning between operations, one in which ubiquitous social media and regular media has played an unwitting part.

The January attacks clearly had a plan, but were not planned to the tiniest detail: the Kouachi brothers asked directions to the Charlie Hebdo building, had to force someone at gun point to let them in the building and had to do a full search of the building to find the targets. They clearly anticipated being confronted by security forces, but ended up driving out of the city and up and down a motorway in what could be viewed as an attempt to attract attention.

The November attacks were again planned, but again quite loosely. The plan to gain access to Stade de France was dependent on being able to convince or coerce entry. The bars that were attacked seemed to be done randomly, whilst the area seemed to be pre-chosen. The media commentary about the TATP bomb vests might have

contributed to changes that rendered them more effective in the Brussels attacks. And the Brussels attacks seemed far better planned.

We would naturally assume military forces to learn and evolve. How possible this is when the vast majority of attackers perish in the attack lends itself to thinking the media (both regular and social) are unwitting assistants in this effort.

MANAGING THE MESSAGE



This era of what is called in the west as ‘jihadist terrorism’ was first seen in the war against the USSR in the early 80s, but predominantly the former Yugoslavia in the 1990s. At this stage the jihadists were pursuing foreign policy agendas that were aligned to western interests – hence funding and arming.

It brings out a reality of some young men just want to fight – we know this isn’t just a problem in our Islamic communities, because recruitment to our armed forces also depends on this motivation.

The question is, then, why people choose to fight for these irregular armies:

Partly it has been because of wars in Iraq and Afghanistan (plus Guantanamo, plus Abu Ghraib) as neo-imperialist adventures

Partly it is because of the perceived glamour of ISIS, matched to professional propaganda

Partly it is an issue of identity and belonging.

Jihadists have been far better at managing the message than western governments. Only very recently have western powers announced offensive cyber capabilities to

disrupt multi-channel media efforts.

WARS IN CYBER-SPACE: ISIS VS ANONYMOUS



There is a war being conducted in cyber space between ISIS, government intelligence agencies and security forces, and unaligned activist groups such as an anonymous.

Anonymous have pledged to attack ISIS online activities and has successfully taken down many websites, online accounts and so on.

ISIS appear to have been successful in attacking some high value news media targets, as well as government computer infrastructure. We can reasonably assume that part of their income is derived from hacking activities online.

With the increased transparency of SWIFT brought about after the 9/11 attacks, the growing popularity of crypto-currencies such as bitcoin has provided terrorist groups with an alternative place to put funds, but these are subject to high pricing volatility. So there's a trade-off between anonymity and pricing vagaries (as well as no underpinning value, as there is in state-backed currency).

ENCRYPTION AND ASYMMETRY



So, whilst the November 2015 attackers didn't use encryption on their phones as they attacked (making the correct assessment that live interception of burners was difficult), it has become a significant policy issue in Europe. The short message service – Whatsapp, owned by Facebook – has incorporated end to end encryption into its service, which law enforcement officials have bitterly complained about. The Russian designed 'Telegram' platform, which also has end to end encryption has been said to be used by jihadists, prompting the operators to say they would remove extremist materials.

There are a large number of commercially available encryption email services, and encryptions for web-traffic. Services like TOR (the onion ring, designed by US Navy) also offer some protections to people seeking to hide what they're doing. They might have legitimate, whistleblowing reasons to do so.

Asymmetric communications are also now a feature: the use of messaging during cooperative play on video games or pre-planned firing patterns during cooperative play are the modern day equivalent of secret coding or dead letter drops, and are almost impossible to detect.

“WE’RE OFF...WE’RE STARTING”



- Abaaoud directed operations from the ground and from a 'burner phone'
- The smartphones used were unencrypted
- The modus operandi is one where there was a plan, but it was not highly detailed. This implies a level of innovation and manoeuvre

NOVEMBER ATTACKS



A DANGEROUS MEDIA?



Censorship has been a feature of western medias in modern times. During the whole of the 20th century the British government has retained the right to censor news media coverage at moments of war or acute security related tension. This played out most obviously during the two world wars, and the Falklands conflict where information deemed to be sensitive was forcibly redacted for operational reasons.

In less tense times the D-Notice system has – by convention – required news media to redact sensitive stories.

What is notable about the attacks on Paris in January and November 2015 (and Brussels too) was the unrestrained nature of reporting at a moment of national security threat.

In the case of Amedy Coulibaly - who followed on from the Charlie Hebdo attacks – he was called by French newsmedia whilst in the hostage situation and learned that he had more hostages than he had realized. This was potentially very dangerous for those inside the building. He had pledged to blow up the supermarket if the Kouachi brothers were harmed - and he had 21 sticks of commercial dynamite to that end - and so the picture on the left is the moment at the supermarket when the Kouachi's

had been shot dead and just before it was perceived to be reported on the news. The BRI stormed before the news broke.

On the flip-side Coulibaly had not removed mobile phones from the hostages and thus they were also communicating with the outside world, providing important intelligence about the situation inside and where people were positioned in advance of the raid.

2nd – compared to the ongoing conflicts in Syria and Iraq and the daily kill rates there, Europe has – thus far – been relatively spared. The fear generated from these attacks has been immense however. We can see that for limited military output, the political impact created has been very large. We can see one of the core tenets of the European project in Schengen and the free movement of people dismantled and the rise of anti-immigrant parties and groupings. The refugee crisis and attacks have produced social fracture. Regular media have escalated this with reporting that has emphasised risk and replayed the messages the belligerents wanted played. Social media has ensured that like minded people have been able to create epistemic communities.

OPPORTUNITIES THROUGH ORDINARY POLICING



The weaponry for the November 2015 attacks came through organised crime groups, over which the policy may well have had some sight.

The weaponry had made its way from the Balkans to Europe, offering opportunities for further agencies to have curtailed its path.

The attempt to capture Abaooud was achieved not through any electronic surveillance, but through luck. In calling his cousin: Hasna Ait Boulahcen for accommodation she had brought her best friend, who told the police. By chance, Hasna was also having her phone tapped as part of a drugs investigation and so the police were able to connect up where she was, and then were able to follow her to the apartment where the final attack was made.

A SURPRISING ANALOGUE CONCLUSION

- Despite all the digital tools, the ultimate CT policy involves:
 - Strategic level solutions
 - Human intelligence
 - Community relations
- The digital tools are an important second order considerations

