Terrorism Without Borders: ISIL and Cyber-Space

Cyber-space through globalization is getting much more into our lives as days go by. With means of a click of a button, much needed daily chores and necessitates are procured through cyber-space and the internet, as the virtual space and reality are being intertwined more and more; virtual life and reality are being fused to become one. Such also applies to terrorism as well, with the latest example being the Islamic State of Iraq and the Levant (ISIL) group in Syria, Iraq and the Levant region. As ISIL is losing its ground day by day, the key question arises; will ISIL shift to becoming a 'virtual caliphate'?

According to Bruce Hoffman, terrorism in this respect has three motivations and criteria: 1) acts of terrorism which are performed are generally politically (or religiously) motivated in nature 2) They are calculated and not done by 'chance' and 3) Terrorism as an act is performed to kill and send a message for propaganda purposes to the general public. One point should not be forgotten here though, even if terrorism is motivated by religion, the underlying factor for using religious or leftist third-wave doctrine for ideological purposes is politically motivated, which is the idea of 'state-building', such as building a caliphate like ISIL, or a 'Kurdish homeland' like the PKK.

Throughout the four waves of terrorism identified by David Rapoport, no other terrorist organization has used technology and cyber-space as effective as ISIL, even catching Facebook and Twitter off-guard in 2013, with algorithms being in-effective for pointing out and catching terrorism content. On the other hand, the organization is losing land in both Syria and Iraq. Current trends also show that its attacks are being in-effective in Europe as they are less lethal, and the medium used for conducting the attacks are much more simplistic in nature, such as the utilization of a knife, or the renting of a van and using it run-over innocent bystanders. As ISIL is losing land in the Middle East and being less-effective in Europe, will it shift to becoming a virtual caliphate? How will this effect dis-engagement and de-radicalization activities?

What organizations from both left-wing and religion-inspired terrorism have shown is that through cyber-space, state building and the spreading of ideology can continue, even though areas gained by the organizations have been lost back. Current trends show that, even if Raqqa is taken from ISIL ,the organization may shift its activities to the cyber-realm, creating a 'cyber caliphate'. Within this digital realm, ISIL will be able to execute its attacks, keep its hierarchy going, continue its spreading of radical ideology and propaganda, and further on its recruitment. By shifting its activities to the digital medium, ISIL can also perform cyber-attacks as well as continuing its coordination on physical targets and facilities.

If ISIL shifts it's so-called caliphate to the digital realm, this brings about certain questions regarding the organization and changing paradigms in regards to counter-terrorism and rehabilitation: 1) How will ISIL continue its hierarchical structure within the digital realm? 2) What form of communication will the organization have to utilize to not being tracked? 3) How will the processes of radicalization be subject to change within cyber-space? 4) How will terrorism rehabilitation change and what processes could be applied for effective rehabilitation?

By ISIL shifting its caliphate to the digital realm, access to the dark web will allow for firearms, explosives and other necessities to be procured easily. It will also allow for access to blueprints of important structures, and also the procurement of illegal substances such as drugs and narcotics for financial gains. Social media will allow for recruitment as it is currently doing also. Another option to look out for would be ISIL and other terrorist organizations to building their own social media platforms whereby effective communication among members, sympathizers and recruits will be able to come about. The utilization VPN's and programs such as TOR will make tracking harder. Encrypted forums will also allow for hierarchical structures to continue on, with a deliberate chain of command to be present.

The ideology of ISIL as it involves state-building will also be subject to slight change with the virtual caliphate. Rather than concentrating on the 'final war' and 'promised land' phenomena, ISIL and organizations alike will again distort religious doctrine to allow for a gaining of sympathizers. The changing of ideology may include narratives such as 'the final war will be fought on cyber-space', 'we are the only army of god present, and like we built the caliphate, we can do it once more', 'the cyber-space and digital realm allows our caliphate to be global rather than being sandwiched in the Middle East', 'fight your enemy with their weapons' and narratives alike.

With this shift of ideology of ISIL, the key question here arises: What will be the most effective form of counter-terrorism and rehabilitation to fight this virtual caliphate? Governments should be prepared to find ways for rehabilitation within the cyber-realm. Online counseling for militants could be considered firstly. This will allow for rapport to be formed between the counselor/psychologist and the militant, and allow for trust to come about because of anonymity. A second point to consider would be the distortion of ISIL ideology through the interception of ISIL social media accounts, encrypted chat rooms and forums, and also mobile messaging applications such as Telegram. Rather than just banning these platforms, one could use these to their own advantage by intercepting and gaining access these platforms, and providing counter-narratives for potential recruits, sowing suspicion into the minds of sympathizers and having them move away from the ideology of ISIL.

All in all, the idea of ISIL and other organizations shifting their resources to the digital realm is becoming more real, and getting closer as days go by. Governments will have to find ways to both defend their countries within the cyber- realm against these organizations and more importantly find mediums as to how rehabilitation can take place online towards sympathizers and militants of these organizations.