Tackling Global Terrorism in 2018 – ISIS 2.0 and Beyond

Ozer Khalid

*The author is a geo-strategist, a senior management consultant, a development sector director and an international journalist. Twitter follow @ozerkhalid and e-mail ozzerkhalid@gmail.com

†Disclaimer: Opinions expressed herein are a collation of thoroughly researched empirical and expert views, and neither necessary reflect the author’s nor Criterion Quarterly’s editorial stance.

Abstract

(Discerning Criterion Quarterly readers, fasten your seatbelts and brace yourselves for the bellicose advent of what this analyst terms ISIS 2.0 which sees ISIS now evolve into a looser fragmented network of trans-national terror, moving from a physical place to fight in toward an idea to die for. The latter being more sinister, potent and insidious. Fluid and asymmetric in tactical maneuvering, relying on “freelance lone offenders” and a “Cyber Caliphate”, this is ISIS 2.0. – Author)

A Halloween from Hell

On October 31, 2017, as a rented truck ruthlessly rammed into cyclists and pedestrians, leaving at least 8 civilians dead and 12 injured, “Manhattanites” witnessed what seemed to be a haunting Halloween prank only to discover that this was real-life terror unfolding before their unbelieving eyes.

The location of the terrorist attack was symbolic and strategically chosen: a stone’s throw away from the World Trade Center Memorial, giving the “Big Apple’s” resilient residents an eerie spectacle of déjà vu. The perpetrator has been identified as Uzbek immigrant Sayfullo Saipov, who confessed to being ISIS inspired, which is likely to stimulate many more “copy-cat” attacks in 2018 and beyond.

With the precipitous fall of Mosul and Raqqa, ISIS’ territorial cookie crumbles, degrading them from a “proto-state” to an “insurgency” which is all the more Duid, deceptive and asymmetric in maneuverability, making them a more insidious menace to monitor and capture. To compensate for territorial losses in their hinterland of Iraq and Syria, IS will, from afar, keep conducting such “remote-controlled” face-saving atrocities to remain relevant.

Territoriality vanquished, IS, have momentarily reconciled themselves to a “Cyber Caliphate” to digitally incite hatred, drive engagement, bolster recruitment and what this author dub freelance terrorism or home-grown nihilistic “lone wolf attacks”. Welcome to the insidious advent of ISIS 2.0. Such digital tactics are proving horribly useful. Saipov, the Lower Manhattan attack perpetrator, notified the police that he purposely chose Halloween to target maximum civilians. Saipov stated that he was especially touched after watching Abu Bakr al-Baghdadi’s video questioning the American Muslim response to Muslims killed in Iraq. Investigators found other IS streaming and content on his electronic devices. This sick depraved
individual even requested to display the ISIL flag in his hospital room and stated that he “felt good” about what he had done.

The headline-hungry IS death cult will claim any attack they can (even when not their own), as the recent Las Vegas shooting attests. IS, through online propaganda will brain-wash currently returning fighters, who will sneakily camouflage themselves as refugees, sneaking their sinister way into Western nations, laying low till the dust settles, before striking again when the iron sears hot. Tactically speaking, IS now decrees aspiring militants to mount increasing attacks using everyday items like knives, acid and vehicles.

Manhattan’s vehicular assault mirrors the Nice Bastille Day, Barcelona, Berlin Christmas Market and London’s Westminster Bridge attacks, all being ISIS triggered vehicular attacks ordained by IS head-quarters. IS are now hell-bent upon unleashing terror in the West, which they term as Rumiyah, a nauseating reference to the Christian Roman empire of yore, to unleash terror upon infidel “Crusaders”.

Halloween’s Manhattan attack reveals that militarily vanquishing IS in Syria and Iraq does not suffice; the main challenge remains an ideological one, which cannot be curtailed by kinetics but rather by delegitimizing the ideology.

Our reaction to such attacks must be calculatedly discerning and not knee-jerk reactionary. Our world is dangerously teetering on a hotbed of hate speech. Military stealth is at best a momentary stepping stone, and at worst a superficial victory indicator, never a substantive long-term action plan.

Terrorism is like Nosferatu, in that no matter what authorities seemingly do, it just never dies, merely mutates and metastasizes. In the absence of any striking counter ideology, terrorism has become the counter-culture, the zeitgeist du jour, the movement du moment. To make things worse, the world in general, and the U.S. in particular, are more racially, ethnically and religiously polarized than ever before. Charlottesville, Ferguson, San Bernardino and Orlando vividly exemplify this. Racists promptly jump onto the Islamophobia bandwagon claiming that the Manhattan terrorist proclaimed Allah-hu-Akbar (God is Great) before unleashing hell in Manhattan. Every devout Muslim utters “God is Great” during prayers. Prosecute the crime. Never the faith.

The Manhattan attack should not become a predictable scapegoat to parade religious bigotry and exclusionary identity politics which have alarmingly risen. The U.S. is home to 3 million Muslims, and Europe hosts 26 million, these citizens are the essential “eyes and ears” of the community and should not be alienated as it ferments venal extremism.

As IS now evolves from a “physical place” to fight in toward an “ideological idea” to die for. Non-military intellectual capital is needed to counter radicalize because ideas are bullet-proof. Insidious ideas are ultimately only countered by better ones, by nurturing religious tolerance, offering minorities a true feeling of freedom, especially a freedom to practice and peacefully profess their own faith along with a carefully co-ordinated deradicalization program of IS’ returning fighters, especially stateless widows and children, under the auspices of the UN and international donors.

Social inclusion, counter-narratives, positive Muslim role models for an alienated youth to look up to, civil society push-back, education and grassroots momentum are the way forward.

Now, the intellectual challenge against extremism is the real “ideological war after the physical war”. It requires the international community to evolve from solely deploying “hard power” of military might towards exploring the suasion of “soft power”.

By course of necessity, deploying “soft power” in counter radicalization involves sensitization, rehabilitation, education, refugee repatriation and inter-faith bridge-building.

The Advent of ISIS 2.0

An inflammatory civil war in Syria rages to date, destabilizing the entire region with hideous spill-over effects. Radicalization is culturally and conceptually embedded within the veins of an increasingly disenfranchised population in Iraq and Syria.

In 2014 this power vacuum gave incestuous birth to ISIS, which in October 2017, territorially speaking, encounters irreversible demise, especially in their hinterland of Iraq and Syria, losing precious land, momentum, human-power and operational capabilities. Such defeat is a watershed against IS but it scarcely represents the “Waterloo” which coalition forces envisaged.
The forces of time, space and geography coalesce against IS. For now IS’ faux-Caliphate and their looming apocalyptic narrative is physically (yet not conceptually) undermined. ISIS have lost territory conquered, resources captured and fighters recruited which inevitably tames their expansionist zeal. Final nails are being hammered into IS’ territorial coffin with the liberation of Raqqa and Mosul from IS’ tyrannical grip as the images hereunder illustrate.

In addition to the coalition’s aerial assaults, Kurdish forces, SDF ground attacks, a leadership vacuum (when rumors ran rife that al-Baghdadi breathed his last), internal dissent among their ranks and other factors catalyzing IS’s demise. IS’s Faruq Al-Masri, their War Minister, who...
In 2014, when IS evolved from an insurgency to a full-fledged state, it lost many competitive advantages it once enjoyed (which it will devastatingly regain in 2018). As a fixed proto-state, with a Weberian monopoly over the use of force within it’s territories, IS had to shoulder the necessary responsibilities that accompany governance, from conferring ample resources to securing cities and offering essential services. By becoming physically bound to specific locations, IS opened itself up to years of punitive airstrikes. Russian, U.S. and Alliance led coalition bombing assaults, commencing in August 2014, meaningfully degraded IS’ military prowess by destroying a considerable amount of its equipment and troops.

Even in its core territory in Syria and Iraq, IS struggled to conquer areas with Sunni majorities and into Shiite and Kurdish communities. Growth stymied, IS lost Manbij, a crucial smuggling/human trafficking route and a strategic gateway to Turkey. IS was defeated in Mosul, a financial haven. They were vanquished in the prophetically significant town of Dabiq in northern Syria and have now been dealt a definitive blow in their symbolic capital of Raqqa.

Cautious optimism is warranted, for even though ISIS has momentarily been defeated, they are now dangerously dispersed, rendering them tougher to trace, monitor and pin down, IS might be down but they are certainly not out, as this author observed in Criterion Quarterly’s Volume 12, No.3 July-September, 2017 edition 14. The ecosystem of civilization’s enemy (IS) remains.

Discerning Criterion Quarterly readers, fasten your seatbelts and brace yourselves for the bellicose advent of what this analyst terms IS 2.0 which sees IS now evolve into a looser fragmented network of trans-national terror; moving from a physical place to fight into an idea to die for. The latter being more sinister, potent and insidious. Fluid and asymmetric in tactical maneuvering, relying on “freelance lone offenders” and “Cyber Caliphate”, this is IS 2.0. It is a fluid, menacing global guerilla insurrection, forging more extended affiliations and alliances when and where expedient, ISKP or IS Khorasan in Afghanistan becoming bed-fellows with the Taliban, IS tie-up’s with Boko Haram in Nigeria along with deeper penetration into Western Africa such as in Mali, Chad, Burkina Faso and the uranium rich strategically sensitive Niger, Lybia and the Sahel region (which is a hotbed of violent extremism since lawlessness engulfed Libya in 2011). IS 2.0 is also making inroads into the Sinai Peninsula in Egypt, strategically closer to Israel, and has recently reinforced links with Abu Sayyaf in the Philippines (especially in Marawi) where the 100 day battle ensued as 600 IS fighters were held by an iron fisted Duterte (with new Wilayats or Provinces declared by IS).

All the above are but a few examples of how IS are rebranding and regrouping when and where necessary. IS has now evolved from a Weberian state model (or a semi-government entity known as Tamkeen) to a lucid striking force as it’s maneuvering space has widened in an inter-connected porous global world “disorder”.

Conceptually re-adapting Immanuel Wallerstein’s World Systems Theory, IS’ core leadership may have been weakened but their periphery and semi-peripheral/’grass-roots’ world-wide franchises are emboldened.

Rumors are awash that Abu Bakr Al-Baghdadi, IS’ delusional self-appointed Caliph still breathes. Irrespective of whether or not Baghdadi has a pulse, we live in an age of leaderless terror. IS now develops an agile and broadened Weberian span of control and a dehumanizing Kafkaesque bureaucratic apparatus, enabling terror aspirants to climb up the food chain. IS spokesman Al-Adnani’s demise certainly does not end IS. As Al-Qaeda’s example vividly attests, the killing of Bin Laden did not terminate an intellectually poisonous ideology. Fluid trans-national terrorist networks are Hydra-headed serpents, where if one arch tyrant is killed, a hundred more ideologically infested zealots are ready to worm their way up the terror woodworks. The verge of defeat allows IS 2.0 to radically regroup and transform itself with a Duid globalist agenda – exporting hate further afield.

Territorial setbacks have dispersed and discouraged certain IS heathens. Such dispersion implies that authorities will be hunting in the shadows, making their lives infinitely harder. Many disgruntled and now rehabilitated fighters have returned to their original homeland where legal responsibilities that accompany governance, from conferring ample resources to securing cities and offering essential services. By becoming physically bound to specific locations, IS opened itself up to years of punitive airstrikes. Russian, U.S. and Alliance led coalition bombing assaults, commencing in August 2014, meaningfully degraded IS’ military prowess by destroying a considerable amount of its equipment and troops.

In 2014, when IS evolved from an insurgency to a full-fledged state, it lost many competitive advantages it once enjoyed (which it will devastatingly regain in 2018). As a fixed proto-state, with a Weberian monopoly over the use of force within it’s territories, IS had to shoulder the necessary responsibilities that accompany governance, from conferring ample resources to securing cities and offering essential services. By becoming physically bound to specific locations, IS opened itself up to years of punitive airstrikes. Russian, U.S. and Alliance led coalition bombing assaults, commencing in August 2014, meaningfully degraded IS’ military prowess by destroying a considerable amount of its equipment and troops.

Territorial setbacks have dispersed and discouraged certain IS heathens. Such dispersion implies that authorities will be hunting in the shadows, making their lives infinitely harder. Many disgruntled and now rehabilitated fighters have returned to their original homeland where legal responsibilities that accompany governance, from conferring ample resources to securing cities and offering essential services. By becoming physically bound to specific locations, IS opened itself up to years of punitive airstrikes. Russian, U.S. and Alliance led coalition bombing assaults, commencing in August 2014, meaningfully degraded IS’ military prowess by destroying a considerable amount of its equipment and troops.

In 2014, when IS evolved from an insurgency to a full-fledged state, it lost many competitive advantages it once enjoyed (which it will devastatingly regain in 2018). As a fixed proto-state, with a Weberian monopoly over the use of force within it’s territories, IS had to shoulder the necessary responsibilities that accompany governance, from conferring ample resources to securing cities and offering essential services. By becoming physically bound to specific locations, IS opened itself up to years of punitive airstrikes. Russian, U.S. and Alliance led coalition bombing assaults, commencing in August 2014, meaningfully degraded IS’ military prowess by destroying a considerable amount of its equipment and troops.

In 2014, when IS evolved from an insurgency to a full-fledged state, it lost many competitive advantages it once enjoyed (which it will devastatingly regain in 2018). As a fixed proto-state, with a Weberian monopoly over the use of force within it’s territories, IS had to shoulder the necessary responsibilities that accompany governance, from conferring ample resources to securing cities and offering essential services. By becoming physically bound to specific locations, IS opened itself up to years of punitive airstrikes. Russian, U.S. and Alliance led coalition bombing assaults, commencing in August 2014, meaningfully degraded IS’ military prowess by destroying a considerable amount of its equipment and troops.
On the brink of territorial desolation, IS will pursue global attacks to reinvigorate their brand. Sneaking their sinister way into crippled and fractured states, seeking safe sanctuary in Libya, Tunisia, the Sinai, Somalia, the Philippines, to name but a few. They will seek shelter and safe-havens in such fragile and fragmented states. They will also exploit refugee camps and global migration patterns, from Jordan and Turkey to Calais and the Coast of Greece, in an increasingly insular, nationalistic, protectionist world saddled with the worst refugee, IDP and humanitarian crisis since World War II.

The bitter irony is that such an insular world will only breed more civilizational enmity between East and West, nourishing all extremes of an ever-swinging political pendulum.

ISIS 2.0 operatives are likely to birth and disband terror cells more swiftly, form sleeper cells (many sleeper cells in Germany were recently re-awakened which probably explains the recent IS attacks in Germany and perhaps even in Barcelona, Spain) and purposely remain dormant till the opportune attack time arrives.

ISIS 2.0 is likely to metastasize into a full-fledged, geographically dispersed guerrilla insurgency using 5th generational assymetrical warfare tactics, which rely on deception, distraction, chaos, confusion and propaganda. History has proven, time and again, in cases such as the FARC in the cocaine kingdom of Colombia, Zapatistas in Mexico or ETA in Spain, that mobile agile insurgencies battling visible and fiercer foes bear the advantages of relative mobility and agility. Insurgencies, such as ISIS might be splintered and fragmented but can asymmetrically attack at a time and venue of their choice, exploiting the enemies’ unpreparedness, where tactical shock and awe, and an air of ideological invincibility merge in the insurgents’ favor.

The international community is likely to be bedeviled by a return to a 1990’s style globally distributed terror landscape, often being bank-rolled from afar.

Proxy warfare, petro-politics, sectarian-saddled state-sponsored terrorism will all continue unabated, replenishing the coffers of gold-digging opportunity-exploiting defence contractors and corporate warlords in an Eisenhowerian Military Industrial Congressional Complex (MICC). IS, by altering the nomenclature of its major foreign-language magazine from Dabiq to Rumiyah is brazenly shifting its follower’s focus from foretelling a glorious victory in Dabiq (which clearly failed to materialize) to fairy-tale predictions regarding the conquest of Rome. View below the types of articles they post in their English magazine. Rumiyah underscores the urgent need to take the battle to their prophesied crusader infidels in Western cities.

Source:  

A Tale of the Tortoise and the Hare - Differences between IS vs. AQ – A Global House of Terror Divided? – Mujahideen 3.0

Whereas ISIS raced head-long like a hare towards a Caliphate, with rampant death and destruction, Al-Qaeda (AQ) (by and large) took a tortoise-like calculated, step by step, gradualist incremental approach. IS believes in break-neck "revolution;" AQ prefer gradualist "evolution". IS` top brass were only appeased by a Global Caliphate; AQ are more pragmatically satiated with a relatively quieter proto-Emirate – in Idlib for instance.

IS out rightly reject the Westphalian super-structure, for instance their Wilāyat al-Furāṭ breached the Sykes-Picot borders straddling Syria and Iraq, while AQ is deeply embedded in the political structures of Yemen and Syria, deceptively masking themselves as the "soft face" of appeasement. AQ have made overtures (much like the Taleban and Hamas) to politically negotiate and compromise with, and accommodate (in varying degrees) Western interlocutors within a democratic election-based Westphalian state paradigm.

Note how AQ keep rebranding themselves, this is a textbook asymmetric deception technique to confuse opponents and form previously unthinkable alliances. For instance, AQ’s al-Nusra became Jabhat Fateh al-Sham and are now convenient bed-fellows with the Western alliance against IS.

Where IS focused on total “disruption,” AQ emphasize on “creation” (cunning coalition-building, consensus mobilization with local party structures) embedding themselves within the political apparatus.
IS and AQ operate on a totally different time-horizon in terms of attack and action planning. AQ’s time-horizon stretches 5-10 years, whereas IS executed a knee-jerk immediate short-game. AQ’s devious longer-game is a more sneaky, silent, sinister gradualist plan, now keen to exploit the IS territorial vacuum in the Middle East.

AQ, harvesting the poison that Zawahiri and Zarqawi have sewn, have taken a longer-term politically-strewn “strategic” approach (as seen in AQ’s Agenda 2020), whereas, IS will now unleash more low-intensity “tactical” level hit-and-run terror. AQ and its ever-multiplying regional off-shoots are deeply exploiting and embedded in the Syrian civil war and insurgency.

AQ is more selective and discerning vis-à-vis who it recruits amongst its ranks (for instance the 9/11 perpetrators were highly qualified in engineering and aviation), whereas, IS is much less selective with its intake, which is probably why IS are a much more “infiltrated” organization, inside-out and from top to bottom.

IS uses slick social media campaigns to lure adherents into their lion’s lair. They have a more engaged and robust online presence as opposed to the more traditional older-generation AQ. An example of a sick but slick IS campaign can be viewed here which urges an immediate call-to-action:

Source: Haya Alal (2016) Al Arabiya English, Jihad: A Call to Action,

AQ would use older social media networking sites such as the now dinosaur-like MySpace whereas IS swiftly moves into Next-Generation-Networks (NGN) and social media platforms.

AQ’s Zawahiri was never deemed a charismatic leader. He was, at best, an ineffective manager and the internal dissent between Zarqawi and Zawahiri caused many to defect from AQ and gave IS immediate manpower, territorial traction and land-grab from 2014 onwards. Whereas AQ is characterized as older militants, IS is manned and managed by younger zealots, so a generational gap is also at play. AQ recruits were geographically more locally concentrated whilst IS lured in an unprecedented number of foreign militants, and will now focus more on instigating far-flung home-grown nihilism and terror, especially in the West, conflict-laden zones and regions bedeviled by fragile corruptible states.

IS losses work to AQ’s advantage. Both groups will keep trying to out-do each other in the global theater of militant extremism. Many former IS foot-soldiers, with no army to fight for, will be embraced (albeit suspiciously) with open arms by a re-invigorated AQ unleashing what I label a Mujahideen 3.0.

Whilst IS’s priority is now to wage a Crusade against Rumiyah, a term for ancient Rome of yore (exporting terror to Western capitals in other words), AQ’s focus is firmly (for now) rooted in the Middle East, Northern Africa where AQ Islamic Maghreb is active in Algeria and in South Asia, where AQIS and Taleban have a training complex in Kandahar, which the US took out in a Counter Terrorism (CT hereafter) raid.

The Syrian civil war break-down, an inability to agree on chemical Assad’s exit, the flammable tinderbox that is the “petro-state” of Kurdistan that will destabilize four neighboring states coupled with an internally disunited Iraq offers AQ ample marche de manoeuvre. AQ will endeavour to recapture territory. AQAP is already capitalizing upon anti-Houthi sentiments in Yemen, whose people, much like the persecuted Muslim Rohingyas, are seen as Children of a Lesser God in a cruel and harsh world.

Whereas IS and AQ are at ideological loggerheads, staunch dichotomies between IS and AQ should not prematurely be cast in stone, since both have already been forming (momentarily at least) joint alliances together in Yemen and Bangladesh of late, and certain attacks like the 2015 Charlie Hebdos in Paris reportedly involved both terror networks simultaneously. Shifting oaths of allegiance and marriages of convenience amongst militants are likely to be the norm in 2018, followed by the usual vicious cycle of splintering and mushrooming into more visceral factions.

As compared to IS, AQ now cunningly rebrands and name-changes into various reborn guises, reinvigorating a plethora of unsavoury new Jamaats and Ansar who will keep competing for resources and enjoy more buy-in from militants in conflict zones.

As per this analyst, the split between IS ad AQ might also lead to what I term as a ”Third Paradigm” of terror where smaller militias (as witnessed in Libya’s Sirte or Misrata) will find sectarian donors, including proxies and the usual state sponsors and engage in small-scale Emirate (rather than State) building. Such militias, unable to replicate IS’s Riyaasat-Wilayat formula, will remain content with running their “mini-Emirates”. When North Africa offers multiple prison amnesties to Tunisian, Libyan, Egyptian and Algerian radicals, expect them to architect such “mini-Emirates” and militia
factions to destabilize their more secular rulers. With IS territorially cornered, AQ will certainly utilize the opportunity to springboard back up to the terror limelight, albeit in more subtler ways, working internally from "within the system". However, AQ will not remain static but keep planning attacks abroad. On April 17, AQ claimed responsibility for the St. Petersburg metro bombing.

Although the schism between AQ and IS remains palpable, it is naïve to assume the two entities will not (at least temporarily) co-operate where and when it serves their vested interests. One pressing ideological menace ISIS poses is that, whereas, al-Qaeda believes that a Caliphate can only transpire after Uncle Sam and it’s European allies have been so scrupulously overwhelmed that they are impotent to impede upon Muslim majority lands, ISIS, by contrast, instigates a more urgent and pressing timeline for such a sinister agenda – with an undying conviction that the time for seizing, acquiring and conquering virtual cyber-territory (if no longer physical land) and brain-washing minds is now or never.

The Future of Terrorism – Cyber Caliphates and Digital Terror in 2018 and Beyond

As our world has evolved from "pens and papers" to "bits and bytes", a bone-chilling Godless ISIS death cult and many future emerging terrorist cells have reconciled themselves to the reality of hosting a Cyber Caliphate spreading digital terror. They will use the information superhighway and social media to bypass mainstream media (which has already lost precious currency and credibility) and amplify their narrative. Online terror pushes our world from "Networks" to "Netwars".

As the daunting infographic hereunder illustrates, empirical evidence suggests that there are massive audiences, the world over, susceptible to cyber-terrorist propaganda, below are the countries where they are most concentrated:

![The Biggest Global Audiences For Jihadist Web Content](image)


The above graph shockingly places the USA at number two with the UK and Germany trailing not far behind in terms of global audience demand for the consumption of extremist material. This might help explain the increasing number of attacks in these three countries in 2017.

IS' growing presence in the USA is most alarming as the graph hereunder from September, 2017 depicts. Statistics from George Washington University (below) indicate that the FBI finds that 28 states and the District of Columbia are infested with IS related charges. 136 individuals have been charged since 2014 and the average age of perpetrators is 28. The huge demographic bulge in this particular age bracket is all the more worrisome. The numbers below merit cause for concern and might be suggestive that more Lower Manhattan type attacks maybe imminent.
IS are currently controlling a vast Digital Caliphate. IS social media propaganda spin masters cannot be stopped, in an age of ubiquitous social media. Where the deep dark world wide web, non-traceable proxy servers, and cloud computing render information more susceptible to hacking from virtual private networks.

For every physical act of terror there is now a virtual counterpart, which compensates for territorial loss, and offers groups like IS an artificially exaggerated perception of strength, credibility and durability. This hyper-accelerates the radicalization process and stimulates potent calls-to-action.

As the physical barriers to Hijra close, the virtual doors to waging online so-called Jihad from afar open, where currently IS (and future mutations) emphasize the need to mount an increasing number of home-based localized terror operations, especially with knives and rental trucks (the Ohio state university attack started with a vehicle and ended with a knife).

IS has a sprawling digital media enterprise. IS’s media assets range from e-zines (online magazines like Dabiq and Rumiyah) to online news agencies issuing digital press releases, such as Amaq, al-Hayat, al-Furqan and Khilafah News and the weekly al-Nabah, to name but a few. IS have radio channels and frequencies in multiple languages dotted all around the globe.

Cyber terrorists utilize online psychological warfare and emotional manipulation techniques to bolster recruitment, galvanize support and sway fence-sitters to their deadly cause. For example, IS used their social media platform Amaq to show videos of U.S. and Russian aerial strikes to emotionally seed doubts in the minds of reticent prospective recruits. Amaq then proliferates these videos onto ‘stand-alone’ websites which are more concealed and take longer to censor, enabling their audience more access. The video for Muhammad Riyad, Germany’s Wurzberg attacker, is a similar case in point.

Under a Digital Caliphate ISIS operatives and hackers in addition to VPN’s and proxies which offer instant anonymity, are also likely to use keystroke recognition devices and algorithms to boost their search rankings. They may use anonymous browsers (such as TOR which masks online presence) cookies (which track the prey’s online activity), browser plug-ins (especially for Firefox which was conjured up by the hacking community), and other such “entrapment” information to uniquely identify a politically sensitive end-user.

IS uses existing apps such as Twitter’s Dawn app and justpaste.it to keep operatives updated and use applications like Hallumy, often to translate content from Arabic to multiple languages.

IS leveraged digital platforms to notify and warn audiences of their upcoming activities. For instance, images of IS’ Turkey invasion appeared online just days before the ghastly Istanbul Reina attack.

They upload flashy infographics (to exaggerate their on-the-ground successes), videos, electronic-flyers often as a call to martyrdom operations. As the image hereunder exhibits, IS use social media to expand far across all borders, passing violated images through Instagram to entice violent-prone lone offenders to mirror the same. They especially influence teenagers via Facebook and Whatsapp.
My forecast is that IS will now increasingly start using ephemeral social media such as Periscope and Snapchat, the latter widely used in the Arabian peninsula.

Such online activities are especially potent as terrorists manipulate electronic platforms to inculcate an “identity de-marginalization” in their potential recruits, through powerful peer pressure, crowd psychology and virtual group participation. Terrorists draw conflicted identities, especially those of lost souls, into spheres of evil by offering them a sense of inclusion and belonging not offered in their real physical world.

Social media can be extremely socially menacing. IS “de-individualize” humans, break them down into pieces, get fence-sitting prospective militants to copiously self-disclose facts about themselves (to be used later on for emotional blackmail or online abuse) coaxing them to carry out terror without their volition. This is using cyber influencing to play on our most viscerally primal impulses and drivers as humans.

IS digitally migrated from in-house “proprietary” software to “off-the-shelf” easily accessible faster-paced software. Whereas AQ would write their own sophisticated code, IS utilizes easily accessible off-the-shelf software, and migrates from classic websites to encrypted social media networks such as Telegram (a micro-blogging channel and instant messaging service), as well as Surespot, Kik, Wicker and Twitter. Users who post and proliferate their content are often contacted to resurrect the now Digital Caliphate.

Twitter and Telegram are by far IS’s preferred social media platforms because it is easier to open accounts on these channels and they tend to be more politicized than other platforms. IS, would, on average, amass at least 14,000 online followers daily, via various anonymous accounts. Even though Twitter (and other social media platforms) have belt-tightened, shutting down 250,000 online accounts, yet a lot still needs to be done. AQ’s As-Sahab account only had 20,000 Twitter followers by contrast.

IS uses its online media empire to train combatants on how to use weapons, where and when to strike, ideal targets to aim at. These are practically virtual online training and indoctrination sessions:
In such a hauntingly Huxley-like Brave New World Order, lonely online misfits are seduced by the dystopian “parallel universe” ISIS sucks them into. Such growing “lone offenders” are likely to operate and seek inspiration from multiple online platforms, deploying low to medium scale intensity attacks within the Internet of “Stings.”

Slightly more sophisticated cyber terrorists will graduate to: installing malware, ransomware (holding end user’s sites hostage till handsome ransom money is paid), firewall leaks, online identity theft (phishing, blended threats (a cocktail of viruses), privacy breaches, a Denial of Service (DDos) attack by overwhelming servers and distributing electronic kill lists.

IS often use cyber media to post gruesome execution pictures. A recent example of this was when ISIS supporters promised to bring mayhem to the 2018 Russian Soccer World Cup and have uploaded a series of stomach-turning posters depicting a sick execution of the prodigious Neymar and Lionel Messi. Through web defacement IS leaves unsavoury images, lists and messages to trigger “lone-offenders” into deadly action.

Consistently pushing out their vile propaganda on popular channels broadens their consumer base, reach and distribution networks. Such a stream of constant engagement renders credibility and augments their virtual support base to a generation unhealthily glued to their smart-phone screens and addictively glued to social media.

To elevate their online visibility and drive interest IS deploys hash tagging (easily searchable words, especially on Twitter, by Tweeting certain keywords preceded by a hash tag, like ISIS Daesh Caliphate Khalifah al-Furqan and al-Hyat or common hashtags such as #KhilafaEn #alFurqan #alhayat which in turn eerily climb to the top of multi-platforms and Google search rankings. As these hash tags trend right on top, they are consumed by impressionable minds who go on to further research these concepts, which in marketing is known as a “pull” technique to increase conversion ratio. These hash tags are often linked to posts related to a bellicose call-to-action (for instance to increasingly use knives and vehicles to attack innocent civilians) or belligerent crusades, and those who retweet such messages fall under IS social media army’s potential recruitment radar, as being sympathetic to their cause.

Worryingly the circle of IS online sympathizers might be much larger than analysts envisage – claimed to currently be 23,000 in the UK alone. When terror sympathizers and social misfits on the fringes of society, recycle, retweet or upload content onto their social media time-lines and walls the “Like” button by their virtual friends gives them instant gratification, status and validation in our dystopian post-industrial information age, where “ghettoized online communities” are increasingly living their lives more on social media and less in the physical realm.

Such clichuit “ghettoized online communities”, especially amongst hate and terror groups, often form “echo chambers” where the group reinforces received messages – focusing on perpetuating a victimhood narrative, prevailing global injustice, the failure of globalization, a binary “us versus them or us versus the world” mentality, foreign policy grievances – necessary for legitimizing terror. Such self-reinforcing “echo chambers” trigger self-validation which is the fuel needed to animate radicals to attack, often soft civilian targets.

Such “echo chambers” are often (inadvertently) designed by social media platforms themselves, where your online behavior and preferences are tracked and your timeline gets full of messages or hashtags you and your circle of influence have posted. Such predictive behavior analytics, Artificial Intelligence and manipulated content reinforce existing world-views and narratives, no matter how deviant or despicable.

IS often organizes, for its online adherents, patterns of activity with which to pledge their allegiance as a sign of initiation or a rite of passage. This precipitates “lone wolf” attacks. IS also deploys armies of cowardly keyboard warriors to keep cyber bullying threatening, trolling and irritating reporters and counter terrorist analysts who vehemently oppose them and officials who institute harsher policies against them. Cyber terrorists of the future will even be able to “tease out” future trends and policy insights from social media character profiles.

For cyber terrorists, there is likely to be a precipitous rise in cyber crime to fund their low-scale attacks. Such scams currently include online bank
account infiltration for quick funds transfer, e-black-mailing and threats.

IS 2.0 and their forthcoming offshoots, with an enhanced media product, high-resolution graphics and technical quality, professional production capabilities would/will often broadcast their terror in real-time, glorifying gory violence to seduce the adventure prone (often video-game obsessed) adrenaline-fueled youth male demographic, in an almost surreal manner.

Such bloodthirsty (video-game like violent) were uploaded to sites like YouTube[^84] for optimal viewership and linked to keywords even in the video gaming community, to widen their recruitment net with a *many-to-many* as well as *peer-to-peer* (P2P) recruitment modality paradigm. IS would fine tune, narrow-cast and market segment their messages based on age, gender, demography and disposable income. From the younger to older online communities.

One lurid emotional example of this is by having handsome soldiers romantically seduce aspiring so-called *Jihadi Janes*[^85] on Skype and WhatsApp, showering them with attention, praise and lavish gifts (physically delivered to them from afar), promising them a *Halal* relationship of intimacy through marriage if they came and joined them in Iraq or Syria’s Caliphate[^86].

*Cyber-brainwashing* of impressionable minds on the social periphery is now IS’ perceived historical calling; an inevitability in the battle of ideas; a digital reality on the insidious information superhighway.

**Future Emerging Cyber Threats**

Future terrorists are prone to engage in *Cyberspace Cyberwarfare* where the virtual battle space targets entire Industrial Control Systems (ICS), electricity grids[^92] (already hacked by spies back in 2009), mass transit and transportation systems, and entire utility networks (water, gas, power) on which our modern lives depend upon. As the image below cautions:

![Image: New Security Threats for Europe](https://example.com/image.png)


Future cyber terrorists will have their eyes set on end-to-end encryption networks. Entire Smart Cities (including Islamabad[^88]) and Smart Systems...
could be compromised. For safety purposes, many former (now rehabilitated) terror czars advise that industrially sensitive systems should be disconnected from the internet altogether – be they transport hubs, energy and electricity infrastructure, thermal or nuclear installations. Wi-Fi, SCADA and ICS systems are all inter-connected which can be piggy-backed and infiltrated in our day and age. Any mass transit system such as trains (the terrible train accident in Bad Aibling Germany 2016 caused due to a single moment of distraction from a computer game), buses, and driverless cars are all prone to hacking which can cause huge fatalities. We now live in a world where a USD $ 50 off-the-shelf Radio Frequency device can hack an entire car, control its engine and imperil all seated passengers.

The aviation industry is particularly sensitive to cyber susceptibilities, where Wi-Fi networks and cellular links have already been ethically hacked by white hackers. This exhibits huge system potential weaknesses. Ethical hackers have already infiltrated second tier systems, such as communication systems, take off and landing strip application and control systems.

In 2012, Newark International Airport came to a grinding standstill by a USD $ 50 GPS signal jammer which disrupted the entire airport and even Port Authority’s communication systems. On June 21, 2015 OT airline had a cyber breach. On July 8, 2015 United Airlines had to cancel 4900 flights, due to a single cyber glitch and in 2015 United Airlines gave a US $ 1 million bounty to ethical hackers who successfully infiltrated their systems. Delta Airlines had one single power outage which triggered a computer glitch grounding thousands of flights, disrupting its systems worldwide.

Cyber terrorists hacking into peripheral second tier systems or grids can cause such power outages, wreaking havoc on carrier’s reservations systems. The Delta Airlines meltdown testifies to ageing equipment and (back then) a potential lack of alertness. On July 20th South West Airlines had to cancel 2300 flights due to a router problem, whereby the airline suffered the worst system outage in it’s history along with a failure of all backup systems. This not only accentuates the need for cyber contingency planning and safer redundant N + 1 network configurations but also exposes the dark reality that a tech savvy hacker who can disrupt networking systems and routers can make life a living hell for commercial aviation and any other industry they so chose.

British Airways has encountered massive IT failures. American Airlines faced cyber glitches due to which Miami and Denver airports had to temporarily close down.

Chronicking such vulnerabilities seek not to stoke hysteric alarmism but rather to underscore the urgency that there are multiple digital vulnerability points which terrorists can prey upon. The Holy Grail of Cyber Security is beyond our comprehension. We are only coming to terms with it. This is not pie in the sky, nor drawing daggers in the dark but concrete real-life empirical industry-based examples which can all too easily be exploited by tech savvy terrorist or criminal mavericks.

The International Civil Aviation Organisation (ICAO) kick-started a program titled ‘No Country Left Behind’ (NCLB) which is a positive start provided member states follow-up. Of particular relevance are ICAO’s SARP’s documents 17, 187 and 394 which address cyber vulnerabilities. The US Federal Aviation Authority is rapidly seeking to comply with ICAO’s NCLB initiative. Other transport and infrastructure industries need to intensify and hasten the pace of their cyber risk preparedness and disaster recovery based contingency planning.

Advanced simulation and preparedness exercises are rapidly required to future-proof and secure-proof a brave new world based on advanced automation and analytics. One interesting example is The U.S. Department of Justice which started researching into possible cyber threats to driverless cars, as external devices can easily hack the engine and purposely cause atrocious road accidents.

Current and future cyber-warfare entail both offensive and defensive tactics, espionage and high-scale sabotage. Nations must develop virtual warfare readiness capabilities. The advent of anti-western anti-civilization terror groups imply that such eye-watering cyber terror attacks are likely to intensify sooner rather than later.

Future cyber shockwaves as described above might serve to very painfully illustrate how woefully unprepared governments are for such digital assaults, even though most governments are already tacitly engaged in Cyber Warfare themselves. Cyber terrorism, by leveraging encryption apps along with potential alliances on the deep dark web with criminal syndicates may see new spheres of virtual evil emerge. The deep dark web is much tougher to monitor than the above examples which can all too easily be exploited by tech savvy terrorist or criminal mavericks.

Cyber terrorism, by leveraging encryption apps along with potential alliances on the deep dark web with criminal syndicates may see new spheres of virtual evil emerge. The deep dark web is much tougher to monitor than the above examples which can all too easily be exploited by tech savvy terrorist or criminal mavericks.

ISIS 2.0 and other cyber MNT’s (Multi-National Terrorists) are likely to intensify a so-called “Electronic Jihad” of incitement. To fund such campaigns collaborative cyber fund-raising modalities will develop (terrorists already use mobile payments, digital wallets leveraging high tele-density in developing countries, to crypto-currencies like Bitcoin and crowd-sourcing/crowd-funding terror campaigns). These finances will be used for terror recruitment, to spread Dawa (a skewed and distorted interpretation of the religion). Even though Bitcoin issued new money laundering guidelines the risk of funding cyber warfare via crypto currencies remains real and imminent.

On an institutional level, a delicate, finely-tuned sensible balance has to be sought. One concrete recommendation which this author recommends that the U.S. Federal Communications Comission (FCC), Pakistan’s PTA, PEMRA and other similar global media and telecom watchdogs ensure and verify that only social media accounts be allowed to open or access their social media accounts via VPN’s or specialized browsers, or at the very least, levy a monthly fee for so doing, whereby online payments would act both as a deterrent plus leave a digital trail of footprints enabling Counter Terrorism (CT) authorities to swiftly locate and triangulate the user’s physical location.

On a social level, online users of the world must unite to form electronic counter extremist advocacy campaign groups. A lot is at stake. By not doing so we have a lot to lose. By uniting we have everything to gain. The civilized world must counter terrorism’s next generation electronic psychological warfare. Recent online activism sprung from noteworthy campaigns such as #MeToo and #BlackLivesMatter illustrate that positive messaging on social networking sites yield positive awareness, outreach, sensitization, attitudinal and behavioral change, essential ammunition to delegitimize the nefarious propaganda of militancy and hate.

Both offline but now especially online, the international community needs to roll out more podcasts, video logs, live streams, outreach programs and debates centered around cyber counter narrative programs, peer-to-peer and many-to-many counter messaging counter-extremism initiatives and deployment of counter terror hashtag activism (#CVE or Countering Violent Extremism is one stellar example). Global engagement initiatives are afoot but need to be less fragmented and more concerted.
With fear and loathing spreading like wildfire on our online world, and the weaponization of social networks, social media behemoths need to more actively engage in content moderation and control. Suspending 250,000 ISIS linked Twitter accounts is a start, a stepping stone, but a lot more is required to take substantive moves forward. Terrorists have weaponized social networks, therefore social media and telecom operators would be well advised to rapidly suspend a “cluster” of accounts which publish inflammatory hashtags such as the ones cited earlier in this paper. This can be achieved via Behavioral Mapping and Advanced Analytics. Suspicious Activity Reporting (SAR’s) which have made steady milestones in the financial sector need to broaden their reach into other industries especially in the technology, social media, telecom (TMT) and other sensitive sectors (defence, nuclear, critical infrastructure).

Thwarting cyber-terrorism requires a concerted multi-stakeholder effort and engagement. The international community must prevent terrorism but preserve innovation. This is a judicious balancing act at the easiest of times. An urgent response with special Anti-Cyber Terror task force and monitoring units (like Pakistan’s FIA Cyber Security division), harsher Security Hash Algorhythm (SHA) encryption protocols, deeper probing and penetration testing constitute steps in the right direction.

Admittedly, CEO’s of publically listed and traded tech companies of course worry about their PR and reputation, especially seeking never going to trial, neither with terrorism’s family victims and affectees nor with liberal free speech activists, as it dents their equity value and stock price. Such social media and online companies and their Senior Management remain stuck between a rock and a hard place. If they are seen as too lenient they are labeled as terror sympathizers, if they crack-down hard they are seen as Orwellian Big Brothers watching over an over-surveyed citizenry whose 1st amendment and freedom of speech rights are being curtailed.

States need more trained Certified Electronic Ethical Hackers (CEH). Better network defence and cyber security capabilities and architectures are needed which deny current and future terrorists “cyber sanctuaries” who can wreak catastrophic scale atrocities. A maximization of cyber combat readiness and resilience is long overdue, including in the private sector.

As the future unfurls, in an age where Artificial Intelligence, Big Data, Advanced Analytics, Quantum and Cloud computing redefine how marketplaces operate, more industries will be dependent upon and vulnerable to mission-critical digital infrastructure running entire industries. Countering cyber terrorism must be a top-priority and strategy for all serious stakeholders and innovators in an increasingly compromised hyper-connected, cyber risk-prone virtual world of terror.

Legality Governing Cyber Terrorism: New Battlefields Old Laws?

In an increasingly compromised cyber risk-prone virtual world, let us now impartially review measures which the international community has initiated to legally counter this palpable menace. The international community has stepped up its efforts to regulate and police (to the best of their abilities) the world wide web and cyber space, a de facto ungovernable space (due to its increasingly open source cross-border nature). Under the auspices of Article 51 of the UN Charter, countries have the right to self-defence, this definition now encouragingly broadened its remit to encompass protection from cyber attacks also.

The Budapest Convention on Cyber-Crime, the Talinn Manual on cyber self-defence and cyber warfare, NATO’s Cyber Defence Pledge of July 2016, Article 3 of the Washington Treaty are just some major multi-lateral legal milestones governing cyber-space, cyber warfare and cyber security. UNDOC and UNCITRAL deal with cyber issues and the United Nations Group of Government Experts (UN GGE), comprising of twenty five nations, advanced a series of recommendations for countries to protect themselves from cyber threats. The International Multilateral Partnership Against Cyber Threats (IMPACT) is the first United Nations-lead cybersecurity alliance. It is the first comprehensive Public-Private Partnership (PPP) against cyber threats. It remains a politically neutral global platform bringing together world governments, academia and industry to boost our global community’s cyber threat capabilities. IMPACT’s Global Response Centre acts as the first line of defence against cyber threats.

The OECD’s 35 member states achieved commendable work on digital security risk management, especially on issues pertaining to critical infrastructure (grids, power stations, transport hubs). In 2016, the OSCE’s 57 member states issued confidence building measures related to cyber resilience, especially with regards to interception and escalation mitigation.

International forums currently tackling cyber security include the Billington Cybersecurity Summit, the Internet Governance Forum which has undertaken laudable efforts towards incident response management and cyber security teams and the Global Counter-Terrorism Forum (GCTF).

Despite all the above, however, Silicone Valley, ICT tech companies and social media behemoths need to be more integrated and involved. Admiringly, Microsoft proposed international legal norms that could govern cyber-security which was quite a break-through from the private sector but their norms need to be followed up. The above measures, (with further refinements and necessary amendments) can act as a future industry blueprint.

Critical facilities (especially in sensitive industries such as nuclear and thermal) pose a larger threat and are currently not fully cyber protected. A comprehensive cross-border Threat Vulnerability Assessment needs to take place and prosecution norms need to be better defined. Laggard companies failing to comply with these emerging precautionary measures should at first be fined and subsequently perhaps black listed for non-compliance. Global supply chains are vertically and horizontally interdependent and inter-related, where digital system dependencies are higher than ever before, whereby a single glitch in one virtual application, or a cyber security breach of any kind, is likely to have monumentally negative ramifications for entire industries. This paper shed light to some concerning examples from the aviation industry. This alone should jolt industries and governments into action.

A major problem with most of the aforementioned legal instruments is that they are, voluntary non-binding limiting norms rather than mandatory legally binding decrees. The Conventions, guidelines and legislation highlighted above are broad recommendations and general principles as opposed to legally enforceable instruments of potency. More substantive and specific measures are needed as our world vulnerably teeter’s on a knife edge of cyber uncertainty, where criminals, terrorists and miscreants may/are forging Unholy Alliances to undermine the cyber world order.

Nation-states can no longer afford to be negligent and have to rapidly undertake compliance of the above as legally enforceable and immediately
Selected Bibliography


Mückenberger, Christiane (1993), "Nosferatu", in Dahlke, Günther; Karl, Günter, Deutsche Spielfilme von den Anfängen bis 1933 (in German), Berlin: Henschel Verlag, pp. 69-72.


Aymenn Jawad al-Tamimi (2016) "Dissent in the Islamic State's Yemen Affiliates: Documents, Translation & Analysis," Combating Terrorism Center (CTC)


Weber, Max (1904) Die protestantische Ethik und der Geist des Kapitalismus translated in English as The Protestant Ethic and the Spirit of Capitalism


Philip Sherwell (2011) »Osama bin Laden killed: Behind the scenes of the deadly raid». The Daily Telegraph. London.


C. Christine Fair (2011) "The bin Laden aftermath: The U.S. shouldn't hold Pakistan's military against Pakistan's civilians". Foreign Policy. May 4, 2011.


Revkin, Mara, "The Legal Foundations of the Islamic State," The Brookings Project on U.S. Relations with the Islamic World, July 2016, 16;


Bothelo, Greg (2014) "ISIS Executes British Aid Worker David Haines; Cameron Vows Justice." CNN.


Ough, Tom; Smith, Hannah Lucinda (2015) "From Loving Rihanna to Loving Jihad – Mohammad Uddin tells how daughter Sharmeena Begum became the first British schoolgirl to join ISIS in Syria". The Times. 14, March, 2015

Bennhold, Katrin (2015) "They were the girls you wanted to be like: How teenage rebellion sends girls into the arms of ISIL". National Post, 18 August, 2015.
Early reports indicate that Saipov was “self-radicalized”. John Miller, of the New York Police Department, said that Saipov unleashed terror on lower Manhattan following ISIS’ social media counsel on how to carry out vehicular attacks.

Fayol further expounded on the span of control proposing that subordinates should be allowed to communicate directly with each other, which may stretch. As IS 2.0 will rely on repetitive simpler terror assaults including everyday items like knives and rented vehicles, the span of control may


10. The 2017 Battle of Raqqa was the fifth and final phase of the Raqqa campaign spearheaded by the U.S. bank-rolled Syrian Democratic Forces (SDF) against IS, reinforced by airstrikes and SDF ground troops, titled the “Great Battle” taking place concurrently with the Battle of Mosul, as part of the CJTF–OIR to dismantle its structure strip IS of its regional centers of power and territory. For more: Damien Gayle (14 October 2017). “Last Isis fighters in Raqqa broker deal to leave Syrian city – local official”. The Guardian and “Raqa’s Al Naim roundabout liberated, 37 ISIS members surrender”. Hawar News Agency. 16 October (2017).


12. Al-Masri was IS’s Minister of War and presented strategic advice on the Majlis al-Shura (consultation council) of IS. This work, titled ‘Message on the Manhaj’ (‘Manhaj refers to direction/vision), which was disapproved by senior rank and file, his books were censored. Al-Masri vanished, and was most likely arrested by IS’s heavy-handed security apparatus. Al-Masri’s role in birthing a council that played a part in organizing the Hisba (Islamic morality enforcement) and Zakat (Alms giving) bureaucracies was not viewed very favorably. For more on dissent within IS’ upper echelons review: Aymenn Jawad al-Tamimi (2016) “Dissent in the Islamic State’s Yemen Affiliates: Documents, Translation & Analysis,” Combating Terrorism Center (CTC) and also Aymenn Jawad al-Tamimi (2016) “Dissent in the Islamic State: Abu Al-Faruq Al-Masri’s Message on the Manhaj: Documents, Translation & Analysis,” Combating Terrorism Center (CTC) 2016.

Nahda, World

18. In Greek mythology the Hydra, was a nine-headed serpent. It was believed that if you cut off one head, two more grow back and the monster shouldered an immortal head in the middle. The second of the 12 labors of Hercules was to kill the Hydra. All the heads could spew deadly acid. To defeat the Hydra, Hercules sought assistance from Iolaus. When Hercules cut off one head, Iolaus sealed it with a red hot poker so that nothing could grow to replace it. Having removed Hydra's immortal head, keeping the serpent's poisonous blood. Afterwards he dipped his arrows in the blood so that they would instantly kill whomever they struck. Knowledge thirsty mythologists should read Graves, Robert (1960) The Greek Myths, Penguin Books, pp. 70-470 and "Hydra." Myths and Legends of the World (2001) Encyclopedia.

19. Analyzing 200 documents such as intimate letters, expense reports and membership rosters captured from ISIS, external donations constituted only 5% of IS's operating budgets. Cells were mandated to cough up to 20% of the income generated from kidnapping, extortion rackets and illicit activities to their upper echelons. Top-rank and file then redistributed this to local IS cells required to initiate terror attacks. By 2015 Iraqi intelligence confirmed that IS was worth US $2 billion, making them the richest so-called Islamic terrorist group world-wide. Out of this sum, roughly US $429 million was looted from Mosul's central bank including copious amounts of gold bullion. See: Moore, Jack (11 June 2014). "Mosul Seized: Jihadis Loot $429m from City's Central Bank to Make Isis World's Richest Terror Force". International Business Times. UK. Post 2012, to lure donors, IS produced annual corporate-like financial reports.

20. IS also accrued wealth via taxes and extortion. Christians and foreigners, if not slaughtered or thrown off buildings, were liable to pay a jiiza tax levied thanks to its fighters in battle. One-fifth of the ghanima, or the spoils of war (khuma) were being replenished back into their coffers. Property acquired peacefully, termed fay, was subject to a 20% tax. IS levied an 'ushr tariff on imports and exports from their territory. IS routinely practiced extortion, by demanding money from truck drivers and threatened to blow up businesses. Bank robberies were commonplace. Most tragically, Iraqi government indirectly financed IS, by carrying on paying wages to thousands of government employees who labored under IS controlled territories, only to be confiscated by ISIS. Workers who had labored for "religiously inappropriate" entities paid for a repentance ID card, annually renewed. IS announced a new currency, the Islamic Dinar and a gold dinar, though the US dollar is the de facto currency utilized in its territories. Kulish, Matthew Rosenberg, Nicholas; Myers, Steven Lee (29 November 2015). "Predatory Islamic State Wrings Money From Those It Rules". The New York Times. Revkin, Mara, "The Legal Foundations of the Islamic State," The Brookings Project on U.S. Relations with the Islamic World, July 2016, 16; Gordon, Matthew S. The Rise of Islam. Indianapolis: Hackett Publishing Company, 2005 and Peritz, Aki (4 February 2015). "How Iraq Subsidizes Islamic State". The New York Times.

21. Bothelo, Greg (2014) "ISIS Executes British Aid Worker David Haines; Cameron Vows Justice." CNN.


23. ibid

24. As per the Congressional Research Service (CRS), experts estimate that IS paid roughly between $400 and $600 to each fighter monthly, before their resources dried up leading to an inevitable pay cut. That's significantly higher than the minimum wage dish out to public sector employees in Syria at the beginning of the uprising in 2011—between $176 and $266—which terrorist experts opine was an essential recruitment magnet for ISIS. Nicks, Denver (2016) ISIS Fighters just got a huge pay cut, Time Magazine, January 19, 2016.

25. One such example is Sharmeen Begum, a fifteen year old British schoolgirl of Bengali descent from Bethnal Green Academy who left the UK to join IS in 2014. In February 2015, her school friends Amira Abase, Shamima Begum and Kadiza Sultana joined her in Syria proving the potency of 'pulling power' when it comes to poisonous propaganda, especially amongst a younger demographic. Ough, Tom; Smith, Hannah Lucinda (2015) "From Loving Rihanna to Loving Jihad – Mohammad Uddin tells how daughter Sharmeena Begum became the first British schoolgirl to join ISIS in Syria". The Times. 14, March, 2015, and Bennhold, Katrin (2015) "They were the girls you wanted to be like": How teenage rebellion sends girls into the arms of ISIL". National Post. 18 August, 2015.


27. Tunisians make up the largest contingent of foreign IS fighters, especially disgruntled with their moderate Islamic democratic government of Al-Nahda, which in this analyst’s view is a beacon of hope for Islam with enlightened moderation. In 2017, IS related terrorist activities have been rising in Tunisia. Discovering the body of the shepherd Khelifa Soltani on Mount Mghila and a mine explosion at Jebel Mghila (Sidi Bouzid), during a sweep on CNN on the 4th of February, 2016.


31. Tin, Alex (2016) "ISIS faction raises black flag over Somali port town". Telecast on com CBS News.

32. Spain, with the heated controversy over the Catalan referendum, is in the throes of uncertainty.


34. The MICC " is an informal and changing coalition of groups with vested psychological, moral, and material interests in the continuous
development and maintenance of high levels of weaponry, in preservation of colonial markets and in military-strategic conceptions of internal affairs. This is a "war-based" industrial complex. Douglas Brinkley asserted that the US has a «military–industrial–scientific complex». Henry Giroux reasons that the U.S. is a «military–industrial–academic complex». In 1956, the eminent sociologist C. Wright Mills in his epic oeuvre *The Power Elite* writes that a cadre of military, business, and politicians, stimulated by mutual interests, were the true leaders of the state, and beyond the remit of democratic norms. Friedrich Hayek in his seminal 1944 *The Road to Serfdom* cites the perils of supporting any monopolistic organizations. Also consult: Wright Mills C (1963) *Power, Politics and People*, (New York) 1963, pp.1-173.


39. Ofcourse gruesome AQ attacks have taken place in the West as well, for instance 9/11 and Charlie Hebdo with the Kouachi brothers claiming to have links to AQ.


43. Lands often termed as *Dar-ul-Islam*, or the House of Islam.


45. Where cyber miscreants undertake anonymous web browsing by disguising, in a most shadowy ever-changing manner, their Internet Protocol (IP) addresses with devices such as Tor. VPN’s and proxy servers work by sending information via multiple switches and routers to conceal the source and destination of information. However, there is never a cast-iron guarantee of anonymity as such servers fall prey to traffic analysis used for advanced algorithms by search engines and data collection by online law enforcement authorities, who are trying, their level best, not always to much avail, to crack down on such activity. Moreover, cookies, browser plugins, and other information can be used to uniquely identify a user even if they have hidden their IP address. Eckersley, Peter 15 October (2014) “How Unique Is Your Web Browser?” (PDF). *Electronics Frontier Foundation*. Springer.

46. A VPN extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.


48. For the perverted IS the word Hijra detonates a migration to take up arms with them in Syria and Iraq.


50. Al Hayat Media Centre 2014. There’s no life without Jihad. YouTube, (June 19) Available at: https://www.youtube.com/watch?v=sFltVWWBUYE


65. A malware could turn networked devices into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. Devices infected by malware often scan the internet for the IP address of Internet of things (IoT) devices with a table of IP Address ranges. Malware attacks
66. With Ransomware IS could conduct a worldwide cyberattack (for example as was done during the WannaCry attack), install ransomware cryptoworms, which target desktops running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.
67. A blended threat is a software exploit which in turn involves a mixture of attacks against diverse threat vulnerabilities. This could include worms, a Trojan horse and a computer virus exploiting multiple techniques to attack and propagate.
71. In order to hash-tag an online user simply adds a # (i.e. a hashtag symbol) before any given word.
73. Well known ISIS media dissemination outlets.
74. An interesting portrayal of how IS deployed hashtag activism can be found at Channel 4 News (2014) IS supporters demand police #FreeShamiWitness after arrest.
78. Especially true for 'likes' gained on Facebook. Fiegerman, S. (2014) Facebook Messenger now has 500 million monthly active users.
88. Islamabad’s Smart City project involved installing city-wide high definition CC and IPTV surveillance systems for traffic but also terror monitoring.
89. ICS is an acronym for Industrial Control Systems. ICS components cover various embedded systems, including smart home components, solar panels, wind turbines, SmartGrid and much more.
90. Such as those being proto-typed by Uber, Elon Musk’s Tesla and Alphabet (the parent company of Google).
94. An N + 1 configuration implies that back up IP network links are secured within the system, usually by deploying a totally separate Tier 1 broadband provider.
95. The No Country Left Behind (NCLB) campaign underscores the ICAO's efforts to assist States in implementing ICAO Standards and Recommended Practices (SARPs) to assure implementation is better coordinated globally so that all States have access to the significant socio-economic benefits of safe and reliable air transport.
96. The NCLB effort particularly promotes ICAO’s initiatives to resolve Significant Safety Concerns (SSCs) brought to light through ICAO’s safety oversight audits as well as other safety, security and emissions-related objectives.
101. Physical location concealing proxies and TOR immediately spring to mind.


112. The Talinn Manual signed in Estonia, *inter alia*, issues critical guidelines on cyber attacks, rules prohibiting the threat or use of force, the scope of self-defence against on-going or imminent cyber attacks, but it also deals with the question of attribution, the use of force by and against non-state actors along with the topic of non-intervention. Section 2 of Article 6 allows a Party to the Protocol at their discretion only to prosecute if the offense is committed with the intent to incite hatred, discrimination or violence; or to make use of a reservation.

113. The Organisation for Economic Co-operation and Development (OECD) Recommendations of the Council concerning guidelines governing the protection of privacy and trans-border flows of personal data was promulgated in 1980 and in 2002 were the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (25 July 2002). These guidelines informed entities how to develop, own, provide, manage, service, and use information systems and networks. The OECD Guidelines underscore the fundamental principles underpinning risk management and information security practices. While no part of the text is binding as such, non-compliance with any of the principles is indicative of a serious breach of good practices that can potentially incur liability.

114. Cyber risks can be mapped and measured via an ATVI model which is: \[
\text{Risk} = p(\text{Asset, Threat}) \times d(\text{Asset, Threat}) \]

\[
A = \text{measuring and mapping the value of the assets, } T = \text{the likelihood of the threat occurring, } V = \text{the nature of vulnerability i.e. the likelihood that can be exploited (proportional to the potential benefit for the attacker and inversely proportional to the cost of exploitation) and } I = \text{the likely impact, the extent of the harm could cause, financial and otherwise.}
\]

115. Which can be accessed at [www.gctf.org](http://www.gctf.org)