CYBER VIGILANTISM, TERRORISM AND GUERRILLA WARFARE: NEW CHALLENGES, NEW PERSPECTIVES

ASHISH GUPTA

Many individuals and groups are responding to the opportunities and challenges that cyber space brings in ways that are significantly different and hardly in consonance with the earlier observed and reported events. The proliferation of the internet and the advent of the new cyber space technologies have introduced a new security paradigm, with challenges that are far more intractable and pervasive than ever before. For an understanding and appreciation of the new threats, and for capacity enhancement to thwart them, there is a need to focus on assets, strengths and capabilities build-up.

In recent times, the whole tenor and tone of the cyber security policy deliberations reflect the continuing attention and commitment of governments and military and law enforcement agencies to protect and defend cyber space against threats emerging from the evolving cyber technologies and operations. The inalienable significance of cyber space at multiple levels of individual and social functioning has heightened the quotient of vulnerability due to increased criminal and anti-national activities in cyber space. Such activities—ingenious in planning, inventive in execution and effective in accomplishment of objectives—have changed the global landscape for crime and anti-national activities. Utilising Twining's Cheshire Cat metaphor, the emerging challenge in cyber space resembles the Cheshire Cat in *Alice in*

Group Captain **Ashish Gupta** is a Senior Fellow at the Centre for Air Power Studies, New Delhi.

Cyber space provides a conduit and mechanism for propagation of propaganda, convoluted ideological and extremist rhetoric and a platform for planning and executing cyber enabled criminal acts.

Wonderland, who keeps appearing, fading away, and disappearing, so that sometimes one may see the whole body, sometimes only a head, sometimes just a vague outline, and sometimes nothing at all.[1] Buttressed by the cyber infrastructure, globalisation is changing the very nature and consequences of unlawful activities. Cyber space provides a conduit and mechanism for propagation of propaganda, convoluted ideological and extremist rhetoric and a platform for planning and executing cyber enabled criminal acts.

The terms *vigilantism, terrorism and guerrilla warfare*, as understood within mainstream conceptions of security and as used in the current social-political debate, have contextually different connotations in the cyber related lexicon. Over the last few years, acts classified by the media as online vigilantism have begun to attract public attention.[2] Vigilantes are those who take enforcement of the law or moral code into their own hands.[3] Acts of vigilantism often grab the headlines and capture the imagination of ordinary folk. Vigilantes are either revered or reviled but undeniably form part of the popular folklore. With the advent of social media, vigilante justice is also being meted out over cyber space. Similarly, the architects and perpetrators of terror—in order to retain/ propagate the potency of terrorist acts—rely heavily on cyber space to pervade the collective consciousness and to infest societies with terror and hatred. Terrorism thrives on publicity and cyber space facilitates terrorists to vicariously expose the global community to the pain and suffering of the victims and their families. Similarly, a new form of *cyber guerrilla warfare* has emerged in which states are often pitted against groups, capable of waging relentless asymmetric war, unlimited in scope and duration. While 'guerrilla warfare' is a specific way of waging asymmetrical war in a specific situation

1. William Twining, *Rethinking Evidence: Exploratory Essays* (Illinois: Northwestern University Press, 1994), p. 197.
2. Smallridge, Wagner and Crowl, "Understanding Cyber-Vigilantism: A Conceptual Framework", *Journal of Theoretical & Philosophical Criminology*, vol. 8(1), January/February 2016, pp. 57-70
3. Vincent N. Parrillo, *Encyclopaedia of Social Problems* (California: Sage Publications, 2008), p. 998.

against a conventional army, cyber guerrilla warfare is more universal[4] and has been used, not only as a manifestation of political dissent, social unrest or conventional conflict but also as a form of voicing dissent against regressive and retrograde policies.

Cyber guerrilla warfare is more universal and has been used, not only as a manifestation of political dissent, social unrest or conventional conflict but also as a form of voicing dissent against regressive and retrograde policies.

CYBER VIGILANTISM

The word vigilante is of Spanish origin, meaning 'watchman' or 'guard'. It has its roots in Latin: "vigil" means "awake," "watchful," or "observant." The term has been loosely used to describe a variety of forms and degrees of violence, in various spatial and temporal settings, perpetrated by individuals or groups. There is no consensual definition of what constitutes vigilantism. Various authors have used different concepts and dimensions to define vigilantism. In one of his seminal works, Johnston argues that vigilantism has six necessary features.[5]

- First, it involves planning and premeditation by those engaging in it;
- Second, its participants are private citizens whose engagement is voluntary;
- Third, it is a form of "autonomous citizenship" and, as such, constitutes a social movement;[6]
- Fourth, it uses or threatens the use of force;
- Fifth, it arises when an established order is under threat from transgression, potential transgression, or imputed transgression of institutionalised norms;
- Sixth, it aims to control crime or other social infractions by offering assurances or guarantees of security both to the participants and to others.[7]

4. Jelle van Haaster, Rickey Gevers and Martijn Sprengers, *Cyber Guerilla* (Massachusetts: Elsevier Inc., 2016), p. 2.
5. L Johnston, "What Is Vigilantism?", *British Journal of Criminology*, vol. 36, issue 2, Spring 1996, pp. 220-236.
6. Ibid.
7. Ibid.

Like a myriad meanings and innuendos associated with the word "vigilantism", the term cyber vigilantism has been loosely associated with a wide range of acts. Some of the activities—including, but not limited to hacktivism, cyber stings, scam baiting, cyber crowdsourcing—are defined as acts of cyber vigilantism. One way to clarify the ambiguity in defining acts of cyber vigilantism would be to fall back on Johnston's conceptualisation of traditional vigilantism. The act must be perpetrated as a premeditated one by private citizens voluntarily participating in it, without any support or authority granted to them by the state. The act must be in response to a perceived crime or social deviance, with an implicit or explicit threat of the use of force. Lastly, the central objective of the act must be to assure, or guarantee, security, both to the participants and to others.[8]

However, there are many cases that could be construed as fit for inclusion under the broader definition of 'cyber vigilantism' though they fail to comply with Johnston's definition of vigilantism. This variance is not due to the contextual differences between 'traditional vigilantism' and 'cyber-vigilantism' but is largely attributable to the disparate and idiosyncratic nature of cyber space. With a little tweaking, Johnston's definition will become more contemporary and will help in delineating other forms of cyber deviance from cyber vigilantism. By keeping the focus firmly on the first three requirements of Johnston's definition of traditional vigilantism—i.e. planning and premeditation by perpetrators; engagement on voluntary basis by private citizens; part of a social movement (whether genuine or pseudo)—a broader framework can be formulated for defining activities as cyber vigilantism. The remaining three criteria are not necessary for an activity to qualify as an act of cyber vigilantism. Most of the cyber attacks perpetrated through computer technologies and networks do not have a streak of violence, but sometimes, threats of violence, if not real violence have also been encountered.

8. Smallridge, et.al., n. 2, pp. 57-70.

SCAM BAITING

The advent of the internet is closely linked with the emergence of a new breed of scammers, keeping a look out in cyber space for unsuspecting victims, luring them into financial traps and fleecing them monetarily. The most well known among these is the Nigerian '419' scam. The community of scammers in many variants of this scam was initially operating from Nigeria and as an act of mocking defiance, took its name from the Nigerian criminal code, Article 419.[9] The unsuspecting targets were promised large monetary rewards in return of a small sum of money as fee or for circumvention of some fabricated problem. If a target responded in an accommodative manner, the con artists kept extorting money from him on one pretext or another..

In one of the first instances of cyber vigilantism, as a counter-measure to 419 and similar scams, an online community of cyber vigilantes '419Eater. com' came into being. Established in September 2003, it advocated a form of cyber vigilantism termed as 'scam baiting' in which "the vigilante poses as a potential victim to the scammer in order to waste his time and resources, gather information that will be of use to the authorities, and publicly expose the scammer". Under the guise of a fake identity, a scam baiter responds to a scam mail and while enthusiastically feigning excitement, tries to divert the resources, and waste the time, of the scammer for as long as possible. The scam baiter also tries to lure the scammer into revealing some personal information which later could be handed over to the law enforcement agencies. In a sense, it is a case of deceit pitted against deceit.

HACKTIVISM

This neologism was coined by combing two terms, 'hackers' and 'activism' by members of the hacking group Cult of the Dead Cow (cDc). As per Oxblood Ruffin, a member of cDc, hacktivism "uses technology to improve human rights. It also employs non-violent

9. "Offences Relating to Property and Contracts," http://www.nigeria-law.org/Criminal%20 Code%20Act-Part%20VI%20%20to%20the%20end.htm. Accessed on July 20, 2017.

Since 'hacktivism' perpetrators can remain anonymous or disguised, their chances of getting caught or being meted retributive punishment or oppressive retaliation are reduced considerably.

tactics and is aligned with the original intent of the internet, which is to keep things up and running."[10] Hacktivism was fundamentally a non-violent conception which has now mutated into many forms of protest; some righteous, some innocuous, some dubious and some even harmful. Over the internet, the hacktivists employ two types of methods: Mass Virtual Direct Action (MVDA) in which many people simultaneously use the internet to launch a kind of digital disobedience movement; and Individual Virtual Direct Action (IVDA), which can manifest in the many forms such as defacements, Denial of Service (DoS) or network penetrations.[11]

The political and social activism paradigm gained traction in cyber space because of three primary reasons. Firstly, the internet provides protestors a platform to propagate their ideological precepts among the populace almost instantaneously. Secondly, since governments or institutions have a recognisable and legitimate presence over the internet, the acts of acktivism against these garner the same effects as physical or street protests. Thirdly, since 'hacktivism' perpetrators can remain anonymous or disguised, their chances of getting caught or being meted retributive punishment or oppressive retaliation are reduced considerably.

In the late 1980s, hacking was no longer an activity for just amusement or monetary profitability but had become a threat of noticeable proportions. During the same period, the hacktivist subculture also emerged. Examples of early hacktivism included "Worms Against Nuclear Killers (WANK)," a computer worm unleashed by anti-nuclear Australian activists into the

10. L. Allnitt, "Old-school Hacker Oxblood Ruffin Discusses Anonymous, and the Future of Hacktivism", http://www.rferl.org/content/hacker_oxblood_ruffin_discusses_anonymous_and_the_fuure_of_hacktivism/24228166.html. Accessed on July 20, 2017.
11. Tim Jordan and Paul A. Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (London: Routledge, 2004), p. 69.

networks of the National Aeronautics and Space Administration (NASA) to protest against the launch of a shuttle which carried radioactive plutonium.[12] The repository of the hacktivists' arsenal grew with the addition of DoS attacks. The so-called "Intervasion of the UK" took place in 1994 in the form of electronic civil disobedience when the UK's Criminal Justice Bill sought to outlaw outdoor dance festivals and "music with a repetitive beat". In protest, a group called 'The Zippies' from San Francisco's 181 Club brought down the government websites for at least a week by Distributed Denial of Service (DDoS) attacks. [13]

The term hacktivism became popular in the mainstream media during the 1998-99 Kosovo conflict, when websites of countries participating in the aerial bombardment of Yugoslavia under the umbrella of the North Atlantic Treaty Organisation (NATO) came under DoS attacks.

On December 21, 1995, a one-hour "Netstrike", organised by Italian activists, targeted the websites of French government institutions in protest against the nation's nuclear policies. The participants were asked to direct their browsers at government sites and keep clicking, thereby orchestrating a DDoS attack. The Netstrike per se, was not an act of cyber space vandalism, but a new form of virtual civil disobedience.[14] The term hacktivism became popular in the mainstream media during the 1998-99 Kosovo conflict, when websites of countries participating in the aerial bombardment of Yugoslavia under the umbrella of the North Atlantic Treaty Organisation (NATO) came under DoS attacks.[15] The American-based group Team Spl0it, the Russian Hackers Union and the Serb Black Hand Group (Crna Ruka) attacked, defaced and hijacked websites as a form of protests against the war as well as against countries engaged in it.[16] In the aftermath of the accidental bombing by the US of the Chinese Embassy, the hacktivists

12. Peter W. Singer and Allan Friedman, *Cybersecurity: What Everyone Needs to Know* (New York: Oxford University Press, 2014), p. 77.
13. A. Kiyuna and L Conyers, *Cyberwarfare Sourcebook* (North Carolina: Lulu Press, 2015), p. 193.
14. Barney Warf, *Global Geographies of the Internet* (New York: Springer, 2013), p. 156.
15. Kenneth Geers, *Strategic Cyber Security* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2011), p. 14.
16. Ibid.

from China also got involved in defacing US websites and launching DoS attacks. [17]

CYBER ANTAGONISM BETWEEN INDIA AND PAKISTAN

The belligerence between India and Pakistan continues unabated and has become a determinant of strategic posturing by both nations. In spite of the fact that both nations possess a formidable arsenal of nuclear weapons, the mutual hostility between the two shows no signs of waning. The prevailing atmosphere of hatred and trust deficit between these South Asian neighbours has metastasised in cyber space and has even sucked the common citizens from both sides into the vortex of distrust. This spiralling antagonism, primarily in the wake of state-sponsored terrorism by Pakistan, has given rise to a breed of netizens from both countries, competing with each other in cyber space in a contest of one upmanship to express their anger, frustration and antagonism.

In one of the major cyber attacks, the Indian website owned by the Bhabha Atomic Research Centre (BARC) came under attack by a group called 'milw0rm'. The website of BARC was breached and defaced and it was also reported that megabytes of e-mails and data were stolen by the attackers. The attack was allegedly perpetuated in response to the testing of nuclear weapons by India on May 11 and 13, 1998, as claimed through a message put up on the defaced site.[18]

At first, it was believed that these attacks were the work of the Inter-Services Intelligence (ISI) of Pakistan, but later investigations revealed that it was the handiwork of a group of teenagers who were operating under pseudonyms and had different nationalities.[19] The insidious nature of the Pakistani intent unfolded in the year 1999, when it was revealed that at least four attacks on Indian cyber networks were carried out from Pakistan. In the following years, the numbers and severity of the attacks increased. Some

17. Laura Lambert et. al., *Internet: A Historical Encyclopedia, Volume 2* (Santa Barbara: ABC CLIO, 2005), p. 156.
18. http://ces.iisc.ernet.in/hpg/envis/doc98html/miscbarc69.html. Accessed on July 14, 2017.
19. William C. Boni and Gerald L. Kovacich, *I-way Robbery* (UK: Butterworth-Heinemann, 1999), p. 142.

Indians responded in a similar manner and unleashed a series of cyber attacks against Pakistan rivalling or surpassing in severity the ones originating from Pakistan.

In the meantime, many new hacking groups, with varying capabilities and motivations, forayed into cyber space. Of these, one group, the Z Company Hackers Crew (ZHC) gained tremendous notoriety and media attention when it claimed to had attacked 1,846 Indian websites, both government and civilian.[20] Other hacking groups like Pakistani Hackers Club (PHC) and the G-Force also attacked Indian websites. On the Indian side, many hacking groups emerged, of which, 'H2O' or the 'Hindustan Hackers Organisation' become popular among the cyber hacking community. Another group called 'TEAM NUTS' claimed to have achieved a record feat by hacking and defacing 57 commercial sites in Pakistan in one day in 2010.[21]

These hacking groups from both countries become more ingenious and methodical and tried to target each other in ways that had a greater symbolic as well as coercive dimension to the cyber attacks. In one such case, on the second anniversary of the 26/11 Mumbai terror attacks i.e. on November 26, 2010, members of the Indian Cyber Army (ICA) launched an all-out attack on 87,012 Pakistani websites, of which 34 were crucial government websites belonging to the Pakistan Navy, Maritime Security Agency, Foreign Ministry, the chief minister of Sindh, etc.[22] The ICA, on the website called Hacker Regiment claimed that the main objective of these cyber attacks was to pay homage to the martyrs of 26/11.

On December 3, 2010, the most powerful group called Pakistan Cyber Army, on the pretext of recalling the 39th anniversary of the 1971 Indo-Pak War, attacked 270 Indian websites. Of all the attacked sites, the worst affected was the website of the Central Bureau of Investigation (CBI) which could only be restored with great difficulty, after remaining offline for almost one

20. http://www.hackread.com/read/hackread/3289. Accessed on July 14, 2017.
21. http://thehackernews.com/2010/12/57-pakistani-websites-hacked-by-team.html. Accessed on July 14, 2017.
22. Sandeep Unnithan," Inside the Indo Pak Cyber Wars", *India Today*, March 18, 2011.

month.[23] The retaliatory cyber attacks were swift and the ICA defaced the website of the Oil and Natural Gas Regulatory Agency (ONGA) of Pakistan in response to hacking of the CBI's website.[24]

It is evident that many Indian and Pakistani agencies/ organisations/ individuals are being caught in the crossfire of these cyber skirmishes between the hacking communities of both countries. Hacker groups from both the countries keep coming up with new and imaginative names and driven by misplaced patriotic fanaticism, target their victims with fervour. On the Indian side, the websites of the National Green Tribunal, Parbhani District Police and Bihar State Electronics Development Commission were attacked and vandalised. Similarly, multiple Pakistani government websites and the Pakistan Army website were hacked. Concerns are being raised that any escalation of tension in cyber space can spill over and exacerbate already heightened tensions between the two South Asian neighbours.

CYBER CROWD SOURCING

Cyber vigilantism has many forms and variations, some of which closely resemble acts of vigilante justice committed in the physical world, while some have taken a form different in intent, methodology, and results. 'Cyber Crowdsourcing', a neologism is believed to have been coined in China, and is known as *renrou sousou* in the Chinese vernacular, literally meaning "Human Flesh Search" (HFS).[25] In response to real or perceived social injustices/ wrongs, the netizens congregate and use the internet for meting out punitive justice by posting personal details of the perpetrators—ranging from the phone number and address to the blood type—online for administering punitive retribution. It also involves tracking down the activities of a perpetrator and putting the information on the internet so that it might lead to his/her arrest or detention. There are two types of groups

23. Alamzeb Khan, "Pakistan Cyber Warfare and Internet Hacking", January 17, 2012, http://www.simple-talk.com/opinion/opinion-pieces/pakistan-cyber-warfare-andinternet-hacking/. Accessed on July 14, 2017.
24 Ibid.
25. Anastacia Kurylo and Tatyana Dumova, *Social Networking: Redefining Communication in the Digital Age* (Maryland**:** Rowman & Littlefield, 2016), p. 156.

which practise this form of cyber vigilantism – the first group comprises relatively organised individuals who react to activities falling in the category of perceived societal injustice, while the second group crops up in response to a particular social wrong for a short period of time.

The netizens who participate in online cyber crowd sourcing perceive that the formal justice system is inadequately resourced, ineffectively manned and lacks the capacity to deliver justice commensurate with the perceived heinousness of the crime. They consider themselves to be informal guardians of society, meting out justice to deviants—who are too powerful, too clever, and know the ins-and-outs of circumventing the judicial system. They use the internet and social networking platforms for enforcing social justice against wrongdoers who either circumvent the law or commit infringements that are not punishable by law.

In one such case, a vigilante group, 'Perverted Justice' joined forces with Chris Hansen, the host of NBC's popular network television series "To Catch A Predator" to identify child sex offenders and paedophiles, by luring them to a prearranged place for a meeting between them and potential victims. Then, with Chris Hansen and the news crew from NBC, the offender was confronted with a series of questions, presented with the details of the sexual chat log with the decoy and after his admitting to be the perpetrator of the chat log, the offender was informed that he was being filmed for national TV. Subsequently, the predator was arrested by the police and sent for trial. 'Perverted Justice' claims to have facilitated 623 convictions of predators since June 2004 due to its website Perverted-Justice.com.[26] The website contains details of full transcripts of online conversations between the predator and the decoy, including the photo of the predator. Groups like 'Perverted Justice' that track criminals online, cannot be categorised as 'cyber vigilantes' in the strict sense of the term, as these groups not only have a legitimised existence but also the support and resources of law enforcement agencies. Such groups are driven by the mission to rid society of the "scourge of child predators", who seek out vulnerable and unsuspecting victims through the internet.

26. "Perverted Justice", http://www.perverted-justice.com/. Accessed on July 14, 2017.

Terrorism thrives on publicity and cyber space facilitates terrorists to penetrate the collective consciousness and vicariously expose the global community to the pain and suffering of the victims and their families.

In addition to such well-organised groups, there are groups that crop up temporarily in response to some specific instance of perceived wrong or injustice. After the initial furore over some perceived social injustice, end with waning impact of their cause, these groups eventually dissipate into oblivion. Some groups feel that the scourge of corruption and misconduct by public officials and citizens is taking a toll on the general population. To mete out justice of some kind for the acts deemed ethically/ culturally offensive but not illegal, a group of netizens carry out online surveillance to identify the perpetrators. Cyber crowd sourcing or HFS is deemed by them to be an online instrument for identifying and meting out their version of social justice. The netizens use HFS to mobilise public opinion in instances where the legitimacy of a particular incident is questionable or where inaction on the part of law enforcement agencies is palpable.

CYBER TERRORISM

The scourge of terrorism continues unabated, exacting a heavy toll in terms of human lives, suffering, depletion of resources and imbalance in the demographic structure. Terrorism, in various forms and manifestations, has been practised throughout history and across a wide variety of political ideologies.[27] There is no single accepted definition of terrorism and a multitude of meanings may be inferred in different contextual settings by different people. Similarly, the fluctuating ideological profiles and organisational structures as well as changing means and methods of most of terrorist organisations have led to the circumvention of efforts by many to categorise terrorism in one genre. Most definitions of terrorism hinge on three factors: the method (violence), the target (civilians or the government),

27. Harvey Kushner, *Encyclopaedia of Terrorism* (California: Sage Publications, 2003), p. xxiii.

and the purpose (to instil fear and force political or social change).[28] The efforts of many sovereign states to annihilate the scourge of terrorism and its dangerous consequences are proving to be a chimera. Transnational terrorism is like a hydra that will keep growing new heads if any of the heads is severed or decapitated.[29]

The loosely connected network of individuals, subgroups and groups of a modern terrorist organisation finds the internet both ideal and vital for inter- and intra-group networking. The internet enabled facilities and functions such as email, chat-rooms, e-groups, forums, virtual message boards, YouTube, and Google Earth have added to the terror potency of such organisations.

Terrorism thrives on publicity and cyber space facilitates terrorists to penetrate the collective consciousness and vicariously expose the global community to the pain and suffering of the victims and their families. Besides, by propagating their convoluted ideological discourses with pseudo-religious fervour, the terrorist organisations partially succeed in bringing potential fence-sitters, sympathisers and ideologically aligned individuals into their fold.[30] Cyber space is used by terrorists as a key medium not only for coercion, enticement, indoctrination, proselytisation and propaganda but also for planning attacks after garnering information from cyber space about the potential target's location, security arrangements, and post attack impacts. Cyber terrorism is the convergence of terrorism and cyber space, perpetrated for the attainment of potential objectives such as damaging critical information infrastructure, disrupting vital networks, stealing trade secrets, provoking societal disharmony, and radicalising groups along sectarianism and religious fault lines.

The information revolution has allowed many organisations to dispense with the hierarchical structure and centralised control, and provide much

28. Ibid.
29. Wolfgang Sachs et al., *Fair Future: Limited Resources and Global Justice* (New York: Zed Books, 2005), p.231.
30. Ashish Gupta, *Cyber War: Conquest over Elusive Enemy* (New Delhi: KW Publishers, 2017), p. 241.

larger greater functional autonomy and operational flexibility to dispersed groups. In any organisation, moving away from the hierarchical to the network paradigm brings in resilience, flexibility and adaptability, and ensures its survivability by removing the single point of failure. Similarly, in the present times, we are witnessing a new form of terrorism which has many functional similarities with a network form of organisation. In the case of terrorist organisations, the network may be made up of loosely linked autonomous entities varying from individuals to small groups of individuals of sleeper cells to groups of armed militants to groups of radicalised youth, etc. These groups use various means of communication facilitated through cyber space. The loosely connected network of individuals, subgroups and groups of a modern terrorist organisation finds the internet both ideal and vital for inter- and intra-group networking.[31] The internet enabled facilities and functions such as email, chat-rooms, e-groups, forums, virtual message boards, YouTube, and Google Earth have added to the terror potency of such organisations.

In a report published by Europol, it was claimed once again that the internet has become the principal means of communication for terrorist and violent extremist individuals and groups.[32] The online presence of such groups is frighteningly disturbing and horrifyingly substantial and provides these groups means and platforms for the facilitation of activities contributing to, or enabling, terror. The internet is used for a range of purposes, including instruction, propaganda, recruitment, dispatch of members to conflict areas, fund-raising, cooperation with other terrorist organisations, and planning and coordination of attacks.[33] Presently, and in the foreseeable future, tackling cyber terrorism is a challenge of enormous magnitude. The use of cyber technology for committing, aiding, abetting and facilitating terrorism, and for coercing, enticing, indoctrinating, proselytising or radicalising others to commit primary or secondary terrorist acts can be described as 'cyber

31. Gabriel Weimann, *Terrorism in Cyberspace* (New York: Columbia University Press, 2015), p. 14.
32. Europol "EU Terrorism Situation and Trend Report", https://www.europol.europa.eu/newsroom/news/eu-terrorism-situation-and-trend-report-te-sat-2012. Accessed on July 20, 2017.
33. Ibid.

terrorism'. Cyber terrorism has emerged as an attractive and cost effective option for terrorists offering significant benefits from a logistical, operational and consequential standpoint and a wider media appeal perspective.

Terrorists have relied on high profile violent acts, committed to bring into sharp focus their ideology, cause and narrative, as well as to showcase their capabilities and intent as terror outfits. In addition, contemporary terrorist groups leverage the internet for exerting psychological pressure over a global audience, heightening the fear psychosis and communal polarisation. While analysing the dimensions and dynamics of international terrorism, Brain Jerkins observed, "Terrorist attacks are often carefully choreographed to attract the attention of the electronic media and the international press. Terrorism is aimed at the people watching, not at the actual victims. Terrorism is a theatre."[34] While undertaking a terrorist attack, terrorists aim for a theatrical spectacle and use the body counts as a measure of success. Besides, their main focus remains on the emotional and psychological impacts rather than on the material impacts. The spectacle of carnage and violence is played out over and over again in the news and social media, watched by a global audience. For the terrorist, as Schmid and de Graaf have pointed out, the "immediate victim is merely instrumental, the skin of a drum beaten to achieve a calculated impact on a wider audience. As such, an act of terrorism is in reality an act of communication. For the terrorist, the message matters not the victim".[35]

Publicity is a means of sustenance and survival of terrorism and the internet provides the necessary scaffolding to publicise, plan and orchestrate terrorist activities and attacks. The emergence of "mass-mediated" terrorism is largely attributable to the exploitation of global networks and information highways by terrorists to propagate their mistaken and misplaced ideology as well as to expose the masses to the spectacle of violence as vividly as possible.

34. B Jenkins, "International Terrorism:A New Mode of Conflict", https://www.ncjrs.gov/App/ Publications/ abstract.aspx? ID=30518. Accessed on July 20, 2017.

35 Brigitte Nacos, *Mass-Mediated Terrorism:The Central Role of the Media in Terrorism and Counterterrorism* (Plymouth: Rowman & Littlefield, 2007), p. 14.

THE IS APOCALYPSE: BOLSTERED BY CYBER SPACE

Digital technology is responsible in more than one way for setting in motion the juggernaut of terror and violence by the Islamic State (IS). Political *faux pas*, the misinterpretation of historical events, misreading of cultural sensibilities and a sense of collective victimisation, all have facilitated a 'limited Islamist insurgency' transforming into one of the most dreaded terrorist organisations, the Islamic State (IS). By using technology in many ingenious ways, the IS has been able to capitalise on the alienation and existential concerns of a large population and become the most brutal extremist *jihadi* terrorist organisation the world has ever seen.

IS—a scourge that overran large swathes of northern and western Iraq and eastern and northern Syria, and killed and displaced millions of civilians—tries to retain its terror potency by permeating the public consciousness with fear and infesting societies with hatred. The transformative power of the internet and social networking platforms has been woven into the terrorist enterprise of the IS almost from its inception. In the wake of the IS offensive in June 2014, a number of Twitter accounts came up claiming to represent the IS in Syria and Iraq. During the initial days of the offensive, the various Twitter accounts were giving live updates and images of the IS' advances in Syria and northern Iraq. The IS' digital footprint on social media kept pace with its advances in Syria and Iraq. The images of captured Iraqi security personnel went viral, garnering an even wider online audience. In an attempt to fan religious jingoism, information, including on the number of bombings, suicide missions and assassinations that the IS had carried out, was shared on the growing number of Twitter accounts, with large followings. In an attempt to expand its digital reach on social media, the IS branched out to other platforms like YouTube, Facebook and Instagram. It shocked and enraged the whole world when it posted the video of the beheading of American and British journalists and other innocent individuals. The deliberate attempt of the IS to take its social media strategy to a whole new level probably stemmed from its belief that the overly shocking and terrifying events posted online attracted the maximum viewership and

could accomplish the objectives of their propagandist campaign.

The IS has proven to be highly apt and proficient in using the power of the social media and internet as a key instrument for waging its own version of modern *jihad*. Its operatives use sophisticated forms of encryption to evade detection. Messaging apps like WhatsApp, Viber and Telegram are increasingly being used by the IS and other militant organisations. As these messaging apps use sophisticated and end-to-end encryption, the shared messages—despite their dark and insidious contents—cannot be decrypted even by the app's creators, owners and developers. Other IS members have switched to the internet's dark web— its shadowy alter ego populated by illegal sites which enables routing of a user's communication through an unfathomable maze of networks, obliterating the possibility of tracing its source. Some IS operatives have even resorted to offensive cyber tactics. A group called Cyber Caliphate urged its followers to use Twitter to spread propaganda. IS extremists posted the hacked personal details online, which included the mobile phone numbers of the heads of the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI) and National Security Agency (NSA).

The IS' use of advanced technology of the present century is, paradoxically, diametrically opposite to their *Salafist-jihadist* interpretation of Islam and their ardent advocacy of emulation of a lifestyle practised in the 7th century.

CYBER GUERRILLA WARFARE

Since World War II, insurgency and terrorism have become the dominant forms of conflict—a trend likely to continue into the foreseeable future.[36] Inter-state conflicts have become aberrations rather than existential threats; while, on the other hand, terrorism has become an increasingly regular, visible, repugnant and violent feature of the contemporary international landscape, infested with a number of insurgent, terrorist and guerrilla groups. The term "guerrilla" literally means "small war" and it gained currency during the Spanish resistance to Napoleonic French occupation

36. Max Boot, *Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present*, (New York: Liveright Publishing Corporation, 2007), p. 12.

Cyber guerrillas have created a sense of unease and apprehension for authoritarian regimes in many parts of the world. These regimes are caught in a dichotomous dilemma of reaping economic benefits by adopting information technologies juxtaposed against the political risks presented by these same technologies.

from 1808 to 1814.[37] However, evidence suggests that its various traits in various manifestations had been practised since the acceptance of conflicts/ clashes as a mechanism of achieving specific goals. It is centrally dependent on hit-and-run tactics employed by a small armed group against a much larger and more powerful group or institution for a myriad reasons varying from the political to social to religious. In guerrilla warfare, there are no delineated frontlines and set-piece manoeuvres and the focus always remains on surprise, ambush and tactical agility.

In 1962, Samuel Huntington articulated a clear and succinct definition for this type of warfare: "Guerrilla warfare is a form of warfare by which the strategically weaker side assumes the tactical offensive in selected forms, times, and places."[38] A certain amount of anecdotal folklore and revolutionary romanticism has been linked with guerrilla warfare and many of its proponents and practitioners were able to garner a cult following due to their exploits and exaggerated claims of successes. After all, in a David vs Goliath struggle, it is the underdog David who obligatorily elicits an emotional response from most of us. The accounts of Che Guevara and revolutionary guerrilla movement of Mao Tse-Tung made them legends in their time.

Since cyber space is adept in assimilating and emulating many of the virtues, vices and features of the real world, it was a matter of time for the term 'guerrilla' to be prefixed with 'cyber' and enter the lexicon of cyber warfare. The basis of concepts and convictions in 'cyber guerrilla' stems from the fact that a nondescript and non-threatening entity can suddenly

37. Ibid.
38. Samuel Huntington, *Modern Guerrilla Warfare: Fighting Communist Guerrilla Movements, 1941-1961* (New York: The Free Press, 1964), p. xvi.

spring to life and engage a large, powerful and resourceful organisation. The term 'cyber guerrilla' has a wider connotation. While conventional guerilla warfare includes small, asymmetric and revolutionary conflicts/ wars for liberation or for social, political and economic betterment, cyber guerrilla warfare is not limited by temporal, spatial, political or situational particularities. It is characterised by a number of activities, some of which fall within the classical definition of guerrilla warfare while some may take divergent forms, depending upon the context of the usage and the user's intent.

The cyber guerrilla is characterised by the use of methods which leverage the internet without a possible physical confrontation. The first fundamental characteristic of cyber guerrilla tactics is asymmetry.

The political and psychological impact of guerrilla acts may far exceed the consequences realisable through regular armed engagement. Some of the tactics applied in guerrilla warfare aim at generating momentum and garnering support for a particular cause. The revolutionary underpinnings of some of the most important guerrilla movements have manifested in armed insurgency and acts of physical terrorism. Cyber guerilla tactics can stir up revolutionary sentiments but cannot lead to,or achieve, a physical revolution on their own.[39]

Cyber guerrillas have created a sense of unease and apprehension for authoritarian regimes in many parts of the world. These regimes are caught in a dichotomous dilemma of reaping economic benefits by adopting information technologies juxtaposed against the political risks presented by these same technologies. In its earliest days, the internet was seen as a harbinger and catalyst of democratic movements and political liberalisation against authoritarian regimes.[40] In a seminal paper published in 2005, Mavhunga describe cyber space as an enabler and instrument of liberation for "cyber guerrillas" in Zimbabwe as well as a new addition to the diverse

39. Robert Reardon and Nazli Choucri, "The Role of Cyberspace in International Relations: A View of the Literature" (MIT, Paper Prepared for International Studies Association Annual Convention, San Diego, CA., April, 2012), p.18.
40. Ibid.

As most communications, including sharing of intelligence, coordination among various entities, requests for arms, ammunition, equipment, personnel, etc., take place over networks of computers, any disruption, damage or destruction of these networks due to cyber guerrilla warfare can undermine the operational preparedness and efficiency of the opponent.

arsenal of weapons being used against the Mugabe regime. The internet empowered and enabled them to "refute the misleading and ostensibly distorted narrative with its counter-narrative."[41]

"War is always a struggle in which each contender tries to annihilate the other. Besides using force, they will have recourse to all possible tricks and stratagems to achieve the goal."[42] This statement by Che Guevara effectively touches upon the dimensions and dynamics of war and how these have transformed in contemporary times. The definition of 'war' as used and understood within the context of today's politically charged and terror infested environment has acquired a wide connotation to include armed skirmishes, hybrid war, territorial war, ideological war, demographic war, low intensity conflicts, counter-insurgency operations, war against terrorism and many other forms of conflict. The tactics, strategies and technologies have evolved and all the warring sides try to take advantage of this evolutionary process by changing/ modifying/adapting existing ones. Methods, which are effective but do not rely on any overt use of force or violence in response to provocations, are increasingly being employed as adjuncts to conflicts and rivalries. Within this category, the cyber guerrilla is characterised by the use of methods which leverage the internet without a possible physical confrontation.

The first fundamental characteristic of cyber guerrilla tactics is asymmetry.[43] Guerrilla Warfare Strategy (GWS) is centred around the objectives of imposing costs on an adversary in terms of loss of combatants, severance of

41. Mavhunga, Clapperton, "The Glass Fortress: Zimbabwe's Cyber-Guerilla Warfare," *Journal of International Affairs,* 62.2 (2009), p. 160.
42. Ernesto Guevara, *Guerrilla Warfare* (Manchester: Manchester University Press, 1985), p. 53.
43. Haaster, et.al.,n. 4.

lines of communication and supply, damage to infrastructure, deprivation of peace of mind and, most important, time. With the exception of neutralising soldiers, the cyber guerrilla can achieve all the objectives of GWS. As most communications, including sharing of intelligence, coordination among various entities, requests for arms, ammunition, equipment, personnel, etc., take place over networks of computers, any disruption, damage or destruction of these networks due to cyber guerrilla warfare can undermine the operational preparedness and efficiency of the opponent. Cyber guerrilla warfare can also be effectively waged against the opponent's Critical Information Infrastructure (CII), vital to its security, economic and political stability, essential services and safety.

The constant evolution of cyber threats is a cold hard reality which will continue to cause cataclysmic upheavals in the social, political, and economic landscapes. Their scope, magnitude and implications are limited only by the ingenuity and intent of the perpetrators, and technological advancements.

Successful guerrilla warfare is flexible, not static, and the same principle extents to cyber guerrilla warfare as well. Flexibility and adaptability are two key attributes which are inextricably linked to the success of any guerrilla operation. Constant adaptation to complex and evolving situations during and after termination of operations are the hallmarks of an effective guerrilla strategy. The same notion has applicability for cyber guerillas as well. When pinned down, cyber guerillas try to break up and melt away in the labyrinth of cyber space. When a cyber guerrilla effort is pitted against a technologically superior and resource-rich opponent, the outcomes may not be always favourable for a cyber guerrilla. Therefore, cyber guerillas adopt techniques which are flexible in their approach and execution, and operate incognito in amorphous formations.

CONCLUSION

The constant evolution of cyber threats is a cold hard reality which will continue to cause cataclysmic upheavals in the social, political, and economic

landscapes. Their scope, magnitude and implications are limited only by the ingenuity and intent of the perpetrators, and technological advancements. The impact of information technology on individuals, societies and nations, at the intrinsic as well as extrinsic levels, has resulted in the imputation of new meanings to traditional forms of social deviance and crime. Cyber technology has ubiquitously infringed our daily lives and made deep inroads into several global corners, redefining the parameters of social subsistence and provision of human necessities. As a consequence, new paradigms of social deviance have arisen, old definitions have been reworded, and new challenges have been identified, leading to new paradoxes.

Some commentators view cyber technology as cataclysmic and repeatedly disparage it with apocalyptic exaggeration. They tend to overlook the fact that cyber technology is a cultural construct that does not exist in isolation from the social system. To rein in the tide of cyber crimes, manifesting in terrorist and sabotage acts, it is imperative to have situation specific and contextual knowledge, discerning dispositions and homogenised actions. Such actions, coupled with intuitive ingenuity and intuitional perceptions may stem the spate of insurgency and terrorism in cyber space.