VIF Brief
December 2019

Cyber Enabled Information Warfare

Are Cyber Borders the Solution We Seek?

Snehashree Mukherjee

Vivekananda International Foundation

Published in December 2019 by
Vivekananda International Foundation
3, San Martin Marg | Chanakyapuri | New Delhi - 110021
Tel: 011-24121764 | Fax: 011-66173415
E-mail: info@vifindia.org
Website: www.vifindia.org

Follow us on

Twitter | @vifindia
Facebook | /vifindia

The paper is the author's individual scholastic articulation. The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to be correct.

Snehashree Mukherjee is a young investigative and conflict journalist, a full-scholar at the Tel Aviv University. She holds an International M.A Degree in Security and Diplomacy.

Cyber Enabled Information Warfare: Are Cyber Borders the Solution We Seek?

In this paper, the author, based on certain grey but notable indicators, proposes an idea of 'cyber boundaries' - Editor

Abstract

Who will decide the next head of state? With the advent of third generation of information warfare, is democracy under a threat? What will be the structure of cyber vigilance institutions? Are we at a brink of cyber war which will claim casualties by turning citizens against its own state? The need for Cyber boundary is urgent, considering especially the active and defensive strategies of countries like Russia, China, Iran etc. One of the principal steps to any national security response is to 'defend the borders'. However, such response is impossible to threats in the realm of cyberspace. The scope of the paper focuses on the disinformation and propaganda, a section of Information warfare. This paper attempts to answer the question, "Are cyber-borders the solution we seek for challenges like information warfare"

Introduction

"We live in an age that is driven by information. Technological breakthroughs… are changing the face of war and how we prepare for war".
– William Perry, Secretary of Defence, U.S.A

Military scholars trace one of the earliest uses of information as a tool in guerrilla warfare to fifth-century BC Chinese military strategist Sun Tzu's book *The Art of War* and its emphasis on accurate intelligence for decision superiority over a mightier foe.[1] Although the end results and implications of Information warfare is highly uncertain, given its dynamic nature; its threat to national security posture is quite evident.

Any national information infrastructure, consists of information, information systems, telecommunications, networks and technology, which in turn is dependent on other critical infrastructures such as electrical power and other forms of energy. This interconnectivity and interdependency certainly place any system in a position for possible attack and a threat to national security.[2] One of the principal steps to any national security response is to 'defend the borders'.

1 Theohary, C.A, 'Information Warfare: Issues for Congress', Congressional Research Service, 2018, www.crs.gov

2 DeVries, A.D, 'Information Warfare and its impact on National Security (Unclassified)', Department of Joint Military Operations, Naval War College, 1997 (pg1-2)

However, such response is impossible to threats in the realm of cyberspace. One of the biggest issues is the cyber inter-connectivity within states.

The scope of the paper focuses on the disinformation and propaganda, a section of Information warfare. These words are often used interchangeably but propaganda tries to convince us to believe something whereas disinformation is a highly organised attempt to deceive us into believing it.[3] In order to explore these area, the Russian strategy of disinformation and propaganda and the case of alleged Russian manipulation in USA presidential election are considered as examples.

Figure 1 illustrates the complex network and deep interdependency of cyberspace. This paper attempts to answer the question, "Are cyber-borders the solution we seek for challenges like information warfare"? In order to approach the same, the theoretical part (Information Warfare) is divided in two sections.

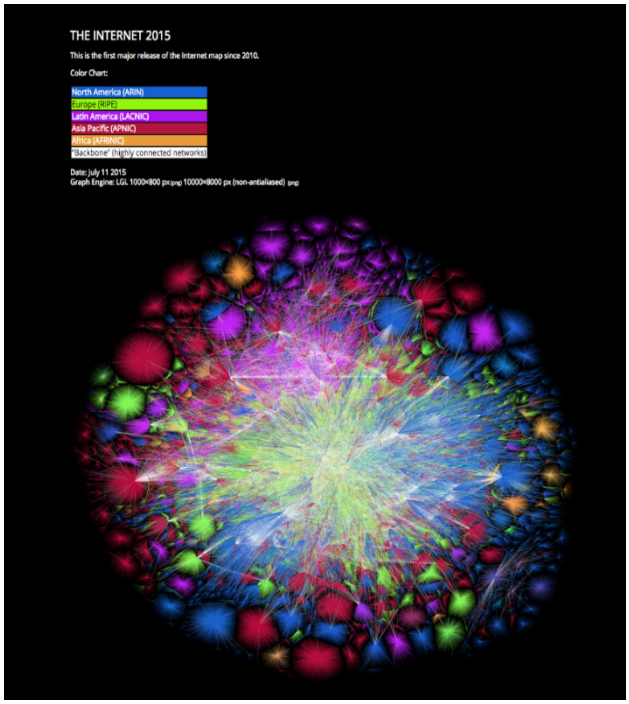

Figure1: Map of the Internet produced by Barrett Lyon and C.

In Section I, the evolving nature and features of Information warfare is discussed and segregated from similar sounding concepts. In the next Section (cyber space and borders) the concept of cyberspace and the possibility of judicial regulations pertaining to cyberspace privatisation is focussed upon, further touching the subject of the Westphalian rise of cyber borders and its necessity.

This paper finally would argue that, in an interdependent, global domain, borders can be a useful construct to address cyber security issues and inform national policy decisions, regardless of the physical location of relevant nodes. However, this paper does not suggest that sovereign powers must regulate borders to curtail the progress of nations due to cyber connections which is helping in construction of a better world via this evolving and expanding environment.

3 Operation infektion, New york Times opinion documentary

Information Warfare

"The supreme art of war is to subdue the enemy without fighting"
- Sun Tzu, The Art of War

Section I: Defining the Concept

In Section 1, The threats faced by a state in the form of Information Warfare (and similar concept) is explained, in order to give a structure to the potential of IW and its evident features.

Dan Kuehl of the National Defence University defined information warfare as the "conflict or struggle between two or more groups in the information environment". Information Warfare have historically been a government's ability to further its national strategic goals and objectives internationally through an integrated, synchronized and interagency-vetted information campaign using the tools of public diplomacy, public-affairs and international military information (DoD Psychological operations) as its media.[4] It consists of both *offensive* and *defensive operations*. It is conducted not only in crisis, conflict, and warfare in the operational sense, but is ongoing in peacetime as well (especially in Russia).

Information Warfare strategy (nature is strategic) is different from Information Operations or IO (nature is operational). The Department of Defense (DOD) Dictionary of Military and Associated Terms defines the strategic level of warfare as the level at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives. Whereas Information Operation involve using various information-related capabilities to implement this strategy.

Several other related terms are often used in conjunction with IW as they convey similar concepts:-

- **Active Measures:** Activities undertaken to achieve foreign policy objectives by state-sponsored influence operations targeting citizenry, influence operations between nations, and population-to-population influence operations.[5]

- **Hybrid Warfare**: It blends irregular, conventional and information warfare.

- **Grey Zone Warfare:** Usually falls between traditional wars and peacetime and includes the involvement of both state and non-state actors. Entails techniques to achieve a nation's goals while denying those of its rivals by employing instruments of power that do not necessarily include use of acknowledged regular military forces.

4 Col.Ward, B.M, '*Strategic Influence Operations- The information Connection'*, USAWC Strategy Research Project, pg1

5 Abrams, Steve, '*Beyond Propaganda: Soviet Active Measures in Putin's Russia*', Connections: The Quarterly Journal, Winter 2016.

- **Irregular Warfare**: A "violent struggle among state and non-state actors for legitimacy and influence over the relevant populations."[6]It is also known as tribal warfare or low-intensity conflict, often characterized by the absence of traditional military entities.

- **Unconventional Warfare:** It is the support of a foreign insurgency against its government or occupying power. It relies heavily on subversion through information and guerrilla warfare, and forces are often covert.

- **Asymmetric Warfare**: It is fought between belligerents whose relative military power or whose strategy or tactics differ significantly. Information warfare can be a successful means of overcoming the disparity.

- **Soft Power**: According to international relations scholar Joseph Nye, it is "the ability to get what you want through attraction rather than coercion or payments." This may involve the use of information with a positive spin in order to compel decisionmakers toward actions in one's own interests.

- **Public Diplomacy**: refers to government-sponsored programs intended to inform or influence public opinion in other countries; its chief instruments are publications, motion pictures, cultural exchanges, radio, and television.

Information Warfare in general share some common features; which is as follows:- [7]

- **Low entry cost:** Unlike traditional weapon technologies, development of information-based techniques does not require sizable financial resources or state sponsorship. Information systems expertise and access to important networks may be the only prerequisites.

- **Blurred traditional boundaries:** Traditional distinctions—public versus private interests, warlike versus criminal behaviour—and geographic boundaries, such as those between nations as historically defined, are complicated by the growing interaction within the information infrastructure.

- **Expanded role for perception management:** New information-based techniques may substantially increase the power of deception and of image-manipulation activities, dramatically complicating government efforts to build political support for security-related initiatives.

6 Department of Defense, "Irregular Warfare Joint Operating Concept," Version 1.0, February 27, 2009.

7 Molander, R.C/Riddile, A.S/ Wilson, P.A, 'Strategic Information Warfare, a new face of war', National Defense Research Institute, RAND, pg14

- **A new strategic intelligence challenge:** Poorly understood strategic IW vulnerabilities and targets diminish the effectiveness of classical intelligence collection and analysis methods. A new field of analysis focused on strategic IW may have to be developed.

- **Formidable tactical warning and attack assessment problems:** There is currently no adequate tactical warning system for distinguishing between strategic IW attacks and other kinds of cyberspace activities, including espionage or accidents.

- **Difficulty of building and sustaining coalitions:** Reliance on coalitions is likely to increase the vulnerabilities of the security postures of all the partners to strategic IW attacks, giving opponents a disproportionate strategic advantage.

The conclusion of the IW features indicates that in the era of 'Third Information Revolution' world Politics will not be the sole province of the governments. As the barriers to entry decline, both individuals and private organisations, ranging from corporations to NGOs to terrorists are empowered to play direct roles in world politics.[8]

Types of Information

In common parlance, the term 'disinformation campaign' is often used interchangeably with information operations. However, disinformation or deception is only one of the informational tools that can be exploited as part of an IW strategy. Factual information can also be used to achieve strategic goals and in some cases more effectively than deceptive means. Different categories of information may be used in IO, including the following:-

Propaganda: This is the propagation of an idea or narrative that is intended to influence, similar to psychological or influence operations. It can be misleading but true, and may include stolen information. A government communicating its intent, policies, and values through speeches, press releases, and other public affairs can be considered propaganda as well as public diplomacy. These communications have strategic value in that over time they can create perceptions that steer decision makers towards a certain course of action.

Misinformation: This is the spreading of unintentionally false information. Examples include internet trolls who spread unfounded conspiracy theories or web hoaxes through social media, believing them to be true. Misinformation can have the effect of sowing divisiveness and chaos in a target society, as the truth becomes harder to discern.

Disinformation: Unlike misinformation, disinformation is intentionally false. Examples include planting deliberately false news stories in the media, manufacturing protests, doctoring pictures, and tampering with private and/or classified communications before their widespread release. All of

8 Joseph. S Nye Jr., 'The Future of Power', https://bit.ly/2Irltik

these activities take place within the information environment, which is the aggregate of individuals, organizations, and systems that collect, disseminate, or act on information.

The information environment can be divided into:- [9]

1. *The physical layer*: Command and control systems and associated infrastructure.

2. *The informational layer (syntactic):* Networks and systems where information is stored.

3. *The cognitive layer (semantic)*: The minds of people who transmit and respond to information.

Section II : Cyber Space and Borders

In Section II, the idea of cyber space and borders is discussed from the prism of distinct scholars of this field.

The DOD defines *cyberspace* as, "the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Some have criticized this as lacking the cognitive, human element that the internet represents, which in turn could adversely affect how the military organizes, trains, and equips for IO.

Cyberspace as compared to land, sea, air and space is the only environment that is man-made, yet there is no physical presence of man. It is just a medium where data in various forms are being exchanged. Thus, before we discuss the possibility of boundary it's important to argue on, if it can be treated as a place or not. *Mark. A Lemle,y* in his paper '*Place and Cyberplace*' rejects the concept of 'Cyber is like a place' as it can never be equivalent to the physical world in nature. On similar lines *Dan Hunter* in his paper '*Cyberspace as Place, and the Tragedy of the Digital anti-commons*' highlights how several courts have made the mistake of overlooking the difference between the Internet and physical space and in particular applying the doctrine of trespass to chattels to email and website access. They both point out that hackers cannot be treated equally to trespassers and judicial applications of laws like Computer Fraud and Abuse Act which was designed to punish malicious hackers is not full-fledged as no one "enters" website. In order to reach such results where cyber is treated equivalent to physical privately owned land in cases like eBay vs. Bidder's Edge, Register.corn vs. Verio, and Intel Corp. v. Hamidi, a court must conclude not only that cyberspace is a place but also that a particular type of property law is appropriate for that place.

Having said that, states have already started creating *cyber boundaries* in the name of security and economic sustainability. It is also perceived as the rise of Westphalian age in Cyber by scholars like *Demchak, Chris C. and Dombrowski Peter*. In their paper '*Rise of a Cybered Westphalian Age*' they describe

9 Model by Martin Libcki, mentioned in 'Cyberspace and the State: Toward a Strategy for Cyber-Power', Betz David, Stevens Tim.

the need of frontiers. They say, "Frontiers are places of conflict between groups, historically lightly and poorly governed, less populated, and risky—places where value is extracted for little cost. When a frontier starts to become a commons, productivity for all is imperilled by the grab-and-go nature of those using it. Those dependent on the frontier tend to form organizations to control their claim. Modern democracies are in essence complex aggregates of large-scale organizations. Their leaders routinely reach out to absorb uncertainties to control them, if possible, or push them away. The rising perception of a national-level threat means that all states, in one way or another, will reach out to control what they fear from the Internet—its frontier nature and the lack of sovereign control over what comes into their area of responsibility."

Although other organisations like Homeland Security would disagree and in their opinion, "Unlike traditional border security, the government's role in defending the nation from foreign cyber intrusion is far less robust. Rather than focusing on preventing the entry of cyber threats, the government functions in a response role, investigating after the fact and after an attack has occurred. Defense of the nation's cyber frontier is largely left up to private entities, both persons and organizations, to protect their own cyber borders."

The traditional border set up is largely a product of The peace of Westphalia which is a territorial design protected by boundaries segregating states. It gave birth to the concept of 'national security'. The key element of this process was the legitimacy of state control, they could defend the territory against outside aggressors against any national security threat. Similar intentions to create boundaries in cyberspace are already in process as discussed above. The scope of the paper focuses primarily on the possible solution rather than its technical possibility.

Today the technological filtering occurs largely through private or semiprivate institutional intermediaries. Across the bulk of democratic and nondemocratic states, ISPs are finding their ability to continue to provide services is increasingly dependent on providing filtering services determined by large, state-level authorities. There is no technological reason why these services cannot continue as regulated utilities, nor is there any reason why governments cannot control what runs into the nation from overseas cables or runs out of the nation to criminally harm citizens of other nations.[10]

Cyber boundary will not only empower a state to take actions it will also provide a system to attach and reveal identities to the offenders, an escape from the political shadows and warfare techniques. Such a concept can only be functional if it's under an agreement signed by all states like Westphalia. The complex and deep integrated nature of internet networks cannot be treated in the same fashion as physical territory. Such highly influential and strategical zone if left borderless and without any law, can eventually give rise to medieval anarchy situation where states will be critically challenged by non-state actors from outside and within.

10 Demchak Chris. C, Dombrowski. P, 'Rise of a Cybered Westphalian Age', Strategic Studies Quarterly, Spring 2011, Pg 41

The Russian Threat

In short, the Soviet approach to international relations can perhaps best be described as a form of "political warfare" with the manipulative and deceptive techniques of active measures playing an essential and important role."
-USIA Report, Soviet Active Measures in the "Post - Cold War" Era 1988-1991

In February 2017, Russian Defense Minister Sergey Shoigu openly acknowledged the formation of an Information Army within the Russian Military. He said, "Information Operations forces have been established that are expected to be a far more effective tool than all we used before for counter-propaganda purposes." The current chief of the Russian General staff, general Valery Gerasimov, observed that war is now conducted by a roughly 4:1 ratio of non-military and military measures.[11]

With roots in Leninist thinking, over generations the Soviets mastered a range of techniques known as 'aktivnyye meropriyatiya' or 'active measures' ranging from simple propaganda and forgery to assassination. A 2009 Volume of the CIA's professional journal, 'Studies in Intelligence', explains the method of active measures which were in use during the Soviet Era, and describes their implementation:-

- Center gives *strategic-go- ahead* for a disinformation campaign.
- *Ideas* would be generated by residency officers assigned to read local press, books and magazines for material that could be use for disinformation purposes.
- Center would *evaluate* the ideas.
- At the Center, *Preparation* involved disinformational specialist writing in their native language, *approvals* by managers and *translation*.
- *Targeting* followed. The Center typically sought to launch a story outside the *Soviet bloc-controlled press* to conceal Moscow's hand. This was done frequently through *anonymous letters* and newspaper *articles* in the Third World.
- Once published abroad, the *Soviet Media* might pick up and further *propagate* the item by referring to its *non-Soviet* source.

One of the most recent example is the alleged involvement of Russian disinformation strategy to manipulate the second largest democracy's 2016 elections.

11 Waltzman Rand, '*The Weaponization of Information: The need for Cognitive Security*', Testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity, April 27, 2017.

(Alleged) U.S.A Elction Manipulation By Russia

During the elections, conspiracy theories spread throughout 4-chan and extremist circles of Twitter and Facebook, claiming that Hillary Clinton was deeply involved in a child sex ring and satanic rituals. These claims were then taken up by a series of sites designed to look like mainstream news outlets, which published sensationalist false content to gain advertising revenue.[12] Throughout late October and early November, more and more such sites published versions of the same story on Facebook, and their links gained hundreds of thousands of shares, reactions, and comments. (The conspiracy theory was also spread by amplification from Trump's team when his pick for NSA tweeted about it)[13].

Soon after, Wikileaks published hacked E-mails from Hillary Clinton's campaign, and 4chan users communally combed through emails from her campaign chair Joh Podesta. They honed in on an email conversation in which Podesta and the owner of a Washington, DC Pizza restaurant called Comet Ping Pong, discussed the details of a Clinton fundraiser set to take place there. Now thoroughly "convinced" of the conspiracy theory about Clinton, 4-chan users identified a series of "clues" that they believed pointed to the fact that Comet Ping Pong was the head-quarters of the purported child sex ring. [14]The theory became known as 'Pizzagate'.

The restaurant owner and his employees soon became the victims of continual harassment, receiving death threats and other threats of violence.[15] On December 4, a man entered Comet Ping Pong carrying an assault rifle, claiming to be there to investigate the claims himself (He fired shots, but no one was harmed).[16] The man was not himself an active member of the alt-right; he has even claimed he is not political and did not vote for Donald Trump.[17] He did, however, state that he read a number of articles on the subject and listened to Alex Jones, who actively promoted the theory.

As in previous cases, mainstream outlets considered the gunman incident news-worthy, and in covering it, they increased exposure to the conspiracy theories. Additionally, even though the gunman did not find any evidence to support his beliefs, the incident has not placated many of the conspiracy theorists. As recently as March 25 2017, protestors gathered outside the White House to demand further investigation.[18]

12 Silverman Craig, "How the Bizzare Conspiracy theory behind 'pizzagate' was spread", Buzzfeed news, Nov 4, 2016.

13 Aaron Blake, "Michael Flynn's tweet wasn't actually about #PizzaGate, but his son is now defending the baseless conspiracy theory", The Washington Post, Dec 5, 2016.

14 Cecilia King, "Fake News onslaught targets pizzeria as nest of child-trafficking", The New York Times, November 21, 2016.

15 Ibid.

16 Eric Lipton, "Man arrested in Pizzagate theory arrested in Washington Gunfire", The New York Times, December 5, 2016.

17 Adam Goldman, "The Comet Ping Pong Gunman answers our reporter's question", The New York Times, December 7, 2016

18 Michael E. Miller, "Protestors outside white house demand pizzagate investigation", The Washington Post, March 25, 2017.

In late July 2016, soon after WikiLeaks's first release of stolen documents, a foreign government contacted the FBI about a May 2016 encounter with Trump Campaign foreign policy advisor George Papadopoulos. Papadopoulos had suggested to a representative of that foreign government that the Trump campaign had received indications from the Russian government that it could assist the campaign through the anonymous release of information damaging to Democratic presidential candidate Hillary Clinton. That information prompted the FBI on July 31, 2016, to open an investigation into whether individuals associated with the Trump Campaign were coordinating with the Russian government in its interference activities. The result of which was the Mueller Report. Special Counsel Robert Mueller began his testimony before a House Panel with an opening statement that called Russian efforts to interfere in the 2016 election that sent President Donald Trump to the White House among the "most serious" challenges to American democracy.

The first form of Russian election influence came principally from the Internet Research Agency, LLC (IRA), a Russian organization funded by Yevgeniy Viktorovich Prigozhin and companies he controlled, including Concord Management and Consulting LLC and Concord Catering (collectively "Concord").[19] According to Section 1 of the Mueller report, the IRA later used social media accounts and interest groups to sow discord in the U.S. political system through what it termed "information warfare."The campaign evolved from a generalized program designed in 2014 and 2015 to undermine the U.S. electoral system, to a targeted operation that by early 2016 favoured candidate Trump and disparaged candidate Clinton. The IRA's operation also included the purchase of political advertisements on social media in the names of U.S. persons and entities, as well as the staging of political rallies inside the United States. To organize those rallies, IRA employees posed as U.S. grassroots entities and persons and made contact with Trump supporters and Trump Campaign officials in the United States. The investigation did not identify evidence that any U.S. persons conspired or coordinated with the IRA. By the end of the 2016 U.S. election, the IRA had the ability to reach millions of U.S. persons through their social media accounts.

In November 2017, a Facebook representative testified that Facebook had identified 470 IRA-controlled Facebook accounts that collectively made 80,000 posts between January 2015 and August 2017. Facebook estimated the IRA reached as many as 126 million persons through its Facebook accounts. On 6 January 2018, Twitter announced that it had identified 3,814 IRA-controlled Twitter accounts and notified approximately 1.4 million people Twitter believed may have been in contact with an IRA-controlled account.[20]

In February 2018, Special Counsel Robert Mueller indicted 13 Russian nationals for their involvement in the U.S. election. [21]

19 Mueller report, U.S Department of Justice.

20 Ibid

21 Ibid

Discussion

A statement that the investigation did not establish particular facts does not mean there was no evidence of those facts.
-Mueller Report, Vol.1, p.2

U.S election manipulation is a classic case of active measures and exercise of soft power. The alarming part is the 'urgent' threat to democracy and the systems of states created as a result of Peace of Westphalia.

The Russian government which strongly advocates communism, in this case launched a targeted non-military but highly effective operation, taking advantage of unregulated cyber borders and using third country cyber identity to realise its objectives. Russian strategy document, the Convention on International Information Security, defines IW as "a conflict between two or more States in the information space with the goal of inflicting damage to information systems as well as carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents.

To accomplish these goals, Russia appears to be using social media tools to spread a mix of propaganda, misinformation, and deliberately misleading or corrupted disinformation. The nature of these activities, particularly tampering with a sovereign nation's internal democratic processes and systems, has raised questions as to whether they constitute an act of war or espionage. While some Russian doctrine suggests that these subversive activities are a way to "prepare the battlefield" in advance of a conflict, it may also be the conflict itself: information warfare is a way to weaken a militarily superior adversary without firing a single bullet.

Other activities conducted outside of cyberspace include production of pro-Russia television shows and broadcasts in Russian speaking areas of NATO, deploying soldiers in Ukraine for propaganda purposes, and the use of "little green men," armed soldiers without insignia, allowing plausible deniability of a military incursion in Crimea while creating fear and intimidation among the local population.[22] Russia is also one of the country which has maintained a very regulated cyberspace. Since 2012, Russia maintains a centralized internet blacklist (known as the "single register") maintained by the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor). The list is used for the censorship of individual URLs, domain names, and IP addresses.

Just for an idea, following are the cyber-defence steps taken by Russian govt.:-

- July 2012: The government can blacklist websites to be shut down or banned by Internet Service Providers.

22 Shevchenko, Vitaly, "Little Green Men or Russian Invaders?", BBC News, March 11, 2014 http://www.bbc.com/news/world-europe-26532154.

- December 2013: The government can block online sources, within 24 hours and without a court order, that call for public demonstrations.

- July 2014: Internet sites with data on Russian citizens must store within the country.

- July 2016: Telecommunications firms and some internet companies must store communications for six months after creation.

- July 2017: Virtual private networks are banned.

- April 2018: The encrypted messaging app, Telegram is banned.

- June 2018: Legislation is proposed in parliament to fine search engines linking to banned sites, VPNs

The question if cyber borders are the solution, that we seek is answered by the defence strategy of the greatest offenders. Russia, China, U.S.A, Israel are the top most countries with highly regulated cyberspace. In another words these countries have already taken the road towards establishing cyber borders in one way or another, and it's just a matter of time until the rest of the states follows.

Conclusion

While exploring the question, if cyber borders are the solution we seek, there are various aspects that one can consider like the need and possibility of cyber borders, nature of cyber borders, the challenges involved due to its integrated nature in territorial states, the possibility of privatisation of cyberspace and last but not the least the technical nature involving the cyberspace.

The scope of the paper dealt with the need of cyber borders with respect to information warfare. U.S election manipulation is one of the recent and potent example to illustrate the potential of threat due to information warfare and the need of cyber borders. Cyber borders, as a result of a similar treaty to peace of Westphalia, can result into a system where progress of nations due to cyber connections- which is helping in construction of a better world via this evolving and expanding environment - is maintained and at the same time, there is a jurisdiction under which threats like Russian influence or non-state actors (terrorists) are curtailed.

Cyber enabled information warfare is the third generation of Information Warfare which is changing the nature of global power shift. The reduction of cost of barriers to entry has led to power diffusion, changing the age old trend of power transition. This has given an open field to exercise various forms of soft power by various states like Russia, China and Iran. Although IW in itself cannot be the only face of war but it definitely is proving to be the seed to germinate conventional wars amongst state. Without cyber borders, a legal jurisdiction, who do we blame, how do we punish, and when can we feel safe?

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organisation to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelise fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its inception, VIF has pursued quality research and scholarship and made efforts to highlight issues in governance, and strengthen national security. This is being actualised through numerous activities like seminars, round tables, interactive dialogues, Vimarsh (public discourse), conferences and briefings. The publications of VIF form lasting deliverables of VIF's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

VIVEKANANDA INTERNATIONAL FOUNDATION
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org,
Website: https://www.vifindia.org
Follow us on twitter@vifindia