# Information Warfare and Influence Operations

Air Marshal Anil Chopra PVSM AVSM VM VSM*

In the aftermath of the Indian Air Force (IAF) Balakot airstrikes of 26 February 2019, and the Pakistan Air Force (PAF) riposte of 27 February, began a propaganda and perception war. The social media battle had the public of both nations as active participants. The importance given to Information Warfare (IW) by Pakistan against India was visible. Former Pakistan President Gen. Musharraf averred that 'on Balakot, we have divided India into two'. It underscores the sinister objective of Pakistan Army/ISI combine of this disinformation campaign.[1] The target of the Pakistan information war is not only Indian armed forces but the entire Indian public perception. Today, a seemingly soft-attack of disinformation delivered through rhetoric and imagery could be as decisive as physical military weapons. The era of perception management is now here and an important part of the war. There is a clear grey area between war and peace and the line between preparation for cyberwar and the actual fighting now is difficult to draw. The political effect of information technology, which has near seamlessly connected the world, has reshaped both competition and conflict, and in turn the security paradigm, and has started affecting the world power structure. The IW and Influence Operations (IO) are now clubbed together as part of the overall Cyberwar which has already been used in many recent conflicts.

## Cyber Era and Information Warfare Evolve

### Cyber Era

Cyber Era emerged from the use of computer networks for communications, entertainment, and business. The new forms of network communications include, online communities, online multi-player gaming, wearable computing, social gaming, social media, mobile apps, augmented reality, and texting. The cyberspace covers entire societies and has made the global public an active participant. It has thrown up issues related to identity (anonymous), location and privacy. With the rise in internet penetration, cyber crimes and use of the internet for offensive actions to deny, corrupt or destroy the use of networks by opponents has snowballed. Cyber attacks could manipulate or leak private information. States exploit the internet and its global reach for coercive purposes, often using relative anonymity, and deniability.[2] While cyber-attacks can be used to produce effects similar to kinetic weapons, the intangible effects are more important. The manipulation of information and decision making adds complexity, provides a source of military advantage, and challenges conventional, kinetic-oriented strategies.[3] Cyber operations allow coercive actions below the implicit thresholds and minimal risk of escalation.

*Air Marshal Anil Chopra is a Fighter Pilot and a Test Pilot who commanded a Mirage 2000 squadron and was head of India's Flight Test Centre ASTE. He has been Member of the Armed Force Tribunal.

## The Internet and Governance

The internet is transforming society, business, and politics as more people use new opportunities online. Knowledge is available at a lower cost and from an array of sources. The internet has redefined the role of the state and strengthened the primacy of the individual. All countries face a political challenge from the internet. The internet also provides individuals new ways to attach their loyalties and to identify with groups. It also disconnects public discussion from a physical location. Individuals with extreme views, earlier isolated from the community, can now share beliefs with thousands. The decentralised media is open to millions of contributors displacing the editors of the past. The internet allows citizens access to information and direct involvement in decision making. Policy and law thus need to evolve to take into account citizen expectations.

Authoritarian regimes try to suppress by restricting access to information, pumping counter-narratives, and using the internet for surveillance to maintain control.[4] Chinese use it to impose conformity in discussion and opinion in their population, and even extend to other countries. Russians have tried to use it to shape the Western view. To defend own populations from information 'onslaught', countries try to create a powerful counter-narrative of own heroic nationalism.

## IWIO Definition

Information Warfare and Influence Operations (IWIO) may be defined as the deliberate use of information on an adversary population to confuse, mislead and ultimately influence the actions that the targeted population makes. IWIO is a hostile activity. Yet, IWIO does not constitute warfare in the Clausewitzian sense, nor is recognised under the U.N. Charter. IWIO is part of soft power, and include propaganda, persuasion, confusion and deception. As Sun Tzu, had said, "The supreme art of war is to subdue the enemy without fighting".[5] IWIO take place without kinetic violence and operate below any threshold of armed conflict. In IWIO there are no noncombatants. Entire adversary population is a legitimate target.

## IWIO Categorisation

- IW can be divided into three general categories.
- Offensive - deny, corrupt, destroy, or exploit adversary's information, or influence the adversary's perception.
- Defensive - safeguard oneself from similar actions.
- Exploitative - exploit information promptly to enhance own decision/action cycle and disrupt the adversary's cycle.

## Basic Features of Strategic Information Warfare[6]

- The seven defining features of strategic information warfare.
- Low entry cost: Unlike traditional weapon technologies, development of information-based techniques does not require sizable financial resources. Information systems expertise and access to networks is the only prerequisite.
- Blurred traditional boundaries: Traditional distinctions public versus private interests, warlike versus criminal behaviour, and

geographic boundaries between nations are blurred within the information infrastructure.

- An expanded role for perception management: Information-based techniques substantially increase the power to manipulate perception.
- Strategic intelligence challenge: Poorly understood strategic IW vulnerabilities diminish the effectiveness of classical intelligence collection and analysis methods.
- Tactical warning and attack assessment problems: There is currently inadequate tactical warning system for distinguishing between strategic IW attacks and other kinds of cyberspace activities.
- The difficulty of building and sustaining coalitions: Coalitions may increase the vulnerabilities of the security postures of all the partners to strategic IW attacks.
- Irrelevance of geographical distance: Targets in the deep hinterland are just as vulnerable as in the tactical area. Given the increased reliance of the economy and society on networked information infrastructure, a new set of strategic targets have emerged.

### Influence Operations (IO)

IO involves convincing, confusing, distracting, dividing, and demoralising the adversary population. Disruption, rather than destroying, comprising or stealing information by accessing networks. Perceptions determine how each actor chooses to act. Manipulated perceptions can influence the battlefield. IO includes clandestine and intrusive activities as part of armed conflict. Russia fought and won an "information war" during the run-up to the Crimean vote. IO is also part of diplomacy. American expert Martin C. Libicki has summarised that "coming to grips with information warfare is like the effort of the blind men to discover the nature of the elephant: the one who touched its leg called it a tree, another who touched its tail called it a rope, and so on".[7]

### Psychological Warfare

It is a broad term related to the emotional aspect of communication, where information involving psychological components is delivered to a target audience to bring a shift in its emotions and outlook. It then brings a shift in the target audience's behaviour. It could also create conditions for surrender or encouraging defection. Psychological warfare is used both during war and peace. Crippling government utility websites, sending damaging messages to the civil population and shutting down media sites for a limited time could have a psychological effect.

## Technological Issues

### Fifth Generation Networks

5G cellular network technology which has started unfolding since late 2018, with substantial deployments since April 2019, provides much faster broadband access. As it replaces current 4G networks, it will accelerate cellular data transfer speeds from 100 Mbps to 10 Gbps and beyond. 5G radio hardware is already in the market. 5G is crucial for the Internet of Things (IoT). Because of espionage fears on foreign users by Chinese equipment vendors, several countries have taken

actions to restrict or eliminate the use of Chinese equipment in their respective 5G networks. 5G will become a faster tool for IW.

### Artificial Intelligence and Cyber Weapons

New Cyber weapons are using Artificial Intelligence (AI) and would be more damaging and destructive. AI-based equipment and systems will bring fundamental changes to military operational planning and execution. AI will allow cyber weapons to exploit existing vulnerabilities and create new ones. China is making efforts to transform 'informative' warfare into 'intelligentised' warfare by using AI.[8]

### Quantum Cyber Security

The development of large quantum computers, along with the extra computational power they will bring, could have a fundamental effect on cybersecurity. Discrete log, whose presumed hardness ensures the security of many widely used protocols, can be broken if a sufficiently powerful quantum computer is developed.[9] The actual prospect of building such a device has only recently become realistic. Quantum technologies may seem negative for cybersecurity, but can be used to own advantage.

### Cybercriminals and Data

The abundance of data and technology provide both challenges and opportunities. A significant part of the world population is still offline. Once they come on board the challenges will be even more complex. Technology facilitates online disinformation, global cyberattacks and terrorist media campaigns. Cyber money laundering and thefts could increase with Cryptocurrency, and greater use of AI.[10] There is now AI technology to create deep-fakes and influence public beliefs and also make evidence difficult. Adoption of end-to-end encryption can make attribution difficult, and globalised real-time communication make jurisdiction difficult. Surveillance-camera records, extracts of social media activities, GPS coordinates of the occurrence are critical evidence but can be manipulated.

### Naming and Shaming - Doxing

Doxing is the Internet-based practise of researching and broadcasting personal information.[11] It could also be obtained through cyber-attack and used for publically shame or embarrass targets. This type of action is on the rise. Countering Doxing is often counterproductive because public memory is short and issue dies down as populations become more aware. It, however, remains a nuisance and fuels insecurity.

## Manipulating Media

### Manipulating Public Opinion

In the 1960s, American diplomat and politician Daniel Moynihan had said that everyone was entitled to their own opinions but not to their facts.[12] The internet allows people to have their facts. Social media amplifies this trend. Many countries use internet trolls to shape social media narrative in ways favourable to their regimes and damaging opponents. Pakistan's Director-General of Inter-Services Public Relations (DGISPR) has a large team of personnel to set the tone of narrative on

social media to manipulate public opinion in Pakistan and India. Nowadays, strategic communication firms take contracts from governments for social media campaigns.

### Government Influenced Media

Information technology and the internet can provide a tool for leaders. Authoritarian regimes like in China, fear that it can be used by their opponents, as happened recently in Hong Kong. Qatar government started Al Jazeera's English language service, in 2006 to challenge established narrative and give the global audience an alternative voice.[13] Sputnik, Russia Today (RT), and China's Global Times were created to provide an English language version and promote a more positive view. China purchased media outlet, the South China Morning Post in 2016, through the Alibaba group, for reshaping opinions. The success of all this is mixed, as the public can see the hidden agenda. In 1926 a leading Chinese dissident and author, Lu Xun, wrote, "Lies written in ink can never disguise facts written in blood".[14] Governments use internet trolls and favourable television channels to shape public opinion.

### Social Media Soldiers and Fact Check

Cyber troops are a pervasive global phenomenon.[15] 'Social media soldiers' actively advance national goals on social platforms. Social media has provided opportunities for 'citizen journalism', and they have no less weight than the major content producers and established media personalities. Unfortunately, any information may be manipulated or given a tilt. Some countries like Pakistan are successfully using automated trolling through the use of 'chatbots'. Many websites and cyber handles have now come up for 'fact-checking', to help the public know the truth, but they are not being able to keep pace.

## Influence of Operations Campaign

### IWIO Identification

For an IWIO campaign to be successful, it should be invisible, as the primary goal is to make adversary population an unwitting accomplice. Conversely, the identification of a foreign hand is central for detecting an IWIO campaign. Unlike kinetic weapons, a cyber campaign may not be detectable. The sudden emergence of large numbers of automated social chatbots promulgating similar political messages could signal the start of a concerted campaign.[16] Combination of volume (messages per day), type of content, and platform could help identify automated IWIO weapons carrying divisive or inflammatory messaging.[17] The investigation could point to national affiliations. Coordination among intelligence-gathering agencies will improve capabilities for detecting IWIO campaigns.

### Effective Campaign

An effective IW campaign must feature social media, intelligence and cyber units at the tactical and strategic level for military and political influence. The campaign must disrupt the enemy's ability to accurately grasp reality and establish an effective response. Breeding negative feelings, doubt, fear and uncertainty in the public perception will have its impact. Pumping information through a 'personalised' model, to individuals or groups

based on geography, interest, or passion will always work. IO should be conducted along with offensive cyber operations to disrupt the opponent's communications. Development of dedicated cyber warfare tools for social media is important. The initiator wrests advantage in the overall campaign.

## Defence Against IWIO

### Responses to IWIO

Mobilisation of intelligence resources, psychological warfare, public diplomacy, social media platforms, political and legal channels and dissemination of counter-narrative more aggressively, to own advantage, is important. It has to be a collaborative yet decentralised effort of state and military. Liberal democracies, committed to adhering to laws, need to find national security-related means to overcome bureaucratic and political complexities. Identifying the national affiliations of individuals operating such bots is important. Coordination among intelligence-gathering agencies, tactics and technologies used, may provide early warnings of an impending IWIO campaign.

### Preparing Individuals For IWIO

Although the volume and velocity of information have increased phenomenally, the architecture of the human mind has not changed appreciably over the last few thousand years. Public needs to be supported for defensive measures to resist the IWIO weapons targeted at them. As humans, we are subject to a variety of systematic cognitive and emotional biases which often distort our ability to think rationally and clearly. It will be worth-while inoculating own population against fake news, by exposing the original message and flagging the false claim. Meanwhile, the organisation must take measures to degrade, disrupt or expose the adversary's IWIO campaign.

### International Fact-Checking Network (IFCN)

IFCN has been set up to promote excellence in fact-checking and accountability in journalism.[18] Responsible media must make commitments to nonpartisanship and fairness; transparency of sources, and funding. Facebook is already committed to providing fact-checking services to Facebook users. Facebook has also introduced an option making it much easier for users to signal if they regard a given story as fake news. For political advertising on Facebook are required to include information about who paid for them. With advanced Photoshop and audio and video editing software widely available, the authenticity of images and recordings should not be automatically trusted.

## Military Approach to Information Warfare

### Military Cyber Capabilities & Strategies

USA, China, Russia, Iran, and North Korea, have well-developed military cyber capabilities. Cyber operations are combined with electronic warfare, anti-satellite attacks, informational campaigns and other unconventional tactics and weapons. The intent is to degrade enemy 'informational warfare advantage' by attacking communications and ISR assets and capabilities;

slow and damage decision making and operations; and to create political uncertainty, turmoil, and dissent. Actions are laced with espionage techniques through new military doctrines. Pre-conflict opinion-shaping could create political turmoil and discord.

### Cyberspace Upsetting Status Quo

A Center for Strategic and International Studies (CSIS) report of September 2018[19] has brought out how information technology is reshaping international security and helping new resurgent powers to upset the status quo in the existing world order. Cold War was bipolar, but a new conflict is multi-polar. Wars between heavily-armed states are expensive and risky, so cyberspace has become the preferred battleground, taking advantage of the 'grey area' that is neither peace nor war.

### Well-Known IWIO Operations

'Operation Cupcake'[20] was launched by MI6 in 2011, to replace al-Qaeda bomb-making instructions with cupcake recipes. When followers went to download 67 pages of instructions for how to "Make a Bomb in the Kitchen of Your Mom" from 'Inspire Magazine', al-Qaeda's first English-language magazine, the terrorists were instead greeted with a page of cake recipes. In May 2014, the group known as Cyber-Berkut compromised the computers of the Central Election Committee in Ukraine.[21] This hack did not hinder the election process, as voters had to cast an actual physical ballot. It did, however, damage the credibility of the Ukrainian government in overseeing a fair election process. In April 2015 the French television network TV5 Monde was the victim of a cyber-attack from hackers claiming to have ties with Islamic State's (IS) 'Cyber Caliphate'.[22] Later in June 2015 investigators revealed that Russian hackers used the pseudonym of IS 'Cyber Caliphate' for this attack.

## Cyber Warfare Military Structures

Several countries have set up military cyber command structures and have formulated national cyber strategies to deal with the emerging threats in cyberspace.

### United States Cyber Command (USCYBERCOM)

USCYBERCOM was created in mid-2009 at the Nation Security Agency (NSA).[23] Initially created with a defensive aim, it has been viewed as an offensive force. In May 2018 USCYBERCOM was elevated to the status of a full and independent unified combatant command. IWIO is an important part of the operations. The Joint Information Operations Warfare Center is subordinate to the Joint Chiefs of Staff and is manned by experts from military, government and private sector.

It serves as an IW authority for all U.S. Department of Defense (DoD) agencies. The teams advise combat forces on the ground on how to carry out IO strategies. The U.S. Central Command (CENTCOM) is one of the main entities tasked with organizing influence operations. CENTCOM has teamed with people fluent in languages such as Arabic, Urdu, Persian and Russian.

## EU and United Kingdom

The British 77th Brigade[24] was created in 2015 to execute psychological warfare worldwide. In November 2015, the European External Action Service (EEAS) established a special task force charged with countering Russian disinformation campaigns and enhancing participants' capacity and interoperability.

## Russia's Gerasimov doctrine

Russia seems to have integrated cyber operations into national strategic capability because it acknowledges that it cannot match the military power of NATO. Gerasimov doctrine[25] acknowledges that non-military means of achieving political and strategic goals have exceeded the power of weapons in their effectiveness. These include intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems, and propaganda. They use distributed denial of service attacks, and advanced exploitation techniques. Russia's successful use if IO during the Ukraine crisis is well known.

## Israeli IWIO Approach

Israel has three military entities. The Center for Consciousness Operations was established in 2005,[26] and coordinates with the operations branch and military intelligence directorate. During operation 'Cast Lead', the centre-mounted psychological warfare in the Gaza Strip against Hamas, and messages were delivered through newscasts and broadcasts. Israeli C4I Corps is primarily tasked with launching IW against the enemy. The PR branch of the IDF manages PR missions for a variety of overseas conferences and helps pen studies overseas written about the IDF.

## China's Aggressive Approach

The Cyberspace Administration of China (CAC)[27] is the central Internet regulator, censor, oversight and control agency, and comes under Central Cyberspace Affairs Commission headed by President Xi Jinping. China has a national-level data protection strategy. China's first "cybersecurity innovation centre" was established in December 2017. Operated by 360 Enterprise Security Group, the centre's remit is to "help the military win future cyber wars." The People's Liberation Army (PLA) has escalated its partnerships with the civilian telecoms sector, especially ZTE and Huawei, and universities. The Strategic Support Force (SSF) was established in December 2015 by merging and centralising all the PLA's space, cyber, and ISR (intelligence, surveillance, reconnaissance) capabilities. The SSF has assumed control over several PLA research institutes where it will pursue R&D.

China has employed hundreds of thousands in Cyber warfare. All are specially trained and most are English proficient. PLA Unit 61398 has been very active in cyber espionage and cyber-attacks. The unit is located in the Pudong area of Shanghai. Pudong also happens to be the location of the main undersea cable between China and the United States. They have reportedly stolen hundreds of terabytes of data through an extensive network of computers spread across the world. The attack on Google in 2009 was essentially to steal intellectual property rights and assess and use the

near 500 million Google user passwords. Major targets are strategic industries, defence establishments, weapon and military technology companies. China's IWIO efforts are focused primarily on its population and Chinese emigrants. Chinese propaganda has persuaded the world of its inevitable economic ascendancy. To gain access to U.S. weapons systems, to understand their operational limits, copy them, and to prepare to interfere with their operations in combat China has undertaken cyber operations. China works on cyber operations combined with electronic warfare, anti-satellite attacks, informational campaigns and other unconventional tactics and weapons.

## Major Military Cyber Campaigns

### US Online Offensive Against ISIS

The U.S. government launched IWIO operations against Islamic State (ISIS) and al-Qaeda because of these organisations increasing capacity to use social media networks. ISIS had successfully utilised social media to target and enlist potential recruits appealing to young people across the globe. U.S. campaign against ISIS was run in Arabic, Urdu, Persian and Russian languages. They used Twitter, Face book and Instagram to communicate with the populations of 20 countries in the Middle East and Central Asia. A post shared by an ISIS fighter included photos of ISIS command headquarters. The U.S. Air Force was able to identify its location and demolished it within 24 hours. U.S. military operations also destroyed ISIS's communications infrastructure. Moderate Muslims, talented university teams helped create media campaigns. In 'Operation Glowing Symphony' in 2016, U.S. cyber units obtained the passwords and access codes of ISIS operatives.[28] They used them to block access to internet assets and delete content used for propaganda and recruitment.

### Pakistani and Jihadi Approach

Since Pakistan is at a deep disadvantage in terms of conventional military power, it leverages asymmetric options like terrorism and IWIO. They create "deep fakes" videos which appear authentic. Use India's internal social cleavages. Pakistan has run a proxy war over the last three decades in Afghanistan and Kashmir. A group of Pakistani hackers has been hired by the Pakistani Inter-Services Intelligence (ISI) to create spyware versions to target key government officials in India. ISI supports jihadi terror organisations to use cyberspace for the collection of sensitive information and spreading misinformation. Pakistan military is also using radio and TV channels for spreading anti-India propaganda. Jihadi groups are using websites to incite the youth to take to arms. The maximum number of communal incidents in India was preceded by a focused circulation of fake videos inciting people to resort to violence.

## IWIO and Cyber Threats India

### Cyber Target - India

According to a report, in period January-May 2018, of the cyber-attacks in India, almost 40% originated from China, 25% from the US, 13% from Pakistan and 9% from Russia. The attacks from Pakistan are on the increase. The targets

were financial networks, government websites, power plants, oil refineries, and telecom and defence networks. During the first six months of 2018, almost one billion records were compromised in Aadhaar breach incident, including name, address and other personally identified information, according to a report by digital security firm Gemalto. This, however, was denied by UIDAI. The Cambridge Analytica firm was suspected to have harnessed data from almost 87 million Facebook users, out which over half a million were Indians, and leveraging them for political campaigns. Similarly, Microsoft has reportedly has shared the financial details of Indian bank customers with intelligence agencies in the United States. The Chinese website of official newspapers like Global Times and People's Daily contains anti-India articles.[29]

India is one of the fastest-growing markets of social media users but unfortunately due to lack of awareness, laws and mechanism to check the spread of rumours, fake news and manipulated videos, it is easy to manipulate Indian population. Pak ISI cum jihadi combine is increasingly using cyberspace for collection of sensitive information and spreading misinformation. Haribhai Parathibhai Chaudhary, as MoS Home, informed the Parliament in 2016 that ISI was using smart-phone malware embedded gaming, music apps to spy upon military personnel[39]. Even Indian political parties are exploiting them for electoral advantages or to create communal disharmony.

### Chinese Electronic Hardware Threat

India's heavy reliance on imported equipment and mobile apps pose a serious security challenge. Indian intelligence agencies have warned that China was collecting data from India through popular Chinese mobile apps. The Chinese Xiaomi smartphones and notebooks are suspected to be transmitting personal data to the servers located in China. China is exporting devices equipped with backdoor surveillance tools. Huawei and ZTE are notorious in this sphere. China also purchases companies dealing with computer network with this intention. The Chinese company Lenovo, which bought IBM' PC business in 2004, was reportedly shipping laptops with 'superfish' malware which undermines basic security protocols. The threat from imported equipment would significantly increase if we continue to rely on imported equipment for the 5G network as well as that may have back door surveillance system based on Artificial Intelligence.

## India's IWIO Strategy

### Beware, Veterans,

Immediately after retirement, many Veterans get hooked onto social media. They have years of experience and in the know of a lot of sensitive military information. Most have close friends and juniors in active service with whom they converse routinely. Many of them write detailed articles on strategy and tactical appreciation. There are others on panel discussions in seminars or television. Adversaries use social media platforms to extract information and to mould opinions. There is also a tendency among some to forward messages on group messaging Apps without checking authenticity or implications. There is thus a need for Veterans to think twice. Beware that India's enemies want to use Veterans to extract service-

related information and to spread discontent among serving personnel.

## Way Ahead India

India is gradually realising the significance of IWIO but a lot needs to be done in this field. India established the National Information Board (NIB) in 2002 and is chaired by National Security Adviser. The NIB is the highest policy-making body for cybersecurity and IW and periodically reports to the Cabinet Committee on Security headed by the Prime Minister. The Indian armed forces are also represented in it. However, the NIB's capabilities for countering IWIO needs to be enhanced significantly. An independent national fact-checking organisation must be established for transparently checking facts and also to formulate a code of principles for fact-checking. There is an urgent need for making citizens aware of the misuse of social media platform to exploit our fault lines and cultural differences. India must find indigenous telecom solutions and equipment to ensure its safety. An effective system of providing incentives to Indian telecom entrepreneurs should be established. India needs to devise time-sensitive rapid government response to adversary IWIO campaigns. The NIB must engage best professionals in the field to counter IWIO. The government needs to work closely with all social platforms and electronic and print media to counter IWIO. There is a need to make citizens and security personnel aware of the misuse of social media platforms and also include this subject in the educational institutes. The industry and academia should be involved in research, with appropriate incentives.

The newly formed tri-service Defence Cyber Agency (DCA) will work in conjunction with the National Cyber Security Advisor. Its focus will be towards offensive and defensive military cyber-issues. It would include as many as 1000 personnel from the Army, Navy and the Air Force. The National Cyber Security Policy was adopted by the Government of India in 2013 to ensure secure and resilient cyberspace for citizens, businesses and the government. DCA is meant to combat the current threat from China and Pakistan. The Agency will have smaller teams, spread around the country. It will position dedicated officers in major headquarters of the forces to deal with emerging cybersecurity issues. DCA must find indigenous solutions and equipment.

## *References:*


1 *SD Pradhan, Balakot and after Pakistan intensifies information war against India, Chanakya code, Times of India, March 12, 2019, https://timesofindia.indiatimes.com/blogs/ChanakyaCode/balakot-and-after-pakistan-intensifies-information-war-against-india/*

2 *James Andrew Lewis, Cognitive Effect and State Conflict in Cyberspace, CSIS, September 26, 2018 https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace*

3 *Amit Sharma, Cyber Wars: A Paradigm Shift from Means to Ends, Institute for System Studies and Analysis (I.S.S.A), DRDO, October, 2018 https://ccdcoe.org/uploads/2018/10/00_VirtualBattlefield.pdf*

4 *Taylor C Boas, University of California, Berkeley, Weaving the Authoritarian Web: The Control of Internet Use in Nondemocratic Regimes http://people.bu.edu/tboas/authoritarianweb.pdf*

5 *Brainy Quote, Sun Tzu, https://www.brainyquote.com/quotes/sun_tzu_383158*

6 *Roger C. Molander, Andrew Riddle, Peter A. Wilson, Strategic Information Warfare - A New Face of War. Rand Corporation, https://www.rand.org/pubs/monograph_reports/MR661.html*

7 *SD Pradahan, Chanakya Code, ToI Blog, November 3, 2016 https://timesofindia.indiatimes.com/blogs/ChanakyaCode/developing-responses-to-increasing-challenges-of-information-warfare-and-influence-operations/*

8 *Elsa B Kania, Chinese Military Innovation in Artificial Intelligence, Center for New American security, June 07, 2019. https://www.uscc.gov/sites/default/filesJune%207%20Hearing_Panel%201_Elsa%20Kania_Chinese%20Military%20Innovation%20in%20Artificial%20Intelligence.pdf*

9 *Petros Wallden, Elham Kashefi, Cyber Security in the Quantum Era, Wallace Web Design, April 20119, https://wallacewebdesign.com/cybersecurity/2019/8/cyber-security-in-the-quantum-era*

10 *Stephane Duguin, Cybercriminals thrive off big data - this is how to catch them, World Economic Forum, October 28, 2019 https://www.weforum.org/agenda/2019/10/cybercrime-deepfakes-law-enforcement/*

11 *Cannings Purple, What is 'doxxing' and what do we have to worry about? March 25, 2019 https://www.lexology.com/library/detail.aspx?g=5244a646-eb7c-4791-b672-055b822a01e2*

12 *Brainy Quotes https://www.brainyquote.com/quotes/daniel_patrick_moynihan_182347*

13 *Tal Samuel-Azran, Al-Jazeera, Qatar, and New Tactics in State-Sponsored Media Diplomacy, September 2013, https://www.researchgate.net/publication/258122794_AlJazeera_Qatar_and_ New_Tactics_in_State-Sponsored_Media_Diplomacy*

14 *Nicholas D. Kristof , China's Greatest Dissident Writer: Dead but Still Dangerous, Book Review, August 19, 1990, https://archive.nytimes.com/www.nytimes.com/books/97/05/11/reviews/21513.html*

15 *Samantha Bradshaw, University of Oxford, and Philip N. Howard, University of Oxford. Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation, 2017, http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf*

16 *Lawfare Blog, Developing Responses to Cyber-Enabled Information Warfare and Influence Operations, Sept 10,2018, https://brica.de/alerts/alert/public/1228601/developing-responses-to-cyber-enabled-information-warfare-and-influence-operations/*

17 *Ibid.*

18 *Donald W, Poynter, International Fact Checking Network, Accountable Journalism, Raynold's Journalism Institute, https://accountablejournalism.org/ethics-codes/international-fact-checking-network-fact-checkers-code-of-principles*

19 *James Andrew Lewis, Cognitive Effect and State Conflict in Cyberspace, CSIS, September 26, 2018 https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace*

20 *Elizabeth Flock, Washington Post, Operation Cupcake: MI6 replaces al-Qaeda bomb-making instructions with cupcake recipes, June 03, 2011, https://www.washingtonpost.com/blogs/blogpost/post/operation-cupcake-mi6-replaces-al-qaeda-bomb-making-instructions-with-cupcake-recipes/2011/06/03/AGFUP2HH_blog.html*

21 *Mark Clayton, The Christian Science Monitor June 17, 2014, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers*

22 *Gordon Corera, BBC News, How France's TV5 was almost destroyed by 'Russian hackers', October 10, 2016 https://www.bbc.com/news/technology-37590375*

23 *U.S. Cyber Command History https://www.cybercom.mil/About/History/*

24 *Daniel Cohen & Ofir Bar'el, The Use of Cyberwarfare in Influence Operations, October 2017, https://icrc.m.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/Cyber_Cohen_Barel_ENG.pdf*

25 *MOLLY K. MCKEW, The Gerasimov Doctrine, September 2017, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538*

26 *Amos Harel, Israeli Army Sets Up 'Consciousness Ops' Unit to Influence Enemy Armies, Foreign Media and Public Opinion, Mar 10, 2018, https://www.haaretz.com/israel-news/with-eye-on-hearts-and-minds-israeli-army-sets-up-consciousness-ops-1.5888362*

27 *Weishan Niao, Wei Lai, The Cyberspace Administration of China, https://www.researchgate.net/publication/311505481_Policy_review_The_Cyberspace_Administration_of_China*

28 *Josh Kramer for NPR, How The U.S. Hacked ISIS, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis*

29 *Sudhi Ranjan Sen, Hindustan Times, Cyber attacks becoming more frequent in India, November 93, 2018, https://www.hindustantimes.com/india-news/cyber-attacks-becoming-more-frequent-in-india/story-8Os6AtCrHzL6QCBinVQuSM.html*

◆◆◆