Seminar Report

THE IMPACT OF PERSONAL CYBER SECURITY ON ORGANISATIONAL SECURITY

April 28, 2018

Centre for Land Warfare Studies
New Delhi

KNOWLEDGE WORLD
KW Publishers Pvt Ltd
New Delhi

Seminar Co-ordinators: Col Debashish Bose and Col Subhasis Das

Rapporteurs: Harsh Kumar Upadhayay and Kanchana Ramanujam

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Phone: +91.11.25691308 Fax: +91.11.25692347
email: landwarfare@gmail.com • website: www.claws.in
CLAWS Army No. 33098

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent think tank dealing with contemporary issues of national security and sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

The views expressed in this report are sole responsibility of the speaker(s) and do not necessarily reflect the views of the Government of India, or Integrated Headquarters of MoD (Army), or the Centre for Land Warfare Studies.

The content may be reproduced by giving due credited to the speaker(s) and the Centre for Land Warfare Studies, New Delhi.

Printed in India by

KNOWLEDGE WORLD
KW Publishers Pvt Ltd
4676/21, First Floor, Ansari Road, Daryaganj, New Delhi 110002
Phone: +91.11.23263498 / 43528107
email: kw@kwpub.com • website: www.kwpub.com

CONTENTS

EXECUTIVE SUMMARY

- There are increasing instances of cyber security breaches caused by vulnerabilities introduced by ‘the man in the system’ or the soft underbelly of networks.

- The term ‘personal cyberspace’ is a fallacy in the modern connected world.

- As users of the global common digital space, every user has a stake in the security of data. Every netizen is a target and hence, has a role to play in the fight.

- Organisational advisories and measures can help to some extent in securing data and assets, but what is critical is intimate personal scrutiny and knowledge.

- In the battle to secure cyberspace, there is a role for government agencies, cyber militia, academia, hackers, industry and every netizen. Synergy will remain the key aspect in achieving success.

- The activities that one carries out on the internet leaves a trail which can be used to monitor, carry out surveillance or manipulate, which in turn can directly or indirectly harm the organisation(s) one works for.

- The major challenge which is faced by the military cyber-based systems is the endpoint security between the man and the machine.

- Human vulnerabilities can violate even the most robust technical solutions. A reactive approach to cyber security incidents can never result in an infallible solution.

- Personal and official digital identity is enmeshed in cyberspace today. Hence, a minor infringement at personal or organisational level could have serious security implications.

- There is a need to invest time, money and resources to continuously and diligently build the organisation with multifaceted cyber capability and skills.

- The galloping success of social media is essentially driven by economics and the human psychology of sharing. This, in turn, increases cyber threats and attacks driven by social media, which is emerging as a significant threat vector.

- Attacks from social media can be reduced by 'common sense' measures, including sharing of minimal personal information, review of privacy settings, use of discretion while sharing pictures and videos, avoiding opinions on controversial matters and on matters of security.

- The confluence of the Dark Web (a place where anonymity is guaranteed) and virtual currency (a perfectly anonymous currency for transactions) fuels an ideal ecosystem for illegal activities.

- Bitcoin is losing favour among cybercriminals and terrorists and is being replaced by new currencies, such as Monero, Zcash and Ethereum, which provide better privacy. This is creating fresh challenges to national and organisational security.

- Traditional methods of in-house monitoring and surveillance are not designed adequately to detect breaches in the cyber domain. Hence, there is a pertinent need to address cybers ecurity holistically as a combination of technical, human and procedural means.

DETAILED REPORT

A Seminar on 'The Impact of Personal Cyber Security on Organisational Security' was conducted on April 28, 2018, at the Manekshaw Centre, Delhi Cantonment.

Aim

The seminar was aimed at exploring the components and extent of personal cyberspace and utilise this understanding to accurately visualise its impact on organisational security with a special emphasis on information security. The seminar was also aimed at exploring means to ensure that information risks are managed to a level that is acceptable to the organisation and security incidents are dealt with effectively as and when they do happen.

Modalities of Conduct

A one day seminar was conducted at Taber Hall, Manekshaw Centre, Delhi Cantonment on April 28, 2018. The participants were from different government departments and agencies, the three services, strategic community, veterans, industry, research and development organisations, ICT and academia. Nominated army officers from field formations also participated in the seminar.

Speakers

- Lt Gen Ranbir Singh, AVSM**, YSM, SM, Deputy Chief of Army Staff (DCOAS) Information Systems and Training (IS&T)
- Lt Gen S P Kochhar, AVSM**, SM, VSM (Retd), Former Signal Officer in Chief (SO-in-C), Chief executive officer (CEO) Telecom Sector Skill Council
- Mr Dinesh O Bareja, Chief operating officer (COO) Open Security Alliance, India Watch
- Mr Dominic Karunesudas, Director, Information Sharing and Analysis Center

- Shri Amit Sharma, Additional Director, Office of Scientific Advisor to Raksha Mantri (SA to RM), Defence Research and Development Organisation (DRDO)

Inaugural Session

While setting the tone of deliberations to follow, the Director Centre for Land Warfare Studies(CLAWS) indicated that the in the cyber domain, even minor mistakes at the individual level can have a comparatively devastating effect on the overall war effort. Every stakeholder has a stake in the security of the system and the organisation. Hence, there is a pertinent need to recognise the vulnerability introduced by the human factor in our future approach to cyber security.

The keynote speaker asserted that the armed forces across the world have traditionally been proactive and systematic in securing their cyber assets. In the Indian Army, assets such as the army-owned networks, information technology infrastructure, data centres, and so forth, are routinely secured using the best of cyber defence technologies. However, what is emerging by the day is the vulnerability introduced by 'the man in the system' or the soft underbelly of our networks. There have been some unfortunate instances in the past, where a compromise in the organisational security has been affected due to poor cyber hygiene, knowledge and training of armed forces personnel. The speaker reiterated that the revelations of Christopher Wylie in 2018, have exposed the fallacy of the term 'personal cyberspace'. The Cambridge Analytica episode has shown that in the ubiquitous, all-pervasive information space, it is indeed a thin line between the hunter and the hunted. What comes across alarmingly is that the agencies or people, who are now in the dock, were never on the wrong side of the law in the very first place. The agencies being questioned were perfectly legitimate entities, funded by government or public monies with large-scale operations. These agencies were not operating from dark, dingy, underground quarters with computer screens eerily glowing in the dark, but from swanky offices located in costly business districts. The revelations also signalled the emergence of an entirely new dimension of warfare, where actors can allegedly influence the minds of the electorate of another nation.

The world had witnessed twin ransomware attacks of unprecedented proportions in 2017. Both 'Wanna Cry' and 'Petya' exposed the alarming interconnect between the government agencies, software companies, hackers, anonymous groups like the 'shadow brokers,' digital currency and the internet community. Interestingly, the tools used in the attack were initially intended for use in national security by the United States of America, by legitimate government agencies and fully supported by legislation. In spite of the scale of the attack, there has been no clear attribution or accountability till date, and there is likely to be none in the future. The speaker also pointed out that there is a need to delve into the diminishing boundary between the cyber security professional and the common man or the common soldier. As users of the global common digital space, every user has a stake in the security of data. It would be naïve to shift the complete onus of the cyber security of an organisation to a handful of professionals handling the networks. Every soldier is a target and hence, has a role to play in the fight.

The aspect of data security in the age of social media is a grey zone. What Facebook gave away to a respected University of Cambridge researcher and to other legitimate app creators, was information which was handed over voluntarily by the users of the ecosystem, people like you and me. Individually, the pieces of information could be seen as innocuous and minor; however, when seen in the larger context of 87 million users and their alleged effect on elections, the effect is entirely different. We as soldiers are active users of social media platforms, hence our activities need to be well thought out and deliberated. Organisational advisories and measures can help to some extent, but what is critical is intimate personal scrutiny and knowledge. It is in this challenging background that critical national resources and assets, which have a cyber-footprint have to be correctly identified and protected by designated agencies and the personnel within. There can be no compromise in securing such assets since any disruption in such critical infrastructure can even affect the national morale and war effort. The armed forces are just a small part of the concerted national effort. There is a role for government agencies, cyber militia, academia, hackers, industry and every citizen, who is a part of digital cyberspace, towards this. Synergy will remain the key aspect in achieving success.

Theme 1: Personal Cyber Securityand Organisational Security

In the modern era, the internet has become a huge facilitator of our daily lives. Digital citizens may access it for information, accessing bank accounts, sending mails, purchases or for accessing social media. Accessing the internet in a personal capacity brings us to the realm of personal cyberspace. The activities that we carry out on the internet leave a trail which can be used to monitor, carry out surveillance or manipulate, which in turn can directly or indirectly harm the organisation(s) we work for. The key aspects that we were covered as a part of this theme are listed below:

- Online privacy versus national security.
- Online identity and the viability of multiple digital identities as a means to de-risk.
- Tailoring a personal threat model for sensitive appointments.
- Developing a separate authentication protocol for sensitive appointment holders for use during emergencies.
- Keeping personal and organisational data separate.
- Impact of personal cyber security as parents of young children, particularly teenagers.
- Personal cyber security versus convenience.
- Encryption-best practices both for storage and browsing.
- Education and training.

The session chair brought out that cyber security in the modern context needs to be tackled as a judicious mix of outcomes and processes. The outcomes desired from the security system need to be treated as business cases and not technical cases. Hence, in the militaries, this aspect should invariably be the domain of the general staff. The decision on the processes, on the other hand, is a technical case and can be handled by sufficiently qualified technical personnel.There could be be certain occasions where a shortage of in-house expertise may necessitate the amalgamation of expert non-military personnel into the decision-making team. While deciding on the outcomes and the processes, the key aspect is the knowledge of the stakeholders. This can be acquired by studying and interaction with the industry through organised forums. Interaction with sales and marketing teams alone may derail the entire initiative since the inputs could tend to be biased.

A challenge which is faced by military cyber-based systems is the endpoint security between the man and the machine. While machine-to-machine interactions are secure, there is a need to overhaul the man to machine interface. The authentication device (key, dongle, card) can now be carried by any individual; however, the machine cannot identify the imposter. The machine authenticates the device and not the man, which is the key to arrest human-related breaches. Biometrics as a solution to detect a black hat is costly and difficult to implement in all the systems. Hence, there is a need for evolving out-of-the-box and innovative solutions. The speaker gave an example of a smartcard used for authentication, where, in addition to other security features, a series of personal questions could be fed in and the authentication process could generate random questions and seek answers from the user. This could add a layer above the machine-level authentication, that of the human authentication. The issue could be viewed from a different context. There is a problem in military establishments where a few individuals carry mobile phones and other unauthorised transmitting devices to secure zones, inspite of orders on the subject. In such scenarios, human frailties can be countered using technical solutions in addition to physical means. Hence, the solution lies in a judicious mix of innovative technical and process-driven solutions.

In April 2018, a bitcoin exchange in New Delhi lost bitcoins worth Rs. 20 crore after most of its wallets were hacked. The entire cryptocurrency ecosystem sells itself on the robust blockchain technology, which claims better online security standards than the traditional methods. During the investigation, it was found that the wallet private keys that should have been kept in safe custody and never connected to an online system, were made online for more than 12 hours. Unknown actors used these private keys to transfer the bitcoins and also wipe out all traces of the transactions. The investigations have pointed to the role of an insider in the loss. The incident proves that human vulnerabilities can violate even the most robust technical solutions. A reactive approach to cyber security incidents can never be an elegant solution. Proactive solutions based on data analysis and artificial intelligence are available, however, the adoption in the armed forces should be deliberate and cautious. The relevance of personnel education and training in the planning, implementation and the user stages is critical.

The Human Link is the Weakest Link

The speaker introduced the house to twin instances where personal data was lost in big numbers in 2014–15. The first related to the US Office of Personal Management where 21 million records of US Service personnel including background data, social security numbers and personal identity were lost. The second incident was the loss of 32 million records from the database of Ashley Madison, a Canadian web platform dealing with dating and social networking services targeted at already married people. When seen in an isolated manner, these incidents could be seen as unrelated and innocuous. However, what emerged later was that the compromised databases had common data points and around 10,000 US service personnel had their accounts on the Ashley Madison platform. This was lost to hackers including official ids and credit card information. The incident pointed to the enmeshed nature of personal and official digital identity in cyberspace today. Hence, a minor infringement at the personal or organisational level could have serious security implications. Current cyber security paradigms overlook the fact that the human is the weakest element in the chain. The training and education of the human link is disregarded and often gets swept away during a cost-cutting exercise. Marketing personnel selling a security solution find it easy to advertise technological solutions as they can be easy to visualise and comprehend. Inspite of organisations being fully aware of the problem, the human element is unfortunately not given its due importance.

Fixing this weakest link is, however, not easy. There is a need to invest time, money and resources to continuously and diligently build the organisation with multifaceted cyber capability and skills. Skills on how to operate a computer, good values and morals of computer usage, healthy computing and the shades of grey between life and computer crime are pertinent in the current context. There is a unique blend required in a cyber security trainer. He/she should be a technical expert, think like a hacker and also impart ethical skills. The Indian Armed Forces pride themselves for having professional training institutions for all levels of personnel. There is a case in point to include cyber hygiene as a part of the curriculum for all courses. Inclusion of cyber hygiene could start from school with localised content and in local languages. It should invariably be a part of all college education, irrespective of the streams of study. Computer security and hygiene cannot be an ‘elective’ module any longer. Continuous user sensitisation about the risks and the shared stakeholder approach is the way forward.

Theme 2: Personal Cyber Security and Social Media

Social media has become one of the main pillars of modern day livelihood. These platforms have become so ubiquitous that all services and utilities including government services are being linked to social media accounts. The aspects that were deliberated during the seminar are as follows:

- Understanding ‘sharing’ in social media.
- Common risks, including anonymous accounts.
- Social media and social engineering.
- Impact of personally identifiable information on social media.
- Privacy settings and default security settings.
- Social networking etiquettes.

Threats from Social Media: the Human Angle

The speaker brought out that India figures prominently among countries with the maximum users of popular social media platforms. As per Symantec Corporation, India also stands at third position after China and the United States of America, as the leading source of malicious code and cybercrime. The galloping success of social media is essentially driven by economics and the human psychology of sharing. This, in turn, increases cyber threats and attacks driven by social media, which is emerging as the most significant threat vector. A few social media threats could be identified as malware distribution, social engineering, cyber harassment, stalking, sextortion, violation of privacy, loss of brand reputation and cyberchondria, and so on. The use of social engineering against personnel of the security agencies has been on the rise due to its low technology threshold and the gullibility as well as lack of awareness among the personnel. The use of bots in social media is emerging as a major threat area and can lead to spear phishing and can even sway public opinion. The shelf life of even the most innocuous and innocent post on social media is infinite, hence there is a requirement of diligence. Indiscreet information can adversely affect college admissions, employment, insurance, and so forth. Employers, insurers, college admissions officers, financiers are already screening applicants using intelligence provided by firms which use open source information. Information pertaining to buying behaviours, geospatial and location information, social media and internet usage, and so forth, has been digitised, formatted, standardised, analysed, modelled and is up for sale. It may seem intrusive and intimidating to the individual, however, it is a great opportunity for businesses to use this data, essentially generated by users on social media.

Security in the social media space is completely individual driven. It consists of 'common sense' measures, including sharing of minimal personal information, reviewing privacy settings, using discretion while sharing pictures and videos, sharing opinions on controversial matters, avoiding adverse comments on coworkers, fellow students and on matters of security. The access provided to children on social media is a challenge and needs to be monitored/regulated.

Theme 3: Personal Cyber Security and Common Attack Vectors

It is fascinating to understand how hackers and threat actors use personal information to attack an individual and his/her organisation. The threat vectors such as darknet and the cryptocurrency ecosystem offer immense challenges to the national security. Some of the areas of scrutiny which were analysed during the seminar are as follows:

- Mobile device security.
- Sniffing around unsecure Wi-Fi connections.
- Swiping a flash drive.
- Unpatched vulnerabilities in software.

- Impact of internet of things - security with special emphasis on wearables and medical devices.
- Information security and bring your own device concept in the Army context.
- Multifactor authentication-necessity and benefits.

Darknet and Virtual Currencies: Impact on National Security

The speaker brought out that only about 0.03 percent of the web pages on the internet are accessible through common search engines. The balance 99.97 percent of the web, which can be accessed using specialist tools which guarantee anonymity, is a major challenge for law enforcement agencies. The mainstreaming of virtual currencies and the possible access to the darknet through social media brings to focus the relevance of personal cyber habits and actions. It would be pertinent to draw out the distinction between the deep Web and the dark Web, which are at times erroneously referred to in the same context. The deep Web essentially consists of academic information, medical and legal records, multilingual databases, government resources, and so forth. The darknet (dark Web), on the other hand, is an anonymising network where connections are made only between trusted peers sometimes called 'friend-to-friend' (F2F) using non-standard protocols and ports. The regions beyond the deep Web are also referred to as the Charter web and the Mariana's web. Julian Assange and other top-level WikiLeaks members are believed to have access to the deepest levels of the Mariana Web. Many users are increasingly drawn towards the deep and dark Web due to inquisitiveness and the easy and free access to the TOR environment. The TOR browser relies on encryption at the application layer making it simpler to use. Consumers are also being directed to the dark Web through mobile applications, social media, websites, paid search engines and e-mail. There are a large number of dark Web marketplaces such as Abraxas, Agora, Middle Earth, Nucleus and the Silk Road 1, 2 and 3.

Virtual currencies are the lifeblood of the darknet. A virtual currency is not issued or guaranteed by any jurisdiction and fulfils the functions of value, trade and exchange only by agreement within the community of users of the virtual currency. Some virtual currencies such as bitcoin are convertible and have an equivalent value in terms of real-world currencies, while others are nonconvertible and intended only for use in the virtual domain. A kind of virtual currency is the cryptocurrency, in which encryption techniques (cryptography) are used to regulate the generation of units of currency and verify the transfer of funds. The first cryptocurrency to be created was bitcoin, back in 2009. Today, there are hundreds of other cryptocurrencies, often referred to as altcoins. The blockchain technology, which was developed to create bitcoins, has seen a gradual evolution that can be broken down into three categories. Blockchain 1.0 is currency and includes the deployment of cryptocurrencies in applications related to cash, such as currency transfer, remittance and digital payment systems. Blockchain 2.0 involves contracts and the entire slate of economic, market and financial applications that are more extensive than simple cash transactions. It facilitates contracts in stocks, bonds, futures, loans, mortgages, titles, smart property and smart contracts. Blockchain 3.0 includes blockchain applications beyond currency, finance and markets, which functions in the areas of government, health, science, literacy, culture and art.

The confluence of the dark Web(a place where anonymity is guaranteed) and virtual currency(a perfectly anonymous currency for transactions) fuels an ideal ecosystem for illegal activities. It includes money laundering, weapon sales, drug mafia, terrorist activity, trafficking and hit for hire. Cryptocurrencies and associated technologies hold great promise for low-cost, high-speed, verified transactions that can unite counterparties around the world. For this reason, they could appear appealing to terrorist groups. Terrorists in the Gaza Strip have been known to use cryptocurrencies to fund operations. Islamic State of Iraqand Syria members and supporters have been particularly receptive to the new technology, with recorded uses in Indonesia and the United States. Fund raising, recruitment and weapon-making classes are facilitated using these currencies. The speaker also analysed a few case studies such as the case of Ali Shukri Amin, a Virginia teenager. Amin was convicted for conspiring to provide material support and resources to the Islamic State(IS).He used Twitter to provide instructions on how to use bitcoin to mask funds being sent to the IS and to establish a secure donation system that would help facilitate the travel of supporters and foreign terrorist fighters (FTFs) to conflict areas. Although Amin was unsuccessful in his efforts to raise funds for the IS, the incident demonstrated how terrorist groups are actively exploring new ways to obtain funds and the integration of cryptocurrency for use in operations, funding of FTFs and the widespread reach of information through social media outlets. Over the years, bitcoin monitoring tools have been developed and are being used by law-enforcement agencies. Bitcoin is losing favour among cyber criminals and terrorists due to its weak privacy. New currencies such as Monero, Zcash and Ethereum provide better privacy and are increasingly being used by criminals. This is creating fresh challenges for national and organisational security.

Conclusion

In the Armed Forces, organisational security remains a key area of concern. Any leak of data or information in the cyber domain has an impact on multiple other domains, such as the social, economic and physical domains. There is a need to address the challenges in multiple fronts, of which personal cyber hygiene is a critical component. Individual failures, which can lead to a loss of data or compromise of confidential information, can be extremely difficult to detect in a large and diverse organisation such as the Armed Forces, especially since sensitive information is accessible to many members. Deliberate acts of subversion from within the organisation cannot be ruled out, which exacerbates the problem. Traditional methods of in-house monitoring and surveillance are not currently designed to detect these breaches in the cyber domain. Hence, there is a pertinent need to address cyber security holistically as a combination of technical, human and procedural means.

PROGRAMME

0930–1000h	Registration and Tea
1000–1005h	Welcome Remarks:Lt Gen B SNagal, PVSM, AVSM, SM (Retd), Director CLAWS
1005–1025h	Keynote Address: Lt Gen Ranbir Singh, AVSM**, YSM, SM, DCOAS (IS&T)
1025–1040h	Opening Remarks by the Chair: Lt Gen S P Kochhar, AVSM**, SM, VSM (Retd), Former SO-in-C, CEO Telecom Sector Skill Council
1040–1100h	Personal Cyber security versus Organisational Security: Mr. Dinesh O Bareja, COO Open Security Alliance, India Watch
1100–1140h	Questions and Answers
1140–1200h	Tea
1200–1230h	Personal Cyber security and Social Media—Mr. Dominic Karunesudas, Director Information Sharing and Analysis Center
1230–1300h	Darknet, Cyptocurrency and Other Attack Vectors: Impact on National Security—Shri Amit Sharma, Additional Director, Office of SA to RM, DRDO
1300–1345h	Questions and Answers and Closing Remarks
1345–1435h	Lunch and Dispersal