CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 151 September 2018

Cryptography in the 21st century: Advances in Encryption Technology

Kritika Roy is currently a Web Manager cum Researcher at the Centre for Land Warfare Studies (CLAWS). She is an engineering graduate (Electronics and Communication) and holds a master's degree in Geopolitics and International Relations.

In the 21st century, advances in technology have brought into focus the need to have double assurance on data security. With the world moving from classical computing to Quantum Computing, the latter has the power to unlock the toughest of cyber-locks. Most of the states today focus on protecting their critical data as it is directly linked to their national security dynamics. This particular aspect becomes important considering the technologies such as the Internet of Things and Cloud Computing gaining traction in the international system. There is no denying the fact that the world truly is going online from businesses to services, to a myriad of operations all available just a click away. In this context, protection of data is pertinent especially with the surge in data theft, cyber espionage and the fear of more advanced technology, making the current protection matrix redundant.

Information has always been considered as a crucial element that can give a strategic advantage over an adversary. Even during the ancient times, the kings and generals took great care to protect their trade secrets, military secrets and other critical information from adversaries.

Key Points

1. Information has always been considered as a crucial element that can give strategic advantage over an adversary. Thus, protection of data is pertinent especially with the surge in data theft, cyber espionage and the fear of more advanced technology making the current protection matrix redundant.
2. Quantum computers are those systems that would have the capacity to do complex tasks in split seconds; this could also include breaking of the conventional encryption locks.
3. With the world moving from classical to Quantum Computing, data protection would be a challenging task. Most of the states today focus on protecting their critical data as it is directly linked to their national security dynamics.
4. Traditional encryption does not guarantee a foolproof security of the system. Generally, the length of the key determines the possible number of permutations and combinations that can be attempted in order to break the code.
5. India's move towards digitalisation and the initiative to develop smart cities, protection of data has become paramount. Thus, the country needs to take cognisance of emerging technologies such as the Quantum computing and Quantum encryption and develop indigenous capabilities in these areas.

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

Website: www.claws.in Contact us: landwarfare@gmail.com

Cryptography in the 21st century ...

The protection of information was achieved by different techniques such as masking or replacing the letters of the original data with substituted letters or pictures that had certain links or clues in some way or another to the original text. This means hiding the original data to protect it from adversaries and then reconverting the original data by the intended recipient has been termed as cryptology.

The word 'cryptography' has been derived from two Greek words called *kryptós* meaning hidden secret and *graphein* meaning to write. Thus, cryptography can be defined as, *the science or study of techniques of secret writing and message hiding*. The major impetus for protecting the data is to facilitate secure communication between two parties. Cryptography encapsulates two major techniques of encoding data, namely 'encryption' and decoding a data known as 'decryption'. With the advances in Information and Communication Technology (ICT), the means and methods of data transfer have changed. This, in turn, has also changed the ways of securing data communication. In the current scenario, modern cryptology exists at the intersection of the disciplines of physics, mathematics, communication science and computer science.

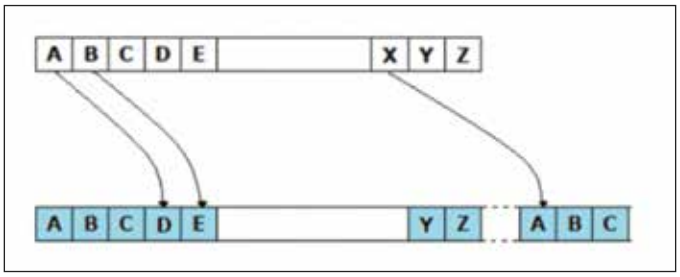
In this context, India has also been moving forward and trying to gain a specific advantage in the field of encryption. The idea has been to protect and secure the data and communication networks so as to prevent it from being misused by the hostile forces. This becomes extremely important, considering the hostile neighbours India has in its backyard that are inimical to its interest.

The paper would provide a comprehensive understanding of cryptography in general and encryption in particular. Over the years, the means and methods of cryptography have also evolved to cater to the needs of Information Age. In this context, the paper would assess the new forms of encryption and its relevance for national security. And lastly,the research also examines India's position and the future trajectory of encryption.

Cryptography: A Brief History

One of the earliest signs of cryptography was found in ancient Egypt on the Tomb of Khnumhotep II. The script used was called 'hieroglyphic symbols', that is, basically a pictographic representation of characters.[1] In 100 BC, during the era of Julius Caesar, a substitution cipher was used to convey secret messages to the army personnel on war fronts. Substitution cipher was simply a means of substituting a character with another and doing the same for other characters while following a singular logic or pattern as shown in Figure 1.[2]

Figure 1: Caesar Cipher



Source: "A Brief History of Cryptography," RedHat Publication, 14 August 2013, see website https://access.redhat.com/blogs/766093/posts/1976023.

These techniques were more concerned with the security of the system rather than the protection of the key. This became the major limitation of the system, that is, once the system is known, the message could easily be intercepted. Thus, there was a dire need to have a more foolproof system.

During the 16th century, another means of encoding data came to the forefront wherein a key was developed and used numerous times spanning the entire message, and then the ciphertext was produced by adding the character of the message with the character of the key using modulus function. Though this concept was not able to get much success, it nevertheless brought in the concept of encryption 'key'.

Over the years more variety of mechanical cryptography came in to the picture. However, a major breakthrough came with the introduction of electricity. Consequently, electromechanicals

techniques were employed to secure messages. The initial of these was 'Hebern Rotor Machine'. It was a single rotor, in which the key was embedded in a rotating disc. The key was used to encrypt a table that was already substituted. The output of each key press was a ciphertext. The key press also rotated the disc by a single notch; therefore, a single table was used for the next plain text. This means of encryption and decryption was broken by using letter frequencies. This technique was succeeded by the Enigma machine. German engineer Arthur Scherbius is credited with the invention of the Enigma machine at the end of World War II. The machine had inbuilt rotors which rotated at different rates whenever the words were typed on the keyboard, which subsequently produced an output appropriate letters of ciphertext. In the later parts, even the Enigma coding was broken by a Polish. This was followed by a British cryptographer improvising on the Enigma machine. By the end of the World War, cryptography also found other applications like securing trade secrets and other commercial applications.

Until the late 20th century, strong cryptography was the preserve of government agencies and the military. However, with the advent of fast modern computers, cryptography with a 'military' level of security is now available to the masses as well. The major idea behind using cryptography has been to ensure the following feature on the message being sent:

Features of Cryptography

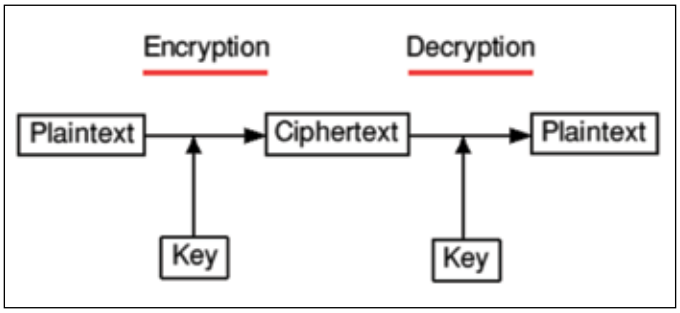
- Confidentiality: The state of keeping a message secret or private.
- Non-repudiation: The ability to ensure that a party to a contractor a communication cannot deny the authenticity of their signature on the sending of a message that they originated.
- Authentication: The process of ensuring the data to be true and valid.
- Integrity: The characteristic feature of the message being worthy of trust.

With the advances in ICT technologies, cryptography also evolved to become more sophisticated, secure and difficult to crack. The growing interconnectivity and interdependency in the ICT age has provided easy access to information from anywhere at any given time. However, this ease of accessibility has also brought in its wake the proliferation of high-profile data breaches, subsequently elevating the need to have far more advanced and foolproof encryption systems to secure confidential data. While good Information Technology (IT) security strategies can be effective in protecting networks, it is still a Herculean task to account for the huge volume of data transiting among mobile devices, browsers, databases and the cloud.

Encryption

Encryption is a specific means of cryptography used to hide data by converting it into an unreadable form. To convert it back into decipherable form, a key is required that is possessed by a dedicated recipient. To better understand the modern-day encryption, it is important to understand the basic process of cryptography as shown in Figure 2.

Figure 2: The General Process of Cryptography



Source: Nat Queen, "Modern Cryptography, "*Acorn User, n. 265*, http://www.queen.clara.net/pgp/AU265.html)

As illustrated in Figure 2, the original data or message is known as plain text that is encrypted to produce the ciphertext. The reverse process is known as decryption. The process of encryption or decryption may employ a number of algorithms, varying from using a complex logarithmic function to factorials or a mix and match of several mathematical operations which is known as cipher. A cipher generally has a set of well-defined steps that can be followed to encrypt and decrypt messages.

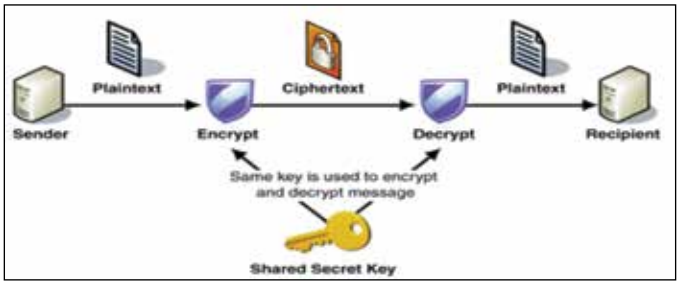
The operation of cipher is largely determined by the use of key. 'Key' here is basically a set of pseudorandom numbers or strings that is used to encrypt a text or decrypt a ciphertext. Many encryption systems also carry out several layers of encryption, that is, the ciphertext output of a particular message again becomes input to another encryption layer. This ensures a strong security of the message. There are two types of encryption which are described below

Symmetric Key Encryption

This type of encryption is also known as shared secret encryption. This form of encryption cipher is any algorithm in which the 'key for encryption is related to the key for decryption' as shown in Figure 3. This process could be considered analogous to a mechanical lock where the same key can be used to lock and unlock it.[3] The major drawback of this form of encryption is that it utilises the same key. Therefore, keeping the key secure is pertinent. Symmetric key encryption is generally used for bulk encryption of data like documents.

There are numerous algorithms that use symmetric key encryption, for instance, stream cipher, where a 'stream of random or pseudorandom numbers are combined with the original message'.[4] The processing is majorly carried out bit by bit as in a chain. A different or unique key is used to encrypt each of the bits and the key is often combined with an initialisation vector. This form of encryption is considered simple and faster. One-Time Pad, RC4, Linear Congruential and so forth, all are prominent examples of stream ciphers. Another means of symmetric key encryption is a block cipher that involves processing or encoding of the plain text as a fixed length block one by one. A block could be either of 64 bits or 128 bits in size. The same key is used to encrypt each of the blocks. This is usually more complex and slower in operation. Nevertheless, due to its inherent complexity, block cipher is often considered more secure. For example, Lucifer, RC5, Blowfish, and Advanced Encrypted Standard: Encryption standard adopted by the US government and Data Encrypted Standard.

Figure 3: Symmetric Key Encryption

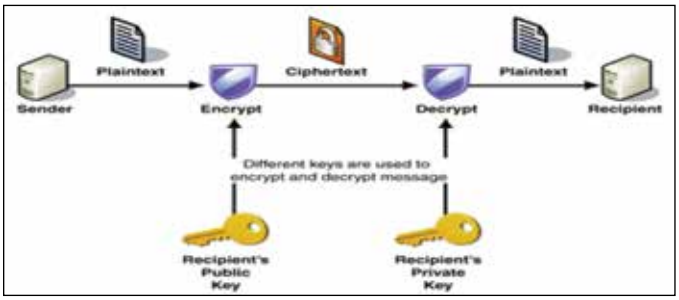


Source: Nat Queen, "Modern Cryptography," *Acorn User, n. 265,* http://www.queen.clara.net/pgp/AU265.html)

Asymmetric Key Encryption

This form of encryption is majorly used to transmit secure messages even to the unknown recipient. This technique employs different sets of keys for encryption and decryption; one is the private or the secret key, while the other is the public key as shown in Figure 4. Both the keys are mathematically linked to each other. When trying to draw analogy with a padlock, it needs to be noted that it uses one key for locking and another for unlocking.[5] This encryption is used to create digital signatures.

Figure 4: Asymmetric Key Encryption



Source: Nat Queen, "Modern Cryptography," *Acorn User, n. 265,* http://www.queen.clara.net/pgp/AU265.html)

The first known asymmetric key algorithm was invented by Clifford Cocks of Government Communications Headquarters in the United Kingdom. It was not made public at that time and was reinvented in 1976 by Ron Rivest, Adi Shamir and Leonard Adleman at the Massachusetts Institute of Technology and therefore the name RSA (abbreviation of their surnames).[6] This algorithm majorly relies on factoring of large numbers for security. Currently, RSA is vulnerable to any attack that is able to factor

the modulus part of the public key, especially the ones shorter than 700 bits. Many of the scientists have suggested keys of 1024 bits to be the most secure till a system comes into place that is able to break through it. In a reported case, a student of Notre Dame University used 10,000 computers and worked continuously for 549 days to break a 109-bit key.[7] This reflects both the difficulty of decrypting a key and also the certainty that some sophisticated system might come through that would facilitate the breaking of all locks that are purely based on mathematics.

In the last few decades, great strides have been achieved in the development of Quantum Computing. It has totally brought forth the fear of the 'sophisticated systems' capable of breaking complex locks in the realm of reality. Quantum computers are different from the traditional in the sense that while the latter uses binary 1 or 0 system to function, the former works using 'qubits'.[8] Qubits are special as they do not simply add processing capability, rather exponentially increases it. For instance, four classical bits can be in 2^4 positions using the principle of superposition (being every possible of 0 or 1 at the same time). Another principle that these qubits employ is the principle of entanglement, that is, 'qubits in a superposition can be correlated with each other: the state of one (whether it is a 1 or a 0) can depend on the state of another; or a change in one part of the system will lead to the rest responding accordingly without changing the entire operation'.[9]

Ina more simplistic term, quantum computers are basically those systems that would have the capacity to do complex tasks in split seconds; this could also include breaking of the conventional encryption locks.[10] Traditional encryption does not guarantee a foolproof security of the system. Basically, the length of the key determines the possible number of permutations and combinations that can be attempted in order to break the code. In other words, 'strength of encryption is directly proportional to the length of the key and the layers of encryption'.[11] The most common form of attack is the 'hit-and-trial method' that tries different combinations of key until the correct one is found. The other form of attack is the side channel attack, which does not attack the cipher directly, rather studies the physical parameters such as power consumption, implementation time and so forth. These parameters could be manipulated in order to get the desired outcomes. This is where quantum computers come in. The pervasive fear of quantum computers breaking complex locks has paved the way 'quantum resistant schemes' that can resist any attack by quantum computers. Most promising among those is Quantum Encryption. In the current context, several scientists have been working towards deploying a foolproof Quantum Encryption before any states gain achievement in quantum computers that can easily break complex locks.

Advances in Encryption Technology

There is barely a field that has been left untouched by rapid advances in technologies and encryption is no exception. In the past few decades, the quantum properties of light and matter have been applied to the field of information security. Indeed, the research in this field has advanced to the point that quantum properties are being used to transmit information over large distances.[12]

Heisenberg's Uncertainty principles states that if "one is able to measure a thing accurately, at a given point of time then one cannot measure another thing accurately."[13] For instance, if someone is able to measure the velocity of a flying electron at a given point of time, then it would be difficult to determine its position in the same time. This is because of the constant changing position of the particles. In case of photons, that has wave-like properties and are either polarised or tilted in a certain direction. These properties have been utilised to develop new means to encrypt messages that are very difficult to decrypt. This has led to the concept of Quantum Encryption that majorly encapsulates the process of Quantum key distribution (QKD) and traditional encryption. QKD can be seen as a theoretically secure solution to the key exchange problem.[14] With QKD, the 'photons distributed at the microscopic quantum scale can be horizontal or vertically polarised but observing it or measuring

it disturbs the quantum state'. This disturbance can easily be noted by both the sender and the recipient. Thus, Quantum Encryption not only facilitates the detection of interception but also destroys the message being sent, thus making the message useless for the eavesdropper and the recipient as well.[15]

In the 21st century, IT has become the cornerstone of modern society, and has therefore, paved the way for global web of interconnected networks. These interconnected networks have eased the way of life and enhanced efficiency by integrating key operations and processes in the arenas of Critical Information Infrastructure such as banking and finance systems, power-grids, and so forth, and have fortified state capabilities with improved intelligence, surveillance, reconnaissance capabilities, early warning system, and so forth. These information systems could be considered as a treasure trove for the adversaries to gather intelligence and key details. There are multiple ways through which malicious groups could break into the system, and encryption would act as the apt shield in those cases. However, lack of strong encryption techniques could prove lethal for states. This outlines the importance of using Quantum Encryption in ensuring the network as well as information security and thereby strengthening the overall national security apparatus.

As mentioned above, the expanding networks of the society do call for a strong level of encryption and for the protection of the critical information. However, there have been several cases where the states have pushed for exceptions in certain cases to gain access to encrypted data. The increased cases of lone wolf attacks across the world indicate that the online impetus to radicalisation have been elevating the paranoia of the state apparatus. Therefore, many of the government agencies seek a backdoor access to the encrypted data, for instance, the 2015 San Bernardino shooting incident that led to the death of 14 people.[16] The perpetrators were found to be using Apple iPhone for communicating and Federal Bureau of Investigation wanted to get access to the data.[17] However, Apple refused to assist the government agency to gain access to the phone. This is not an isolated case; nevertheless, cases like these bring out the prevalent difference between the government agencies and private enterprises. On the one hand, the private agencies feel that giving backdoor access would not only open doors for vulnerabilities or illegal snooping but also break the trust of the dedicated customers on the product. On the other hand, intelligence agencies are more concerned about malicious groups or terrorist groups would use the benefits of encrypted applications to fulfil their objectives. The lurking conundrum of an individual's privacy and the obligation of government agencies to limit nefarious activities detrimental to the nation's security have been a visible impetus to invest more in Quantum technologies across the world.

Nevertheless, various countries such as the United States, Singapore, Japan, Canada, and Italy are involved in conscious efforts to develop efficient quantum systems to hold their information protected. China has been able to build a Quantum Satellite that could be considered as a step towards mitigating threat to security. Even India is not far behind in this regard, rather, it is taking substantive steps to implement advances in Quantum Technologies in its security matrix.

Where Does India Stand?

India is joining the handful of nations that have already embarked on the journey of building satellite networks for secure quantum communications as the existing communication systems are vulnerable to myriad attacks. Under the Memorandum of Understanding signed between Raman Research Centre (RRI) and Indian Space Research Organisation (ISRO) Space Application Centre, the latter would fund the Quantum Information and Computing (QuiC) laboratory at RRI for developing the Quantum Technologies.[18] Many scholars in the strategic community believe that China's US$100 million investment in its quantum satellite called the 'Micius' acted as a major impetus for to initiate such undertaking. The QuiC lab has already been pioneering 'fundamental quantum experiments using single and entangled photons'.[19]

Even Russian Quantum Centre has offered quantum technology to India to keep the hackers at bay.[20]

Scholars view that a technology like 'quantum cryptography' is also significant at a time when there has been a visible surge in nefarious cyber activities in India as the country is steering towards digitalisation. Researchers in India at cybersecurity company, Fire Eye, recently discovered phishing websites created by cyber criminals that spoof 26 Indian banks in order to steal personal data from customers. In another incident, the security of about 3.2 million debit cards got compromised in the country just a month before demonetisation. Likewise, there have been several cases of cyber thefts, crimes and espionage. Therefore, it becomes imperative for the country to secure its data and hence, Quantum Encryption comes as a lifesaver.

Many of the strategic thinkers in India assert that the intelligence agencies within the country 'need to develop a "sixth sense" to predict with accuracy critical inputs on security in today's shifting world order and geopolitical dynamics."[21] Undeniably, the country has had its fair share of successes in acquiring accurate inputs by the intelligence agencies such as Research and Analysis Wing or the Intelligence Bureau. However, there still remains a pervasive need for the intelligence agencies to be more adaptable and cognizant with emerging technologies in data collection and analysis. The role of covert intelligence is going to see an upward trend in the coming years and technological advances like Quantum Computing would further redefine intelligence predictions.

Conclusion

Cryptography has always played a quintessential role in protecting the state secrets. With the dawn of Information Age, the 'information' has become a crucial strategic element that needs to be protected at all costs. However, the advances on ICT have been both the solution and the problem. On the one hand, the advances in Quantum Computers is making great strides and also making the states threatened by it potential of unlocking complex locks with a snap of a finger. On the other hand, the emergence of Quantum Encryption would fortify the security of data. So far, the paradoxical progress is still puzzling the world, whether 'Quantum Encryption will provide unbreakable ciphers, or Quantum Computing will result in ciphers being cracked?'

Nevertheless, states have been readily investing in quantum technologies so as to achieve quantum pre-eminence and subsequently, strategic dominance in the international arena. India, in this regard, has not been far behind. With the country's push towards digitalisation and the initiative to develop smart cities, protection of data has become paramount. The country can no longer choose to overlook the rising cases of data thefts and cyber crimes. Experts are of the view that India needs to take cognisance of emerging technologies such as the Quantum Computing and Quantum Encryption and develop indigenous capabilities in these areas.

As innovation becomes the driving force of the networked world, it is pertinent that security and policy readily follows in order to control the human perception in a more conflicting paradigm. As a matter of fact, there can neither be 100 percent privacy nor 100 percent security in a networked arena. This calls for a harmonious intersection between national security and the individual's privacy. In this context, many scholars have articulated the need for an international agency that could be empowered to have overview of the many intelligence agencies for the mass surveillance and collection of data. Even if the states are able to build a 'fail-safe infrastructure' by facilitating secure and advance encryption technologies rather than striving for a foolproof infrastructure, it would provide a major boost to the nations' national security. Importantly, it should also be noted that Quantum Encryption is not a one stop solution for mass surveillance or protecting one's privacy. There are various means and mechanisms of gathering information. Especially with the surge in state-of-the-art technologies, in this digital age, gathering information has become as easy as reading a newspaper. Quantum Encryption is merely equivalent to a self-destructive iron box that keeps the information tight and gives access only to those who have the right key. Any attempts to forcibly open the box would lead to the complete destruction of the box, not only rendering the message unusable but also leaving a distinctive trail of an eavesdropper.

... Advances in Encryption Technology

Notes

1. "A Brief History of Cryptography," *RedHat Publication,* https://access.redhat.com/blogs/766093/posts/1976023, accessed on August 14, 2013.
2. Ibid.
3. Nicholas G. McDonald, "Past, Present, and Future Methods of Cryptography and Data Encryption," *University of Utah (USA).*
4. Ibid.
5. Tony Howlett, "Open Source Security Tools: A Practical Guide to Security Applications," *Prentice Hall PTR,* (July 29, 2004). http://books.gigatux.nl/mirror/securitytools/ddu/ch09lev1sec1.html
6. Kostas Zotos and Andreas Litke, "Cryptography and Encryption," *Department of Applied Informatics* (Greece).
7. "Notre Dame Math Whiz Cracks Code," *Reuters*, (November 07, 2002). http://www.zdnet.com/article/notre-dame-math-whiz-cracks-code/.
8. Patrick Caughill, "A New Breakthrough in Quantum Computing is Set to Transform Our World," *Futurism,* (July 28, 2017). https://futurism.com/a-new-breakthrough-in-quantum-computing-is-set-to-transform-our-world/
9. Deutsch, David, "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer," *Proceedings of the Royal Society of London A.,* (1985). http://adsabs.harvard.edu/abs/1985RSPSA.400...97D.
10. Ibid.
11. "Quantum Encryption—A Means to Perfect Security?," *SANS Institute,* (2003). https://www.sans.org/reading-room/whitepapers/vpns/quantum-encryption-means-perfect-security-986.
12. Ibid.
13. Ibid.
14. Doug Drinkwater, "What is quantum encryption? It's no silver bullet, but could improve security," (November 08, 2017). https://www.csoonline.com/article/3235970/data-protection/what-is-quantum-encryption-it-s-no-silver-bullet-but-could-improve-security.html
15. Ibid.
16. Evan Perez and Tim Hume, "Apple Opposes Judge's Order to Hack San Bernardino Shooter's iPhone," *CNN*, (February 18, 2017). http://edition.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html
17. Ibid.
18. IANS, "ISRO's New Baby: Building Secure Quantum Communications in Space," (October 27, 2017). https://yourstory.com/2017/10/isros-new-baby-building-secure-quantum-communications-space/
19. Ibid.
20. Peerzada Abrar, "Russia Offers Technology to Keep Hackers at Bay," *The Hindu,* (December 25, 2016). http://www.thehindu.com/business/Economy/Russia-offers-technology-to-keep-hackers-at-bay/article16942015.ece
21. "Intelligence Agencies Need Sixth Sense: M K Narayanan," *The Deccan Chronicle*, (November 19, 2017). https://www.deccanchronicle.com/nation/current-affairs/191117/intelligence-agencies-need-sixth-sense-m-k-narayanan.html

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, Email: landwarfare@gmail.com
Website: www.claws.in
CLAWS Army No. 33098