Cyber Defence — India's Critical Infrastructure

Commander K Ashok Menon (Retd)[@]

Abstract

Cyber war is becoming a greater concern for all nations, including India, than at any time earlier. In the on-going war between cyber attackers and cyber defenders, the defenders are still at the receiving end. Based on available information in the public domain, it is difficult to gauge India's overall cyber defence preparedness, though it has been reported that those engaged in this have taken initiative to improve security. At the same time, the government has mandated that organisations 'implement certain security protocols'. The Indian cyber security establishment, in the meanwhile, must think of counter measures factoring the cyber defence-offence balance, especially when the nature of the attack gets more sophisticated, and it is a determined 'State' that is at the other end.

Introduction

In the on-going cat and mouse game between cyber attackers and cyber defenders — who have an unenviable task of defending their technology systems despite substantial advancements in the field of tech-security — the defenders are still at the receiving end. Letting the guard down would be at its own peril even if the claims from the attacker ilk sometimes borders on hyperbole and tends to blur facts.

The earliest recorded duel between these two sides — though the term cyber in that context may not be appropriate — dates back to 1903, when Marconi attempted to demonstrate secure wireless communication capability between Prof Flemings positioned at the lecture theatre in the Royal Institute in London while he himself was stationed at Cornwall, about 300 miles away.

[@]**Commander K Ashok Menon** is a naval veteran whose key assignments in the service included Joint Director of Personnel (Information Systems) & Logistic Officer INS Delhi among other coveted appointments. He has also held different positions in the Integrated Logistics Management System Centres.

Journal of the United Service Institution of India, Vol. CLI, No. 625, July-September 2021.

This communication experiment was successfully sabotaged by Nevil Maskelyne, 'an inventor, magician and a general troublemaker'. The 'weapon' that was used by him to block the signal and transmit his own content was a transmitter capable of outputting '8 or 9 Amps', which he had 'lowered to 2.5 Amps' and placed it close to the stage from where Prof Flemings spoke. One version of the reported event states that just before Marconi's demonstration commenced, the projection lantern used for the slide show began to click and what it conveyed in Morse was "Rats, rats, rats, rats; there was a young fellow of Italy, who diddled the public quite prettily"[1] targeting Marconi. While some of the facts that Marconi had claimed earlier did come to question as a result of this successful 'interference', it was eventually overlooked. However, seen in today's raging cyber-attack context, Maskelyne did seem to have the last word when he concluded in Latin "Qui vult decipi, decipatur" or "Let him be deceived who wishes to be deceived". Governments at that point in time too were impressed by Maskelyne as they had seen the ease with which signals were monitored by him; subsequently leading to the development of wireless encrypted systems that were used during the World Wars and later.[2]

As the cyber space has grown, the cross-section of the attacker community and the nomenclature for referring to them too have evolved. Terms like Identity thieves, Internet stalkers, Cyber terrorists, Advanced Persistent Threat groups (APT groups) etc. have come into existence. The general classification of White, Grey and Black Hat are used to convey intent, ethics, and legality of the hacking community — with the White Hat hackers being the only safe ones.

Again, to get a glimpse of 'state' involvement in this duel, it would be worthwhile to look at the early stages of the computer era. Cliff Stoll's "The Cuckoo's Egg", a 1989 book, provides a first-hand account of a computer break-in, where he documents the cyber investigation and audit findings of a "75 cents" error in the computer usage account at the lab he was working in California, which after a "dangerous game of deception, broken codes, satellites and, missile bases…"[3] is finally traced to a hacker — Markus Hess in Germany who was incidentally involved in selling his findings to the Soviet Union's intelligence agency, KGB.

In essence, the 'state' has been a key actor in this duel – always.

Information Technology (IT) vs Operational Technology (OT)

While IT infrastructure, and software solutions that ride on them, got early attention from a security standpoint thereby giving rise to a sizeable collection of professionals with the necessary credentials, apart from a fit for purpose collection of products and services that addressed the security need at each 'layer', the Industrial Control Systems or ICS [which in turn includes Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS)] and connected devices fell behind.[4] ICS leveraged OT, essentially meaning "a category of computing and communication systems to manage, monitor and control industrial operations with a focus on the physical devices and processes they use".[5] In the past, these systems were, by and large, managed and monitored manually. The software and protocols that were used were proprietary in nature and most of them operated in 'islands'. So the risk of being targeted by hackers was limited as there was no 'network-interface' and hardly any integration between OT and IT system; neither did they have the same type of vulnerabilities. But over the last few years, this has changed. Efficiency enhancement initiatives and single window control of "industrial systems together with process management solutions" that deliver accurate information have made OT-IT convergence a necessary imperative.[6]

But there are challenges in handling technology security in this hybrid environment as the basic prism through which security implementations in the IT and OT spaces are seen, differ. Whereas a conventional Information Security professional in the IT vertical sees it through the lens of the 'Confidentiality, Integrity, Availability (CIA) triad' — for OT security implementation, 'Availability' comes first. Consider for instance, the case of a typical 'software patch update' where an asset is to be made available for application of a patch. In an IT system, an asset is handed over to the security team first for application of a patch (albeit in several cases for a short duration) as confidentiality and integrity are critical and cannot be compromised once the system is in a production environment. Operations teams need to factor this into the plan and currently for most mature enterprise systems there is a standard template that is followed. But the OT professional's dilemma is different. For him/her, 'Availability' is non-negotiable. A downtime of an asset is likely to affect other linked assets and thereby can impact safety

of people and the entire system as a whole.[7] However, these challenges would have to be managed as with the rise in OT-IT integration, attacks on these systems — especially the ones that operate critical infrastructure (Energy, Transportation, Water etc.) and have embedded cyber devices — have increased.

Technology Security Incidents

The ransomware attack on Colonial Pipeline, a US Company that handles the largest pipeline system in the US that moves gasoline, diesel, and jet fuel from the Gulf coast to the East Coast market[8], in early May this year was one such incident. The attacker was apparently "Dark Side", an East European based criminal gang. Despite the fact that the company stated that its systems had been restored within a week, the impact continued to be felt, be it shortages across states, drivers being stuck in long queues and encountering empty gas stations, oil prices shooting up etc.[9] A cyber audit carried out three years ago had found "glaring deficiencies" and a "patch work of poorly connected and secure systems", while the company itself has claimed that it has taken several measures since 2017 to address the security concerns.[10] US leadership, in the meanwhile, has pointed out that it is a 'wake-up call' for the US energy infrastructure.

Based on available information in the public domain, it is difficult to gauge India's overall cyber defence preparedness in the oil and gas infrastructure though it has been reported that Public Sector Undertakings (PSUs) engaged in these verticals have taken initiative and "were making efforts to beef up security" while at the same time government has mandated that these organisations "implement certain security measures".[11]

India's power establishment had a status check on where it stood on cyber protection measures of its assets, when on 28 February 2021, David Sanger and Emilie Schmall of The New York Times (NYT) reported a study carried out by Recorded Future (RF), 'a company that studies the use of the internet by state actors', on a cyber-break-in, raising a key concern as to "whether an outage that struck on Oct 13 in Mumbai" (last year) compromised our critical infrastructure and was a veiled threat "from Beijing about what might happen if India pushed its border claims too vigorously".[12] Surely, the news of a Chinese malware implant in a nation's power grid infra cannot be music to anyone's ears, least

of all the key stakeholders within the power eco-system responsible for delivering uninterrupted service or the larger cyber security establishment committed to protecting these assets. The report delved into the approach adopted and also revealed that 10 Organisations in the "power generation and transmission sector were targeted".[13]

Preparedness: Power Ecosystem

In December 2019, the Minister of State (MoS) for Power told the *Rajya Sabha* that in order to address cyber threats 'over the national power grid', protection of Transmission Assets, for instance, was achieved by handling 'communication from equipment of substations to control centres' using 'dedicated optical fibre network owned by Powergrid' and in turn 'without any connectivity to external networks'. He further emphasised that 'these assets' were "protected through multiple firewalls and systems" and were "kept isolated from office networks to prevent any malicious online attack because of internet activity". Conveying how closely the "Computer Emergency Response Team (CERT) housed in Powergrid" were working with Indian Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIP), Ministry of Home Affairs (MHA) and Ministry of Electronics and Information Technology (MeitY), he highlighted that "regular cyber audit, crisis management plan, mock drills and exercises… were being undertaken".[14]

Deeper insights can be obtained from a presentation of 2018, titled 'Cyber Security in Power System', by a Chief Engineer (IT) from the Ministry of Power, which delves in detail on the steps that have been taken and are underway in securing the infrastructure. A few key aspects from 'Action to be Taken' & 'Action Points' reflects a forward-looking approach in handling these threat scenarios and at the same time, the section on 'Cyber Security Preparedness' does confirm that the magnitude of the problem at hand is not underestimated either. Since it is stated that entities like National Thermal Power Corporation (NTPC), National Hydroelectric Power Corporation (NHPC) etc. have already implemented ISO 27001 (a standard that provides requirements for an Information Security Management System) controls, there are good reasons to believe that the security-culture would have percolated to other related entities too in the Power ecosystem

during the last couple of years.[15] This is of course with the caveat that the nuances of ICS (that are applicable) were factored as a part of the implementation considering other standards like IEC 62443 that provides a framework to address and mitigate security vulnerabilities in industrial automation and control systems or similar standards like US's NIST 800-82.

Inconsistencies

Yet, what was disconcerting was the conflicting and inconsistent responses from the centre and the state of Maharashtra that were captured by several Indian news outlets in the days that followed the NYT reporting 'the likely power grid sabotage'. Extracts below from these reports[16] are highlighted to substantiate the point:

Centre's position:

- There is no impact on any of the functionalities carried out by the Power Sector Operations Corporation (POSOCO) due to the referred threat.
- No data breach / data loss has been detected.
- The massive grid failure, which hit Mumbai and surrounding areas on 12 October last year, was caused by human error and not due to cyber-attack.

State's reactions:

- The massive power outage in Mumbai last October was an attempt at 'cyber-sabotage' according to a preliminary report.
- 8 GB foreign server data may have transferred into the Maharashtra State Electricity Board system to sabotage the financial capital's power supply.
- Based on the preliminary information, there definitely was a cyber-attack and it was a sabotage.

If indeed most of the information security controls were in place, it is logical to assume that the incident management process, which included responsibilities spanning across multiple stake-holders, the incident escalation matrix, Responsible, Accountable, Consulted, Informed (RACI) matrix etc. would all be in place. In which case, a single root cause analysis artefact for the incident would have emerged that provided details of the incident impact

assessment, issue resolution, prevention of recurrence etc. However, multiple investigating agencies within, what can be perceived as, a single organisation coming out with different findings should be a matter of concern. More so because, an attacker's intent is to not only disrupt a service — but also observe and assess the victim's approach to recover. Further, if the assessment that at the state level there was a "lack of expertise" and an "inability to detect the malware" and therefore it "exposed the country's vulnerability"[17] is read in conjunction with the various responses from the centre and state, the larger question that emerges is that whether there are other weak links that need to be identified and remedial action taken without delay.

Kaspersky in the technical document, which provides details on ShadowPad malware (referred to in the original report and the Ministry's responses), has written that it is what attackers deploy in their target's networks "to gain flexible remote-control capabilities".[18] In an investigation carried out by them in July 2017 in a financial institution's network, "suspicious Domain Name System (DNS) requests were identified" where they explain how "The attackers hid their malicious intent in several layers of encrypted code". Not sure of who exactly was behind the attack, they have stated, "Currently, we can confirm activated payload in a company in Hong Kong", adding that attribution would be difficult as attackers are careful not to leave a trace though "certain techniques were known to be used in another malware like PlugX and Winnti, which were allegedly developed by Chinese-speaking actors".[19]

So, even if we assume the best-case scenario and accept the words of the Power Minister that the cause of outage was human error, at least for the cyber security professionals, handling the domain, it would better to analyse and draw their inferences based on flipped Occam's razor; remain circumspect and prudent and *think zebras and not horses,* even well after the 'hoof beats' created by this report dies down. In other words, not to presume that the inference is as simple as other indicators may lead us to believe.

As CyberWire has stated, while it is possible that the conclusions reached in the report by RF "are more tentative and circumspect" than what NYT or media outlets in India reached, it

is better that we see it "in the spirit in which the researchers have apparently offered it".[20] Also, while we may not accept the rankings given to India (21 out of 30 countries in Cyber space capabilities) – based on the National Cyber Power Index drawn up by the Belfer Centre at Harvard University last year – we still do need to be concerned of China being ranked number 1; as the seven parameters that were measured to assess "intent and capacity" were: "Defence, Offence, Surveillance, Control, Intelligence, Commercial, and Norms".[21] A closer examination of technology security incidents outside India further amplifies this point.

Texas Power Crisis

CyberWire points out that the impact of "cyber sabotage of a power grid" can be gauged when a comparison is made with the Texas power crisis that struck in February – though in that case it was due to severe winter storms across the US – that resulted in major electricity downtime. Fallout of this led to shortages in basic needs – water, food, and heat – and approximately "4.5 million homes and businesses without power at its peak" and an "estimated $295 billion in damage".[22]

But what is significant is the argument made by Control Global (CG) in the context of cyber security that while the US critical infrastructure are "vulnerable to disruption from natural disasters", a bigger concern is that similar disruptions can be "triggered by adversaries" and "cascading effects" ensured by "exploiting control systems". Elaborating on the Texas incident, CG observes that there were "significant grid frequency drops that caused system-wide impacts" which "could potentially be unintentionally or maliciously exploited to cause long-term damage to grid and other critical infrastructure equipment". They fear that adversarial nation states – Russia and China – with considerable cyber offense capability "not only monitor but also affect the magnitude and recovery of events". The concern expressed is not out of place as the power crisis occurred in the 'same time frame as the Chinese-made transformer hardware backdoor issue and the Russian SolarWinds hack'. The impact would have been far graver 'if there were hardware backdoors in Chinese-made transformers that were manipulated'. That assessment that it was a Chinese threat gets a further boost when the statement from the Chinese foreign ministry released during the havoc created by the storm is read in

perspective; viz. "it reinforced a belief among Chinese citizens that their country is 'on the right path'". Clearly, therefore, the threat assessment by CG was not paranoid or made in an isolated vacuum. Hence, the concluding remarks that there is not "only a responsibility but also an opportunity" to leverage what happened in Texas to effect necessary "changes to regulations and guidance on cyber security of critical infrastructures" across organisations including the ones "that have a financial stake in critical infrastructure protection" is as applicable to the US context as it is to India's.[23]

Conclusion

In the context of Texas incident, Mike Rogers has written as to 'Why America would not survive real first strike cyber-attacks", adding "[…] hackers in Beijing or Moscow could turn off our electricity, millions would lose heat, groceries would spoil, banking machines would not work […]". But what would be even more disturbing is when he claims the reasons for any of their systems not going down on a larger scale; that they have so far "escaped a digital catastrophe" is not because of effective defence mechanism in place but "due to blind luck and restraint from our adversaries".[24] That, coming from one of the most powerful cyber capable nations, should surely worry the less capable ones.

As need for Internet of Things (IoT), Machine Learning and Big Data implementations start gaining ground, in the critical infrastructure space the OT-IT integration is set to further increase. In the meanwhile, hackers of all hues continue sharpening their skill sets on OT, while inadequate knowledge of OT on the one hand and the spiralling vulnerabilities on the other are adding to organisational woes — not to mention the large attack surface that they may have an onus to defend. While it is not any one's case that we would be able to establish a 100 per cent hacker proof environment, there is every need for all 'Critical Infrastructure' organisations to get the basics right — recognise that the threats are real, have a defined budget to address this realm, invest in the right set of technologies, and have enough skill sets within to get essential controls in place so that the attacks are not easy to execute. The clarion call to the larger Indian cyber security establishment, in the meanwhile, is to think of counter measures factoring the cyber defence-offence balance when the nature of

the attack gets more sophisticated and it is a determined 'state' that is at the other end.

Endnotes

[1] Kevin E. Hemsley, Dr. Ronald E. Fisher 'History of Industrial Control System Cyber Incidents', Available at: https://www.osti.gov/servlets/purl/1505628.71Nicole ; Accessed on 20 May 2021

[2] Richard Baguley 'Origin Of Wireless Security: The Marconi Radio Hack Of 1903', Available at: https://hackaday.com/2017/03/02/great-hacks-of-history-the-marconi-radio-hack-1903/; Accessed on 20 May 2021

[3] Cliff Stoll, 'The Cuckoo's Egg', (2005), Back Cover

[4] 'Cyber attacks on critical infrastructure', Available at: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html ; Accessed on 21 May 2021

[5] i-Scoop, 'Operational technology (OT) – definitions and differences with IT', Available at: https://www.i-scoop.eu/industry-4-0/operational-technology-ot/#:~:text=Operational%20technology%20or%20OT%20is,assets%20and%20manufacturing%2Findustrial%20equipment ; Accessed on 21 May2021

[6] 'OT Security Defined, Explained and Explored', Available at: https://www.forcepoint.com/cyber-edu/ot-operational-technology-security; Accessed on 21 May 2021

[7] David Bisson, 'ICS Security What it is and Why It's a Challenge for Organizations'; Available at: https://www.tripwire.com/state-of-security/ics-security/ics-security-challenge-organizations/; Accessed on 22 May2021

[8] 'Colonial Pipeline'; Available at: https://www.mckinseyenergyinsights.com/resources/refinery-reference-desk/colonial-pipeline/; Accessed on 18 May2021

[9] The Washington Post, 'As Colonial Pipeline recovers from cyberattack, leaders point to a 'wake-up call' for U.S. energy infrastructure'; Available at: https://www.washingtonpost.com/business/2021/05/13/colonial-pipeline-ransomware-gas-shortages/; Accessed on: 18 May 2021

[10] 'Tech Audit of Colonial Pipeline Found 'Glaring' Problems'; Available at: https://www.securityweek.com/tech-audit-colonial-pipeline-found-%E2%80%98glaring%E2%80%99-problems; Accessed on 18 May 2021

[11] Indian Express; 'Explained: How a US pipeline came under cyberattack, which group was behind it, and how it impacts oil prices': Available at: https://indianexpress.com/article/explained/explained-the-darkside-

cyberattack-on-a-us-oil-pipeline-and-how-it-impacts-prices-7310822/; Accessed on 15 May 2021

[12] David E. Sanger and Emily Schmall, The New York Times, 'China Appears to Warn India: Push Too Hard and the Lights Could Go Out': Available at: https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html

[13] Recorded Future, ´China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions'; Available at: https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf?utm_medium=email&_hsmi=110851062&_hsenc=p2ANqtz-83oaU-RLMlrmA7XBj2H5BzTM0HW9oR-5totH7NfJumY1CITOGQ8uRSfJdXTLI2fTov2oeqXLiCPzTBK9Rb_BgYGR5bTg&utm_content=110851062&utm_source=hs_automation; Accessed on 07 Mar 2021

[14] The Economic Times, 'Multiple steps taken to check cyber threats faced by national power grid' (Response by RK Singh MoS for Power, New And Renewable Energy); Available at: https://energy.economictimes.indiatimes.com/news/power/multiple-steps-taken-to-check-cyber-threats-faced-by-national-power-grid-r-k-singh/72358377; Accessed on 07 Mar 2021

[15] Vijay Menghani, 'CYBER SECURITY IN POWER SYSTEM' (a 2018 presentation by Chief Engineer(IT), Central Electricity Authority, CISO Ministry of Power); Available at: http://erpc.gov.in/wp-content/uploads/2018/03/ERPC_Cyber-Security-in-Power-system_presentation.pdf; Downloaded on 14 Mar 2021

[16] THE HINDU, 'Chinese cyber attack foiled: Power Ministry', Available at: https://www.thehindu.com/news/national/attacks-by-chinese-groups-thwarted-power-ministry/article33965683.ece; Accessed on 15 Mar 2021

[17] The Indian EXPRESS, 'After the blackout', Available at: https://indianexpress.com/article/opinion/editorials/mumbai-power-blackout-cyberattack-china-7213054/; Accessed on 16 Mar 2021

[18] Kaspersky Lab, 'ShadowPad: popular server management software hit in supply chain attack, Part 2: Technical Details' https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/08/07172148/ShadowPad_technical_description_PDF.pdf; Accessed on 16 Mar 2021

[19] Kaspersky, SECURELIST, 'ShadowPad in corporate networks', Available at: https://securelist.com/shadowpad-in-corporate-networks/81432/; Accessed on 18 Mar 2021

[20] https://thecyberwire.com/newsletters/daily-briefing/10/39; Accessed in Mar 2021

[21] The Indian Express, 'After the blackout', Available at: https://indianexpress.com/article/opinion/editorials/mumbai-power-blackout-cyberattack-china-7213054/; Accessed on 18 Mar 2021

[22] Chris Stipes, UNIVERSITY OF HOUSTON, 'New Report Details Impact of Winter Storm Uri on Texans'; Available at: https://uh.edu/news-events/stories/2021/march-2021/03292021-hobby-winter-storm.php; Accessed on 25 May 2021

[23] Joe Weiss, Control Global, 'Texas power outages demonstrate grid cyber vulnerability and inadequacy of existing regulations; Available at: https://www.controlglobal.com/blogs/unfettered/texas-power-outages-demonstrate-grid-cyber-vulnerability-and-inadequacy-of-existing-regulations/; Accessed on 18 Mar 2021

[24] Mike Rogers, THE HILL, 'Why America would not survive a real first strike cyberattack today'; Available at: https://thehill.com/opinion/cybersecurity/539826-we-would-not-survive-true-first-strike-cyberattack?rl=1; Accessed on 18 Mar 2021