VOLUME 1, ISSUE 1, OCTOBER 2011

Battle-Ready for the Fifth Dimension: Assessing India's Cyber-Defence Preparedness

Pukhraj Singh*

This article provides a rare behind-the-scenes look at the cyber war and cyber defence capabilities being developed by various great powers and situates India's own developments in this field within the larger context of emerging threats and modernisation of warfare. The author ascribes the Stuxnet worm of 2010 to be a big eye opener which helped place India's cyber security systems on a war footing. He also depicts a future cyber war scenario in which web-based weapons are integrated into conventional armouries to achieve the perfect fifth dimension of warfare. The article also describes how experts and analysts of strategic affairs who are outside the secretive government establishments dealing with cyber war can contribute to meaningful reforms, institutions and changes that can facilitate multilateral responses in the form of a global cyber security regime.

CHINA'S CYBER LEGIONS

Media reports have indicated that India's National Security Council (NSC) is mulling over a proposal on the institutionalisation of cyber-warfare, to gain tactical and strategic superiority in the region by leveraging this potent form of asymmetric conflict.[1] Groundwork is being laid to address the offensive aspects of Computer Network Operations, which would entail infiltrating the information assets of hostile nations as well as non-state actors. Such covert operations are devised to gain actionable intelligence or cripple the command and communications infrastructure of the enemy.

*The author is a cyber-warfare specialist employed with the National Technical Research Organisation, Government of India. Prior to NTRO, he was associated with well-known cyber-intelligence firms across India, Canada and the US. He has been a speaker at international security conferences and authored many technical research papers. He can be reached at pukhraj@gmail.com.

1 The Economic Times.Spy Game: India readies cyber army to hack into hostile nations' computer systems. *The Economic Times*. [Online] 06 August 2010. http://articles.economictimes.indiatimes.com/2010-08-06/news/27590170_1_computer-systems-spy-game-hackers.

The National Technical Research Organisation (NTRO), a specialised scientific facility under the Prime Minister's Office (PMO), and the Defence Intelligence Agency (DIA), which represents the intelligence Wings of the Tri-Services (Army, Navy and Air Force), would act as the primary stakeholders, along with the peripheral involvement of Defence Research and Development Organisation (DRDO). This seminal development is the outcome of an unusual turn of events in India's long-drawn effort to address escalating incidents of cyber-espionage, a well-orchestrated and systematic campaign of subversion and sabotage.

In July 2010, India's Ministry of Defence (MoD) issued a press-note acknowledging a report submitted by researchers from the Munk School of Global Affairs, University of Toronto, on the "hacking of Indian Defence Networks".[2] Earlier in March 2009, the same group had released its first report publicising the existence of GhostNet, a cyber-spying ring targeting the offices of the Dalai Lama, embassies, foreign offices and ministries of various countries including India.[3] In a subsequent investigation spanning many months, researchers from the Munk School and Shadowserver Foundation, a volunteer group of cyber-crime investigators, laid bare a second white paper divulging details of a newer, much complex and clandestine variant of the snooping nexus, specifically aimed to target the offices of the Indian Government.[4]

The origins of these attacks were traced to China, but no explicit evidence was supplied to ascertain state involvement. In a carefully choreographed move, the second paper was made public on a day when India's External Affairs Minister S.M. Krishna was scheduled to meet Chinese Prime Minister Wen Jiabao on the former's maiden visit to China. The incident sparked media frenzy and had the potential to derail the bilateral agenda.[5] The Canadian researchers were also able to access the attacker's command-and-control (C&C), tapping hundreds of classified documents being purloined, thus adding further to the embarrassment.

---

2 Ministry of Defence, Government of India. Hacking of Security Information. *Press Information Bureau.* [Online] 27 July 2010. http://pib.nic.in/release/rel_print_page1.asp?relid=63588.

3 Information Warfare Monitor, Citizen Lab, SecDev Group, Shadowserver Foundation.*Shadows in the Cloud: An investigation into cyber espionage 2.0.* 2010.
http://www.infowar-monitor.net/2010/04/shadows-in-the-cloud-an-investigation-into-cyber-espionage-2-0/

4 Information Warfare Monitor, Citizen Lab, SecDev Group.*Tracking GhostNet: Investigating a Cyber Espionage Network.* 2009.
http://www.nartv.org/mirror/ghostnet.pdf

5 The Hindu. India not to raise hacking with China . *The Hindu.* [Online] 06 April 2010. http://www.thehindu.com/news/international/article389948.ece

This diplomatic disaster of sorts was quelled in a peculiar fashion with reassuring statements from various organisations mandated to guard the nation's cyber-frontiers. The underlying confidence in their approach came from the fact that the Indian investigators had already homed in on this nefarious web of intrigue. In fact, they were in the thick of things by December 2009, when reports on Chinese attempts to hack the Indian Prime Minister's Office, the Office of the National Security Advisor (NSA) and the Cabinet Secretariat surfaced.[6] The timeline and the modus operandi of this blitz had eerie similarities to the Chinese attacks on Google's infrastructure. At the peak of this debacle, the outgoing NSA, M.K. Narayanan gave a rare interview on the incident and shared some technical details – an unprecedented acknowledgement of India's seriousness on such matters.[7]

As in the case of GhostNet and its variants, attackers sent emails with malicious PDF and Microsoft Office attachments which seemed to originate from trusted senders like friends, family, colleagues or business partners – a highly-targeted campaign using sophisticated exploitation techniques and an improvisation of what is termed as Spear Phishing. This was followed by media reports on a series of similar attempts targeting the NSC, the National Security Advisory Board and a host of other sensitive organisations. Clearly, hacking had come a long way from being the playful antics of garage geeks to changing the course of diplomacy at the press of a button.

Judging from the details available publicly, it is not difficult to estimate that in all certainty, terabytes of information had been exfiltrated from various government organisations including defence, security agencies, ministries, scientific establishments, think tanks, academic institutions, media groups, important individuals and the corporate sector. The scale of such an operation and dimensions of this guerrilla war are simply mind-numbing.

One can imagine a nondescript safe-house with hundreds if not thousands of geopolitical analysts, linguists, military experts and hackers busy in processing and dispatching this data to various "consumers", who are probably scouting for potential moles, gauging the implications of a regional development or war-gaming the readiness of India's defence

6 India Today**.** Chinese hackers target PMO. *India Today*. [Online] 14 January 2010. http://indiatoday.intoday.in/site/story/Chinese+hackers+target+PMO/1/79215.html.

7 The Sunday Times**.** http://www.timesonline.co.uk/tol/news/world/asia/article6991789.ece. *The Sunday Times*. [Online] 18 January 2010. http://www.timesonline.co.uk/tol/news/world/asia/article6991789.ece.

forces. The case of this being an independent enterprise should simply be ruled out for once and ever – there has to be a tacit patronage from the state.

It also shows the amount of dedication and unflinching focus that is needed to hone such a capability. This knowledge-driven domain literally exploits the cutting-edge of technology and the mere fact that India is dubbed as the 'IT Superpower' is therapeutic at best. China, whose information warfare campaign has been much dissected and maligned, is just another player in the game who has become too strong to reckon.

A ground-breaking report prepared by Northrop Grumman for the 'US-China Economic and Security Review Commission' provides a clinical insight into the history of Chinese cyber-warfare and its modest beginnings ten years ago.[8] An exhaustive, concerted, and multi-faceted doctrine of the Peoples' Liberation Army (PLA)on the "informationalisation" of the military has helped it achieve this envious and coveted goal. Between the years 2000 and 2006, hoards of Chinese students attended information security courses at American universities and returned to their homeland ditching lucrative job offers. It was attributed that these state-sponsored students became the backbone of China's cyber-army.

The Russian Connection

While acknowledging the hyper-nationalistic motives driving Chinese hackers, one must not forget the tantalising economics of cyber-crime which make the job of law-enforcement and counter-intelligence even harder. Commercial cyber-intelligence teams at Symantec and iDefense have discovered the emerging trend of transnational mercenary hacking groups selling stolen information to the highest bidders. This is a multi-million dollars arms bazaar, where national or ideological affiliations do not matter and a Brazilian or Moroccan hacker can be found trading with an Iranian.

Another related development which tipped the scale towards China is its will to act as a safe-haven for cyber-crime infrastructure. Around 2006, a powerful syndicate of cyber-criminals based in St. Petersburg, called the

8 Northrop Grumman. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* 2009.
http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

Russian Business Network (RBN), monopolised the identity theft, child pornography, phishing, spam, and malware industry by providing hack-proof internet services.[9]

At the peak of its existence, it had estimated revenues of around $150 million and flaunted connections with Russians politicians. Only after a vociferous campaign by media and international security agencies did the Russian authorities decide to dismantle RBN. In a few days after the crackdown, it had found a new home in China, though only temporarily. This incident became a precursor for the growth of an ancillary industry in China, the bullet proof hosting services, catering to a wide-array of shady clients including espionage operators. Its after-effects are being seen globally now. In a country like China where the Internet is so strictly regulated, this brashness and audacity of non-state actors leaves little to doubt.

The American Response

Such policies, which border on twisting the rules for strategic leverage, can act as a double-edged sword. It can be gauged from the fact that in 2008, the US Department of Defense had to neutralise an extremist website being operated as a honey pot by the C.I.A. and Saudi intelligence to track terror activities, as the forum was being used to plan attacks on US forces in Iraq.[10] Despite the C.I.A.'s objections, the website was taken down in a joint-operation by the Pentagon, the Justice Department and the National Security Agency, leaving Saudi princes fuming at the loss of a critical intelligence asset.

The incident triggered an internal debate on the lack of a clear mandate, guidelines and operating procedures for such operations, prompting the former C.I.A. Director Michael V. Hayden to comment in a state of plausible deniability, "Cyber was moving so fast that we were always in danger of building up precedent before we built up policy". It comes as no surprise that many top officials of the American establishment are being accused of hyping the cyber-war threats to push forth their narrow agendas.

---

9 Wikipedia**.** Russian Business Network. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Russian_Business_Network.

10 The Washington Post. Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies. *The Washington Post.* [Online] 19 March 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464_pf.html

India's Cyber Preparedness

To guarantee and retain information superiority, appropriate defensive measures and countermeasures are a must. While the debate on the exact definition of critical information infrastructure (CII) rallies on, the IT (Amendment) Bill 2008 attributes the designation of a national nodal agency for the protection of CII and the Indian Computer Emergency Response Team (CERT-In) to undertake incidence response under the Sections 70A and 70B, respectively.[11] MoD also mandates Defence Information Assurance and Research Agency (DIARA) as the nodal cyber security agency for the Tri-Services.[12] However, substantive resolution is needed on the role imparted to the National Informatics Centre (NIC), the IT infrastructure services organisation managing a majority of the government websites. A government-wide information security and regulatory compliance policy, dealing with issues like electronic document classification, compartmentalisation and centralised security clearance, is also the need the hour.

Any attempt to arrive at a possible solution to the aforementioned issues from a geopolitical, strategic affairs and policy making perspective will need a holistic approach taking into account the technical, legal and international complexities. India's National Security Advisor, Shiv Shankar Menon, has proposed the ratification of a global cyber-security regime or a cyber-arms control treaty.[13] Similar endeavours of international regulation in domains like chemical, nuclear and space warfare have been impactful. The primary stakeholders are even receptive to the idea of re-engineering the underlying communication protocols of the Internet to reach a level of moderation. While most nations, including those engaged in questionable activities over this medium sounded amenable, the talks have broken down repeatedly.

In this scenario, the responsibility of honing the discourse lands on the shoulders of able policy makers, strategic affairs analysts and geopolitical experts who can go to the depths of the problem and evangelise to the international security community with a fervent zeal. However, there exists a great chasm between the technical security professionals and high-

11 The Information Technology (Amendment) Bill, 2008. [Online] 2008. http://www.cyberlaws.net/itamendments/IT%20ACT%20AMENDMENTS.PDF.

12 The Economic Times. Hostile agencies trying to steal defence secrets from India. *The Economic Times*. [Online] 07 September 2010. http://articles.economictimes.indiatimes.com/2010-09-07/news/27605145_1_defence-establishments-indian-defence-pen-drives.

13. Proceedings of the Munich Security Conference 2011. Cyberspace Presents Complex Global Challenges. [Online] 2011. http://www.securityconference.de/Program.425+M578c0183589.0.html?&L=1.

level interlocutors. The special interest groups on information warfare and cyber-security lack the contribution of technologists with hands-on exposure, thus succumbing to misdirection and confusion. It is imperative that we inculcate in the thought process of contemporary policy makers the multifaceted views of such professionals.

The question that looms large is whether we can reach a coherent and agreeable consensus on attribution, deterrence and pre-emption of cyber-attacks. While India has made tall strides in order to assert its place in the fifth dimension of war, more awareness and seamless initiative is needed. Mere wishful thinking of being the next cyber-power would not take India too far. One must always keep in mind that hacking has its origins as a counter cultural movement preaching fierce individualism, full disclosure and an emphasis on breaking things. The very act of institutionalisation is an antithesis to a domain which breeds on chaos and anarchy.

How Stuxnet Changed Everything

As one picks through the trail of debris left by the Stuxnet worm in India, the turn of geopolitical events behind this watershed incident do not cease to spark the imagination. Enough has been said about the sheer technical brilliance and the blatant shortcomings of this attack believed internationally to be aimed primarily at Iran's nuclear programme. But one could go a bit further and try to hypothesise the strategic and tactical underpinnings of this attack. For the sake of argument, blaming it all on Israel is something that we usually do, but there is more to learn from Stuxnet.

I will continue from where Robert Baer left. The former C.I.A field officer and operative par-excellence wrote an article in March 2010 assessing the potential fallouts of the Mahmoud al-Mabhouh operation.[14] Mabhouh, a senior Hamas operative, was found dead in a Dubai hotel on January 19th, 2010, assassinated by a Mossad hit-squad. The brazenness and temerity with which this operation was executed left many nations fuming. With Dubai leading the acerbic opposition, any hopes to forge an Arab Sunni lobby or availing the Gulf airspace for a missile attack on Iranian nuclear installations were quashed. But the 'Plan B' was already in progress. Stuxnet began spreading in January of that year too. The chain of command must

14 Baer, Robert. Did the Dubai Assassination Really Help Israel? . *Time Magazine.* [Online] 09 March 2010. http://www.time.com/time/world/article/0,8599,1970586,00.html.

have explored all the options. Little did Baer know that the world had changed a lot since Osirak.

A few years ago, when the cyber war rhetoric had picked pace, this domain finally found its place in the 'conflict spectrum' – somewhere between 'petty crimes' and 'organised cartels'. Stuxnet pushed it up by a few notches on an axis which terminated at 'nuclear attack'!

Little known is the fact that with this single incident, the discourse on critical information infrastructure (CII) protection in India was turned on its head. For long, the government had shied away from putting the onus of this gargantuan and intricate effort on the designated authorities. In the bureaucratic muddle that comes with a domain as complex and cutting-edge as cyber security, a lot was lost in translation. The first and foremost problem to be reckoned with was developing a consensus on what the definition of CII implies and how far should India's cyber-preparedness strategy be stretched in order to safeguard the assets not directly under the control of the government. Stuxnet resolved all this and much more.

As the incidence response teams found that a majority of the hosts compromised by the Stuxnet attack were from India, a strenuous effort was undertaken to assess its motive and origins. However, this investigation actually resulted in the eye-opening revelation that India's industrial control systems are susceptible like that of any other nation. It was indeed a matter of grave concern that the only known and documented attempt to compromise SCADA (supervisory control and data acquisition) systems at a widespread scale had a substantial impact on India, including the organisations manning the utilities like power, hydroelectric and gas, etc.[15]

Apart from debunking all theories of conventional wisdom and security through obscurity on cyber security which were a rage in the corridors of power, the Stuxnet attack also provided an impetus to initiate the procedure for an effective and implementable CII protection policy. People knew what was at stake now, far better than living in a state of denial. It set many benchmarks and precedents which are surely to have a positive role in furthering the health and vitality of India's digital economy.

The insertion of section 70A in the amended IT Act makes sure that CII protection has constitutional validity and priority. As premier national

15 Carr, Jeffery. Did The Stuxnet Worm Kill India's INSAT-4B Satellite? *Firewall, The Forbes Blog*. [Online] 29 September 2010. http://blogs.forbes.com/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/; The Economic Times. Stuxnet worm making its way into India quietly. *The Economic Times*. [Online] 23 December 2010. http://articles.economictimes.indiatimes.com/2010-12-23/news/27580939_1_computer-worm-stuxnet-virus.

security policy and advocacy groups like the National Security Council are refining the mandate for the protection of India's cyber-frontiers, the onus of upholding the security of the nation's vital information assets will certainly gain more focus and priority. It is not a matter of surprise that in March 2011, a media report indicated that a joint team comprising of officials from NTRO and Air Traffic Control services were undertaking a vulnerability assessment exercise to ascertain the resiliency of airport networks against attacks like Stuxnet.[16] The article also stated,

> *"…As a counter measure, the top brass of the country, which includes all chiefs of staff and secretaries of home, telecom, defence, finance and IT, has drafted a plan to thwart any such attack".*

While it is indeed a major leap forward, such a surgical exercise can overshadow the broader debate on how these problems are to be tackled at a national or even an international level. What really falls under the purview of CII? How willing is the private sector to invest and contribute? Are the public-private partnerships acting as mere sounding-boards for such ideas? Are the laws and executive directives providing enough clarity? Is the absence, clash or disparity of mandates leading to a bureaucratic logjam or tussle while handling such incidents?

Consider the case of a national-level botnet mitigation strategy, which could possibly become the precursor to an Internet kill-switch mechanism in case of a coordinated attack against the country. It is a known fact that most cyber-espion age rings and worms like Stuxnet have a multi-pronged command-and-control which communicates and relays information to the perpetrators. There are ways in which they can be neutralised or rendered partially dysfunctional by carefully tweaking the backbone routing protocols.

DNS and BGP sink holing are concepts which have garnered a lot of interest among the law-enforcement and intelligence agencies alike. Not only can the botnets be dismantled with the execution of a few commands, but it could also provide counterintelligence or counteroffensive inputs which may lead to definitive attribution – the most challenging piece of the puzzle in case of a state-sponsored cyber-attack.

May 2011 marked the visit of US Secretary of Homeland Security Janet Napolitano to initiate the US-India Homeland Security Dialogue. Home Minister P. Chidambaram represented the Indian side and the Dialogue

16 The Economic Times. Stuxnet attack fear pushes govt to check IT network. *The Economic Times*. [Online] 31 March 2011. http://articles.economictimes.indiatimes.com/2011-03-31/news/29365994_1_scada-atcs-systems.

paved the way for a landmark agreement on cyber-security, in times of its increasing relevance in fighting the war against terror, and CII protection.[17] The corresponding computer emergency response teams from both the countries, US-CERT and CERT-In, would be the primary point of contacts in this bilateral knowledge-sharing exercise. Secretary Napolitano proposed

> *"…to choke off the life line of some of these terrorist organizations, to open a dialogue that includes cyber security which is necessary to protect the networks that are critical infrastructure".*

Not only does it symbolise the start of a new era in fostering a global cyber-security regime but may also prove monumental in dismantling international cyber-crime syndicates which also harbour terrorists, drug smugglers, human traffickers and espionage rings.

Unified Command: A Vision of Cyber War in the Future

The nerve centre of the Unified Cyber Command (CYBERCOM) is brimming with activity. The top echelons of military and intelligence have gathered in the Situation Room, staring at the massive projection screens which display half a dozen key-indicators, getting a minute-by-minute assessment of the emerging crisis. A team of operatives and analysts from Red Team, an elite squad of hackers specialising in offensive tactics, are manning their positions on the operations floor. An unending stream of information is being fed into the Intelligence Fusion Platform, special software running on a grid of supercomputers, supplying real time decision-analytics to the mission directors. Petabytes of structured and unstructured data generated by intelligence analysts and purloined from compromised systems are being processed at lightning speeds – patterns are drawn, anomalies are highlighted and hitherto unknown connections are established. This piece of analytical wizardry, leveraging the cutting-edge of data mining, artificial intelligence and human-computer interaction, acts as the brain of CYBERCOM.

A hostile act of an enemy nation has put India's national security in jeopardy. Decision makers give the go-ahead to launch a military offensive and the armed forces are brought in a state of operational readiness. A massive, multi-faceted cyber-attack will precede the conventional one, thus providing the crucial element of surprise.

---

17 US Department of Homeland Security. Readout of Secretary Napolitano's Trip to New Delhi. *US Department of Homeland Security.* [Online] 27 May 2011. http://www.dhs.gov/ynews/releases/pr_1306521907450.shtm.

A systematic campaign of cyber-espionage undertaken in the last few years, targeting the adversary's key establishments and functionaries, has already given the much-needed tactical and strategic impetus. Virtual spies have accessed the minds of its people, penetrated the labyrinths of its critical infrastructure and sabotaged the industrial foundations. A voyeuristic Brigadier with a penchant for beautiful women, who liked storing his intimate encounters on a personal computer, was blackmailed by the HUMINT division into becoming an asset. The source-code repository of a telecommunications company, which manufactures the majority of that nation's network devices, was stealthily modified to allow the provision of a remotely activated kill-switch.

Some of these backdoor routers made their way to MILNET, the operational network of the adversary's armed forces. Classified information from combat outposts, live video streams from unmanned aerial vehicles and the sweeps of air-defence radars – everything flows through MILNET. The terabytes of information being exfiltrated also aided a covert war of economic subversion and spreading misinformation. Dozens of such executions highlighted the effectiveness of this asymmetric domain.

As the situation crosses the Rubicon, CYBERCOM authorises a sequence of hostile actions that collectively form the first strike of battle. Information flow is altered, blind-spots are created and a communications blackout is perpetrated. Critical infrastructure like power plants, gas pipelines, water distribution and electricity grids are administered using SCADA industrial control systems, allowing the operators to monitor and manage them remotely.

Although the system generally undergoes rigorous security testing and is operated on a network using proprietary communication protocols, this methodology of ensuring security through obscurity is as good as its weakest link. A callous operator or a mismanaged network can allow loopholes to arise– exactly the kind of opportunities that Red Team keeps scouting. The compromised computer of an employee working at the electricity grid, which powers the adversary's capital, gave away the VPN login credentials to the SCADA interface. The deployed system was manufactured by a multinational vendor and had already been reverse-engineered by the Red Team. A handful of vulnerabilities were discovered in it and added to the zero-day exploit stockpile, to be used for situations similar to this. The grid is taken-over and an artificial power-surge cripples the capital of the adversary.

A group of patriotic black hat hackers, clandestinely funded and patronised by CYBERCOM, had created a strain of undetectable malware which infected hundreds of thousands of computers worldwide, forming the part of a massive botnet. The group is given instructions to undertake a denial of service (DoS) attack on crucial targets like the banks, stock market, government websites and ISPs. This bot-army chokes the designated networks with an electronic flood of packets, literally bringing the adversary's economy and information infrastructure to a grinding halt. A series of follow-up attacks on the BGP (Border Gateway Protocol) routers and DNS (Domain Name Service) servers pulverises the last remnants of the adversary's Internet backbone, or whatever is left of it.

The first phase of the conventional attack begins as the ground troops start marching. The Air Force scrambles a formation of fighters to mount an attack. As they enter the hostile airspace, the fifth-generation stealth aircraft leading the air-formation emanates a long-range data beam from an electronically scanned array (AESA) emitter. This special aircraft is fitted with an ultra-secret next-generation jammer, an electronic warfare system that can deliver cyber-attacks through the free space into an aperture. The data beams are packed with specialised waveforms and invasive algorithms that work like keys to open networks and jam electronic equipment. The aircraft also emits a bit-stream meant to be the secret activation code which toggles the kill-switch for a brand of network routers backdoored by Red Team.

This death-ray completely disrupts MILNET, leaving the opponent's military in a state of panic and chaos. The element of surprise provided by the CYBERCOM makes sure that the enemy's command-and-control is neutralised, paving the way for a swift and decisive victory.

Conclusion

The above-narrated semi-fictional tale is inspired from an assimilation of actual incidents and global developments relating to cyber-warfare. In May 2010, the US appointed a four-star general, Keith Alexander, as the head of its Cyber Command.[18] A month later, another four-star general was dethroned for his jaded sense of humour. The *Rolling Stones* article that did it for him also mentions how General Stanley McChrystal would seek

18 US National Security Agency. Biography - Commander, US Cyber Command, .*US National Security Agency.* [Online] http://www.nsa.gov/about/leadership/bio_alexander.shtml.

the help of "cyber freaks" – "24-year-old kid with a nose ring, with some ******* brilliant degree from MIT, sitting in the corner with 16 computer monitors humming" – to aid his counter-insurgency plan.[19]

A little-known company called Palantir Technologies has become a rage in the American intelligence community due its ground-breaking intelligence fusion platform, which is changing the way the CIA looks at each shred of information.[20] There are numerous incidents of hackers running wild over power grids and other critical infrastructure. Then in June 2010, the first instance of a malware specifically targeting installed SCADA software was discovered (W32.Stuxnet). And if there's still any doubt on the veracity of an airborne cyber-jammer, a handful of defence contractors have already developed Next-Generation Jammer with invasive Suter programs to be deployed on the futuristic F-35 fighters.[21]

As countries like the US, China, Israel and India gear up for cyber war, how effectively the conventional forces and intelligence agencies tap its full potential is just waiting to be seen.

19 Rolling Stone. The Runaway General. *The Rolling Stone*. [Online] 22 June 2010. http://www.rollingstone.com/politics/news/the-runaway-general-20100622.

20 Palantir Technologies. The industry solution for cyber. *Palantir Technologies*. [Online] http://www.palantirtech.com/government/cyber.

21 Aviation Week. Navy Confirms That New Jammer Will Be Cyber-Invasion Device. *Aviation Week*. [Online] 1 July 2011. http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckScript=blogScript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%3A27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3Aa2d11ad1-c7d4-403c-ad62-2fb21c53bb9d.