8 July, 2015

US Under Irresistible Cyber Attacks

*Dr. Omair Anas**

Within a few months of the announcement of "Department of Defense Cyber Strategy 2015", the United States faced massive cyber attack on 15 June 2015. The personal information of nearly four million US federal employees has been stolen, which includes social security numbers and other important details. The US media has immediately accused China for this attack and officials have issued statements indicating Chinese complicity. The Chinese Foreign Ministry has rejected these allegations calling them "unscientific and irresponsible."[1] The data allegedly stolen was about employees' records and security clearances. The US cyber security experts think that this information may be used 'for more elaborate, finely-tuned attacks in the future'. They think that this attack and earlier attacks of this nature must have been the work of hackers working on behalf of a state, not the usual cyber criminals.[2] Allegations of involvement of a state behind this attack gains some currency because the security clearance data stored at OPM (Office of Personnel Management)'s database included the Social Security numbers of its employees and their families through which they can hack further weapons programs.[3] According to the Goldman Sachs Global Investment Research, before this attack, IRS, Starbucks, Tesla Motors, Uber, Turbo Tax, Anthem, Malaysia Airlines, US Central Command, University of California, USPS, Snapchat, JP Morgan, Apple, AT&T Mobility, LLC, European Central Bank and Bank of America were high profile victims of cyber attacks from July 2014 to June 2015.

Cyber attacks are becoming the 'new normal' these days. In the last two months, there have been record number of cyber attacks in many countries. Attacks originating from unknown destinations have stolen large number of data or have disrupted some operations. These attacks are nothing, but an alarming indicator of how vulnerable the cyber world is becoming every day. No country is immune from these attacks. In March this year, the Chinese Internet company Qihoo 360's SkyEye Labs accused OceanLotus of executing "elaborately organized" online attacks on China's marine agencies, scientific research institutions and shipping companies since April 2012.[4] Apart from this traditional hide and seek game between the United States and China on cyber security, Israel was also accused of spying on Iranian nuclear talks through a virus program. The Russian cyber security company Kaspersky Lab suggested that Israel had used a new internet worm, "Duqu 2," to hack into networks of luxury hotels that hosted the negotiations between Iran and world powers.[5] On 17 June, the general website for Canadian government, canada.ca and other websites, such as the Canadian Security Intelligence Service (CSIS) were attacked by a group called *Anonymous* to protest the passage of a new anti-terrorism law by Canada's politicians.[6] In Australia alone, 3500 cyber attacks have been reported in April. According to the Australian authorities, "Cyber threats in Australia are typically classified as being state-sponsored or criminally motivated in terms of attribution to the source. The Australian agencies are mulling to recruit 'ethical hackers' to repel and track the threats."[7] With the intensity and scope of the cyber attacks, securitization of the cyber domain is on the rise, by both the states and business groups. Country like the U.S., its' Senate Armed Services Committee is considering adding $200 million to the Pentagon's fiscal 2016 budget for a cyber review of weapons programs. The cyber security programs, softwares and cyber insurance are becoming more important for business groups. With expanding cyber world, cyber attacks are also becoming more professional and expertise driven.

The Possible US Responses

In the past, US responses have been offensive as well as defensive. The attack on Iran's nuclear infrastructure with the Stuxnet virus and the attack on North Korea's nuclear infrastructure were the most targeted cyber attacks. China and the US regularly accuse each other for cyber attacks. Mark Pomerleau, quoting Rosenbach in his article on the recent cyber attack on US OBM networks, says that the US needs to develop the capabilities to deny a

potential attack from achieving its desired effect; secondly, the U.S. must increase the cost of executing a cyber attack; thirdly, they have to ensure that they are resilient.[8]

The burden of security is largely on the government to provide security to the business groups, particularly from the foreign originating attacks. Huge financial loss incurred by the business groups has made them demand that the government should share the loss. There are demands that penalizing American business for having been attacked by foreign powers is antithetical and, hence, legislative changes are being demanded. Among them is the suspension of all government imposed data breach penalties if the attack is found to have originated from a foreign nation state or its affiliates. Also, the U.S. government should help define which hackers trigger the aforementioned protections by establishing a list of state-sponsored or aligned hacker groups.[9]

Unlike the physically identifiable enemy, cyber threat does not come from an easily identifiable enemy, let alone tracing a certain nation state. Despite being at the helm of the US defense, cyber deterrence is not seen to have evolved as of now. The problem of evolving a deterrent doctrine is the red line not yet set for cyber attacks. In his testimony to the Congress, the Testimony Subcommittee on East Asia, the Pacific, and International Cyber Security Policy Senate Foreign Relations Committee, James A. Lewis states :

> In the Cold War, the threat of nuclear war deterred the Soviets from invading Western Europe and Japan or launching strategic attacks against the U.S. While it was often a subject of debate, the nuclear "umbrella" set redlines the Soviets could understand and found credible because they were linked to core American interests. The U.S. has thresholds or declaratory policies, but they are surrounded by a mass of caveats. This is sometimes lauded as "strategic ambiguity," but in fact, our adversaries just find it confusing. If opponents do not know what lines they should not cross, or do not believe that we will penalize them for crossing those lines; it will be hard to deter them.[10]

According to James, in the context of ambiguity in defining the threshold, 'a different approach is required to bring security and stability to cyberspace. And also because the unilateral deterrence is ineffective, there is need for international agreement'. These goals are in addition to DoD's three missions for cyberspace: "Defending DoD networks, defending U.S.

networks overall against significant attacks and providing full-spectrum cyber support for military operations." [11]

Tracing the Origin of Attacks

In the most fashionable way, rather in some hysterical reaction, the US authorities and media have been accusing China and Russia for many of these cyber attacks. The reason for major blame storming between the United States, China and Russia is because the US and China are major stakeholders in the cyber world. According to a report documented by the Akamai, majority of attack traffics originated from 194 unique countries/regions and China remains in the top slot (41% traffics), followed by United States (11%), Indonesia (7%), Taiwan (3%), Brazil (3%), Russia (2.9%) and India (2.6%). Enterprises and international commerce remain at the top of victims of these attacks, which attract 28 and 27 per cent cyber attacks, respectively, followed by the public sector (20%). This makes sense as the US and China dominate much of internet penetration. Of over 795 million IPv4 unique addresses from 240 unique countries/regions, 162 millions are from the United States and 123 million from China, 41 million from Brazil, 40 million from Japan and 37 million from Germany and 18 million from India.[12] With China and the US dominating the e-Commerce markets, combining for more than 55 per cent of global internet retail sales in 2014, transacting $1.316 trillion, cyber security in the US and China has become the most sensitive issue.[13] Given this much internet based economic and administrative transactions; there are also similar amount of cyber crimes. The US and China also dominate hardware industry of the information technology, while India is the second largest software exporter in the world. Given these factual realities, the clash of interests within American and Chinese businesses is very high, which have become more serious in claiming intellectual property rights. Though Russia is far behind China in massive use of information technology, its uneasy relations with the US are historical, both ideologically and politically. The new DoD Cyber Security Strategy 2015 has explicitly identified both China and Russia as major cyber threats for the US cyber security. The DoD report says:

> The DoD Cyber Strategy 2015 states potential adversaries have invested significantly in cyber as it provides them with a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests. Russia and

> China have developed advanced cyber capabilities and strategies. Russian actors are stealthy in their cyber tradecraft and their intentions are sometimes difficult to discern. China steals intellectual property (IP) from global businesses to benefit Chinese companies and undercut U.S. competitiveness. While Iran and North Korea have less developed cyber capabilities, they have displayed an overt level of hostile intent towards the United States and U.S. interests in cyberspace.[14]

Why is China considered as the biggest cyber security threat by the United States? From the US perspective, the Chinese Communist Party and its centralized control of entire state is at the helm of Chinese cyber behaviour. Amy Chang points out that maintaining economic growth and stability, protecting the governing power of the Chinese Communist Party, using computer network operations to signal dissatisfaction with foreign powers, preparing for military scenario and ensuring military superiority, studying potential adversaries' military infrastructures, motivations and objectives and finally advancing alternative narratives of government control of cyber security internationally are the major objectives of Chinese cyber security strategy. Amy argues that 'active defence' of Mao Zedong is still a guiding principle of China's cyber security strategy explained in its 2013 White Paper, The Diversified Employment of China's Armed Forces.[15]

The Chinese obsession had made the US declare establishment of US Cyber Command (CYBERCOM) in June 2009 and declaration of cyber space as a new domain of cyber warfare in 2011.[16] The 2015 Cyber Strategy announced by the US Department of Defense has outlined a five-points strategy: (1) build and maintain ready forces and capabilities to conduct cyberspace operations; (2) defend the DoD information network; (3) defend vital interests from disruptive or destructive cyber attacks; (4) build and maintain viable cyber options to control conflict escalation; and (5) build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability. According to these strategies, the US intends to build up cyber deterrence. Accordingly, the United States is developing not only its own capability, but also evolving a larger alliance from Europe to Asia Pacific to the West Asia with China back on the mind.

What Next

As a result, there is a visible cyber warfare race between China and the USA. Every new cyber technology from one country is in response of the second. Amid this competition, the UN appointed Government Group of Experts, after many failed attempts, has convinced China to accept applicability of international law and, in particular, the charter of the United Nations in the cyber sphere also. The recent attack on OPM has alarmed the American policy makers as it is one of the biggest data thefts in many years. The attribution deficit has always allowed China's deniability; however, the continuation of such massive and concerted attack cannot happen without the support of state authorities. In the American case, China is the prime accused because the United States has enough resources to trace the origin of these attacks. What about countries whose IT infrastructure is far poor? This scenario is extremely nightmarish as it suggests that most of the IT backward nations are almost exposed to big countries' state of art surveillance and espionage machinery. Bugging German Chancellor's phone and phones of French and British politicians mostly by the US National Security Agency had spoiled much of the US-Europe mutual trust. Revelations by Edward Snowden and Wikileaks' accessing confidential and diplomatic documents of several states are clear evidences that big countries and their sponsored or independent individuals are involved in a war for information. Small states, communities and individuals' privacy and property remain in perpetual state of compromise. This huge data theft has exposed the limitations of American power, amid the problem of attribution and persistent deniability. It seems that not much will change even after this attack. The US Chinese cyber conflict will remain a major cyber security concern and both countries will maintain their positions as always. In the absence of very strong multilateral and multi-sectoral intervention involving all stakeholders representing individuals, communities, business and the states, covert cyber conflicts and subsequent weapanization of the information technology will emerge in a dangerous scenario.

***

*Dr. Omair Anas is Research Fellow at the Indian Council of World Affairs, New Delhi

Endnotes:

[1] "Beijing Says Accusations of Federal Cyber Attack by Washington 'Unscientific'", *Global Times*, 6 June 2015. Retrieved online http://www.globaltimes.cn/content/925632.shtml (Accessed 23 June 2015).

[2] "China in Focus as Cyber Attack Hits Millions of US Federal Workers", *Reuter*, 5 June 2015. Retrieved http://www.reuters.com/article/2015/06/05/cybersecurity-usa-idUSL1N0YQ2GW20150605 (Accessed 26 June 2015).
[3] "The US Defense Industry is Reeling after the Latest Massive Cyber Attack", *The Business Insider*, 18 June 2015. Retrieved http://www.businessinsider.com/r-us-cyber-hack-unsettles-frustrates-us-defense-industry-2015-6#ixzz3dsetKSDf (Accessed 23 June 2015)
[4] "China Responds to Cyber Attack", *Global Times*, 3 June 2015. Retrieved http://www.globaltimes.cn/content/925076.shtml (Accessed 23 June 2015).
[5] "Israel Denies Reports on Cyber Attacks on Nuclear Talks with Iran", *Global Times*, 12 June 2015. Retrieved http://www.globaltimes.cn/content/926697.shtml (Accessed 23 June 2015).
[6] "Canada Government Websites Taken Down in Cyber Attack", *The Guardian*, 18 June 2015. Retrieved http://www.theguardian.com/technology/2015/jun/18/canada-government-websites-taken-down-in-cyber-attack (Accessed 23 June 2015).
[7] "Cyber Attacks: More than 3,500 Breaches in April and Threats Set to Increase, AFP Says", *Australian Broadcasting Corporation,* 15 June 2015, Retrieved http://www.abc.net.au/news/2015-06-15/threat-of-cyber-attacks-set-to-increase-says-afp/6547696 (Accessed 23 June 2015).
[8] Mark Pomerleau, "How might the US Respond to Cyber Attacks?", Retrieved http://defensesystems.com/Articles/2015/06/10/US-response-scenario-cyber-attack.aspx?Page=4 (Accessed 10 June 2015).
[9] *Brian E. Finch, "*Companies Facing Cyber Attacks from Nation-States Need Better Legal Protection", *Wall Street journal,* 22 June 2015. Retrieved http://blogs.wsj.com/cio/2015/06/22/companies-facing-cyberattacks-from-nation-states-need-better-legal-protection/ (Accessed 24 June 2015).
[10] James A. Lewis, "Testimony Subcommittee on East Asia, the Pacific, and International Cyber Security Policy Senate Foreign Relations Committee", The US Senate, 14 March 2015. Retrieved http://www.foreign.senate.gov/imo/media/doc/051415_REVISED_Lewis_Testimony.pdf (Accessed 24 June 2015).
[11] ibid
[12]AKAMAI, "Akamai's State of the Internet: Prolexic Quarterly Global DDoS Attack Report", Q1 2014 Report, Volume 7, Number 1. Retrieved http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf (Accessed 24 June 2015).
[13] E Marketer, "Retail Sales Worldwide will Top $22 Trillion This Year", 23 December 2014. Retrieved http://www.emarketer.com/Article/Retail-Sales-Worldwide-Will-Top-22-Trillion-This-Year/1011765 (Accessed 15 June 2015).
[14] The Department of Defense, "The DoD Cyber Strategy 2015", The Department of Defense.
[15] Chang, Amy, "Warring State: China's Cyber Security Strategy", December 2014, Center for a New American Security.
[16] ibid