2 Days International Conference on CSIT-2019, ICSD-2019
Mahratta Chamber of Commerce, Industries and Agriculture Tilak Road, Pune (India)
2nd -3rd November 2019 www.conferenceworld.in
ISBN : 978-81-943584-1-1

REGIONAL RIVALRY BETWEEN INDIA-PAKISTAN A DRAMATIC RISE OF CYBER-ATTACKS IN POST-KASMIR DECISION

Manoj Dathan M
Assistant Professor Inpolitical Science
Department of Humanities, St Paul Institute of Professional Studies Indore

ABSTRACT

Cyber nationalists from India and Pakistan are spoiling for a fight, after an anonymous hacker from India defaced Pakistan government website www.pakistan.gov.pk, weeks ahead of the two countries' independence days. Experts predict the attack on a Pakistani government website is bound to activate hackers from both the countries to try and breach each other's cyber space and over thousands of websites from both the countries face high risk of being hacked. Indian hacker going by a cryptic name of -Ne0-h4ck3r had changed the Pakistani website by posting Indian national anthem and Independence Day greetings on its wall. The hacker posted Ashoka Chakra in Tricolour, along with Indian Independence Day message. Another message that was posted on the website read, "Freedom in the Mind, Faith in the words. Pride in our Souls. Let's salute those great men, who made this possible."The message was followed by the Indian national anthem. Even though the website was quickly restored by the Pakistan's IT team, the move was claimed as a 'victory' by Indian cyber nationalists. The foreign office of the Pakistan in Islamabad has not reacted to the incident. Experts say that August draws maximum hacking of websites in the south Asia as techies from both the countries put their skills and nationalistic fervour to test by hacking each other's websites. The activity is usually limited to one month alone but this year, the India hacker may have riled Pakistani cyber experts by hacking one of the biggest government websites. Action reaction A response in equal measure is expected soon where, observers say, Pakistani hackers will try to target prominent and sensitive Indian government websites. In the past, state police websites have been defaced by Pakistani hackers where they posted anti-India comments with an image of the Pakistan flag.

Keywords: Cyber Attacks, India Pakistan Realtion,Kasmir, New War ,Hacking, Home Ministry

INTRODUCTION

"In almost ritualistic attacks, every year underground hacking communities from both the countries launch cyber attacks on each other, ahead of August 14 and 15, the Pakistani and Indian independence days respectively," said **Kislay Choudhary, director of Indian Cyber Army.**

Choudhary said as Indian hackers have attacked where it hurts the most by taking their most prominent government website, Pakistani hackers will respond in kind by targeting Indian government portals, possibly where Indian take much pride.

"Elsewhere, attackers may try to steal data or acquire digital warriors had crippled 30 Pakistan government websites earlier this year in virtual surgical strikes as protest against the neighbouring country's announcement of death penalty to former Navy officer Kulbhushan Jadhav. Indian and Pakistani hackers also fought pitched battles in cyber space after last September's terrorist attack on a military camp in Jammu and Kashmir's Uri sector. complete control over the infected network. But in

ISBN : 978-81-943584-1-1

the case of India and Pakistan, it's more a display of power and skills. Most of these hackers are school and college students," said another cyber expert. This is not the first time when such an incident has taken place in Pakistan. India's digital warriors had crippled 30 Pakistan government websites earlier this year in virtual surgical strikes as protest against the neighbouring country's announcement of death penalty to former Navy officer Kulbhushan Jadhav. Indian and Pakistani hackers also fought pitched battles in cyber space after last September's terrorist attack on a military camp in Jammu and Kashmir's Uri sector.

REAL RIVALRY

There has been a rise in cyber-attacks on Indian institutions after the abrogation of Article 370 and 35A and the country needs to be extra careful when it comes to the security of websites and critical infrastructure, Russian cyber security firm Kaspersky said on Monday.On Sunday, the official website of the Bihar Education Department was hacked and "RootAyyildiz Turkish Hacker" claimed responsibility for posting messages praising Pakistan and Islam like "We Love Pakistan" on the website.The hacked portal was later restored."We have definitely seen an increase in the cyber-attacks on India after the abrogation of Article 370 by the Indian government. According to our Cyberthreat World-time Map, India is currently the 7th most attacked country in the world," Saurabh Sharma, Senior Security Researcher, Global Research and Analysis Team (GReAT) APAC, Kaspersky, told IANS. However, it is difficult in the current situation to understand if these are state-sponsored attacks."We cannot confirm if it originated from Pakistan or it's a group of cyber attackers targeting India while taking advantage of the current situation and leaving messages that may suggest otherwise," Last month, the Indian Computer Emergency Response Team (CERT-In) informed the Parliament that over 24 websites of central ministries, departments and state governments were hacked till May.

IT Minister Ravi Shankar Prasad said in a written reply in the Lok Sabha that attempts have been made from to launch cyber attacks on Indian cyber space, and these attacks were seen to be originating from a number of countries, including China and Pakistan. "India needs to be more careful when it comes to the security of their websites and critical infrastructure, especially when there are cyber attackers that are ready to exploit our vulnerabilities in the name of cyberwar between countries," the Kaspersky executive cautioned.

Rows colored in gray refer to cyber-related incidents.

08.1947

India and Pakistan become independent states, but the status of the northern border provinces of Jammu and Kashmir remain undecided.

10.1947

The Pakistani government supports a Muslim demonstration in Kashmir and starts the 1947-1948 war.

01.1949

India and Pakistan sign the end of the 1947-1948 war and agree on the creation of a Line of Control.

04.1965

Clashes between border patrols on the Line of Control start the 1965 war that ends in January 1966.

1971

ISBN : 978-81-943584-1-1

East Pakistan achieves independence in the Indo-Pakistani War of 1971. East Pakistan becomes known as Bangladesh.
01.1972
Pakistan starts its nuclear program.
1974
India detonates its first nuclear device.
1988
India and Pakistan agree not to attack their respective nuclear facilities.
1989
Pakistan announces a successful launch of a long-range missile. 1996 India and Pakistan actively try to find a diplomatic solution to ease tensions in the region.
05.1998
India conducts an underground nuclear test in the western state of Rajasthan and Pakistan responds with its first nuclear bomb tests inBaluchistan in the south-west part of Pakistan (BBC News, 2001; Hashim, 2014).
05.1998
Pakistani hackers hack the Indian Bhabha Atomic Research Center's website (Garsein, 2012).
05.1999
Pakistani groups cross the Line of Control in the Kargil region of Kashmir, prompting a retaliatory airstrike from India and starting the Kargil conflict (BBC News, 2001).
10.1999
Pakistani hackers deface an Indian Army propaganda website with messages denouncing torture in Kashmir by the Indian Army (BBC News, 1998).
10.1999
General Musharraf leads a coup to depose Pakistani President Nawaz
Sharif.
10.2001
An armed attack on the Kashmiri assembly kills 38 individuals (BBC News, 2001).
23.10.2001
Pakistani patriotic hackers deface two Indian news websites (Majumder, 2001).
13.12.2001
An armed attack on the Indian Parliament kills 14 individuals.
01.2002
Pakistani President Musharraf declares that Pakistan will fight extremism on its territory, but that Kashmir belongs to Pakistan.
2004
The Composite Dialogue Process, a bilateral meeting process, starts between Indian and Pakistani government officials.
07.2008
Indian officials accuse Pakistani Inter Services Intelligence (ISI) of bombing the Indian embassy in Kabul.
26.11.2008
Lashkar-e-Taiba7, a Pakistani militant group, attacks several targets in Mumbai, including the Taj Mahal Hotel (BBC News, 2018a, 2018b).

ISBN : 978-81-943584-1-1

27.11.2008
As retaliation for the Mumbai terrorist attacks, Indian hackers deface several Pakistani websites
28.11.2008
As retaliation for the defacements, Pakistani hackers deface Indian websites (RFSID, 2016; Ribeiro, 2008).
2009
Pakistani authorities admit that Mumbai terrorist attacks were partlyorganized from Pakistan, but deny ISI's involvement.
01.2010
Pakistani and Indian troops exchange fire in Kashmir across the Line of Control (Hashim, 2014).
26.11.2010
Indian hackers deface 35 Pakistani websites on the anniversary of th Mumbai terrorist attack.
03.12.2010
Pakistani hackers hack and erase data on the Indian Central Bureau of Investigation website as retaliation for the defacements of November 2010 (Leyden, 2010).
29.11.2011
Indian hackers deface hundreds of Pakistani websites (Kumar, 2011a).
12.2011
A series of tit-for-tat cyberattacks occurs between Indian and Pakistani hackers until February 2012 (Joshi, 2012).
26.01.2012
Independently from the series of cyberattacks mentioned above, Pakistani hackers deface more than 400 Indian websites on Indian Republic Day (Mid Day, 2012).
15.08.2012
Indian hackers deface Pakistani websites on Pakistan Independence Day (Garsein, 2012).
17.03.2013
A Norwegian telecommunications firm reveals that it has been targeted by a cyberespionage campaign possibly coming from India (Fagerland et al., 2013).
26.11.2013
Indian hackers deface several Pakistani websites on the anniversary of the Mumbai terrorist attacks. Pakistan Cyber Army, a Pakistani patriotic hacker group, retaliates by defacing the website of the Indian Central Bank (Kovacs, 2013a).
26.01.2014
Pakistani hackers deface thousands of Indian websites on the Indian Republic Day (Khan, 2014).
26.11.2014
Indian hackers deface several Pakistani government websites on the anniversary of the Mumbai terrorist attacks (Web Desk, 2014a).
26.11.2015 Indian hackers target more than 200 Pakistani websites on the anniversary of the Mumbai terrorist attacks. Pakistani hackers retaliate by defacing the Indian Central Bank website.
06.01.2016
Terrorists attack an Indian Air Force base in Pathankot in northern India.
07.01.2016
Indian hackers retaliate for the terrorist attack in Pathankot with thedefacement of Pakistani websites (RFSID, 2016).

ISBN : 978-81-943584-1-1

03.03.2016
Pakistani authorities arrest an Indianindividual suspected of espionage in Pakistan (Shukla, 2017).
15.08.2016
Indian hackers deface more than 50 Pakistani websites on Pakistan Independence Day (TNM Staff, 2016).
18.09.2016
A Pakistani militant group kills 19 individuals in an attack in Uri in Jammu.
23.09.2016
India retaliates for the attack in Uri with surgical strikes.
04.10.2016
Pakistani hackers retaliate for the surgical strikes with the defacement of thousands of Indian websites and Indian hackers claim to have access to Pakistani critical infrastructure networks.

10.04.2017
The Indian individual arrested in 2016 receives the death penalty in Pakistan.
10.04.2017
Indian hackers retaliate with the defacement of hundreds of Pakistani websites to protest against their compatriot's death penalty sentence (Trivedi, 2016).

Effects

This section analyzes the effects of the cyber -attacks between India and Pakistan on both Indian and Pakistani societies, the economic costs of this cyber-conflict, and technological implications. Additionally, the consequences of cyberattacks on the international level will be examined. Increasing levels of interference from non-state actors risks escalating regional tensions into a conventional conflict, and portends cyberespionage campaigns that span far beyond the Indian and Pakistani borders.

Social effects

The most typical type of cyberattack used to denigrate the opposing state was website defacement. Website defacements are more of a disruption or annoyance, and they do not tend to result in lasting or physical damage. Nevertheless, the inconvenience created by website defacement affected the users of the defaced websites, especially because hacktivists and patriotic hackers often targeted government agencies' websites. Given the public nature of the attack, website defacements typically garnered more attention than other types of cyberattacks, such as cyberespionage. The increased visibility may also imply that defacements are a more significant attack on a country than the act itself should objectively merit. Perpetrators of website defacements usually took responsibility for their acts and relied on media coverage to further spread their message. Furthermore, the intense media scrutiny resulting from website defacements can be manipulated to generate fear among the targeted population. These attacks acted as reminders for the rival population that they are at risk and cannot protect themselves from cyberattacks. Often, the website defacements were a reaction to specific events, like a cricket game or the arrest of an Indian individual in Pakistan. Real-world incidents would trigger a response from the hacktivists and patriotic hackers to either express their dissatisfaction with events, denounce a situation that they consider to be unfair, or simply express their patriotism. For example, Indian hacktivists and patriotic hackers regularly targeted Pakistani

websites with Indian patriotic messages (Balduzzi et al., 2018; Bussoletti, 2018; RFSID, 2016; Web Desk, 2014b).

Economic effects

The economic effects of the tit-for-tat dynamic between India and Pakistan in cyberspace are limited. Consequences primarily consisted of the costs of website defacement for the owners of affected websites. These losses are not materially different from the price of similar Distributed Denial of Service (DDoS) attacks. For private businesses, defacements result in lost customers due to the unavailability of the webpages and damages to the businesses' reputation. For other targets, such as government agencies, websites defacement generates a loss of trust from the websites' users. The fact that website owners failed to proactively address vulnerabilities in their website suggested to the users that the website and its owners were not trustworthy (Paladion Networks, 2015). 4.3 Technological effects Cybersecurity experts that studied APT groups from India and Pakistan found that it was easy to conduct significant cyberespionage campaigns using relatively unsophisticated and readily available cybertools. The experts exposed that Indian and Pakistani APTs either built their malware from codes copied directly from hacker forums or open source projects, or used malware that was freely available on the internet. The widespread availability of malicious cybertools and codes is not new, but to witness actors - some with alleged state sponsorship - capitalize on these instruments is rather unique. Combining relatively simple malware with spear phishing and watering hole attacks, Indian and Pakistani APT groups managed to steal a significant volume of information from their victims. These cases demonstrated that APT groups did not have to rely on highly complex technology to achieve their goals. An important caveat to this lesson is that experts also concluded populations in India and Pakistan were not well-versed in cybersecurity issues. In part, this is due to a simple lack of awareness; APT groups appeared to recognize unsophisticated cybertools were enough to achieve their goals (Cymmetria, 2016; Huss, 2016; Sancho and Hacquebord, 2016; Settle et al., 2016). 4.4 International effects The international consequences of India and Pakistan's rivalry in cyberspace are minimal. The main risk presented by continued cyberattacks is a possible escalation of real-world events through the actions of non-state actors on the internet. Additionally, cyberespionage campaigns directed towards third party states hold the potential to significantly damage relations between India, Pakistan, and the rest of the world. Non-state actors While website defacements thus far have largely been considered a mere annoyance, there is a risk that defacement may escalate existing tensions and prompt a conventional conflict. Website defacements were typically conducted by non-state actors, and it remains difficult to evaluate the relationship between these shadowy hackers and the official state apparatus. Even if non-state actors are completely independent from their parent state, their motives were often patriotic and responded to events in the physical world that the hackers considered an affront to their nation. In the case of India and Pakistan, these cyberattacks are largely carried out by the population, not the official state and risk to solidify the conflict at the population level. While these small-scale attacks are clearly derived from the bottom-up, the target state may perceive the attacks as being conducted by the official government. This is of particular risk as cyberattacks evolve and seek to target more advanced targets (e.g., critical infrastructures), or if continuous website defacements become too disruptive to society (Lin, 2012). India and Pakistan have nuclear capabilities and an escalation from cyberspace to conventional conflict also brings the risk of a further escalation into a nuclear conflict. That being said, the effects of cyberattacks have been constrained to the cybersphere for the last 15 years. Hacktivists and patriotic hackers defaced websites as a response to physical events like a terrorist attack or skirmishes along the Line of Control, but thus

ISBN : 978-81-943584-1-1

far, no website defacement has prompted a real-world response. Nevertheless, cyberattacks of low intensity, like website defacements, will most likely continue between Indian and Pakistani hacktivists and patriotic hackers. This pattern will continue to increase the risk of misinterpretation and escalation. International cyberespionage The Indian APT conducted several cyberespionage campaigns, primarily targeting Indian secessionist groups and Pakistani actors. However, this APT also targeted firms and government institutions outside India and Pakistan. The targets appeared to be government and industry-related institutions in neighboring countries, the Middle East, and the West. (Crowdstrike, 2016; Lunghi et al., 2017; Symantec Security Response, 2013). Espionage and cyberespionage may be at least tolerated on the international level for national security purposes, but no such allowance exists for economic espionage. Economic cyberespionage campaigns risk straining relationships between the targeted states and India. Furthermore, targeted private firms may seek governmental support, which would open the Indian APT up to retaliation. This is also true of regular espionage, if a neighboring or partner country of India discovered that it was the target of that APT.

Technological effects

Cybersecurity experts that studied APT groups from India and Pakistan found that it was easy to conduct significant cyberespionage campaigns using relatively unsophisticated and readily available cybertools. The experts exposed that Indian and Pakistani APTs either built their malware from codes copied directly from hacker forums or open source projects, or used malware that was freely available on the internet. The widespread availability of malicious cybertools and codes is not new, but to witness actors - some with alleged state sponsorship - capitalize on these instruments is rather unique. Combining relatively simple malware with spear phishing and watering hole attacks, Indian and Pakistani APT groups managed to steal a significant volume of information from their victims. These cases demonstrated that APT groups did not have to rely on highly complex technology to achieve their goals. An important caveat to this lesson is that experts also concluded populations in India and Pakistan were not well-versed in cybersecurity issues. In part, this is due to a simple lack of awareness; APT groups appeared to recognize unsophisticated cybertools were enough to achieve their goals (Cymmetria, 2016; Huss, 2016; Sancho and Hacquebord, 2016; Settle et al., 2016)

International effects

The international consequences of India and Pakistan's rivalry in cyberspace are minimal. The main risk presented by continued cyberattacks is a possible escalation of real-world events through the actions of non-state actors on the internet. Additionally, cyberespionage campaigns directed towards third party states hold the potential to significantly damage relations between India, Pakistan, and the rest of the world.

Non-state actors

While website defacements thus far have largely been considered a mere annoyance, there is a risk that defacement may escalate existing tensions and prompt a conventional conflict. Website defacements were typically conducted by non-state actors, and it remains difficult to evaluate the relationship between these shadowy hackers and the official state apparatus. Even if non-state actors are completely independent from their parent state, their motives were often patriotic and responded to events in the physical world that the hackers considered an affront to their nation. In the case of India and Pakistan, these cyberattacks are largely carried out by the population, not the official state

ISBN : 978-81-943584-1-1

and risk to solidify the conflict at the population level. While these small-scale attacks are clearly derived from the bottom-up, the target state may perceive the attacks as being conducted by the official government. This is of particular risk as cyberattacks evolve and seek to target more advanced targets (e.g., critical infrastructures), or if continuous website defacements become too disruptive to society (Lin, 2012). India and Pakistan have nuclear capabilities and an escalation from cyberspace to conventional conflict also brings the risk of a further escalation into a nuclear conflict. That being said, the effects of cyberattacks have been constrained to the cybersphere for the last 15 years. Hacktivists and patriotic hackers defaced websites as a response to physical events like a terrorist attack or skirmishes along the Line of Control, but thus far, no website defacement has prompted a real-world response. Nevertheless, cyberattacks of low intensity, like website defacements, will most likely continue between Indian and Pakistani hacktivists and patriotic hackers. This pattern will continue to increase the risk of misinterpretation and escalation

CONCLUSION

Many cyberattacks between Indian and Pakistani actors started with spear phishing campaigns. Spear phishing emails served to lure the victim to download an attachment infected with malware or to click on a link to direct the victim to a malicious website. It is, therefore, necessary to raise awareness among users about such dangers. Sensitization campaigns could help users more easily recognize spear phishing emails and watering hole attacks. Institutions could also implement standardized procedures in case an employee opens a malicious attachment or clicks on a malicious link. A predetermined response would help institutions to deal faster with the intrusion. Implementing an email authentication system, like the Sender Policy Framework (SPF), could provide a technological solution to problems of phishing. The SPF certifies the authenticity of the sender of an email, making it easier to identify spear phishing emails. In the case of website defacement, there is no specific measure that could guarantee that a website will not be defaced. However, there are tactics that website owners can implement to reduce their risk. Website owners could conduct regular penetration tests to detect vulnerabilities. In addition, website defacement monitoring and detection tools could help website owners react faster in the event of a defacement

Bibliography

Bajoria, J., 2010. Profile: Lashkar-e-Taiba (Army of the Pure) (a.k.a. Lashkar e-Tayyiba, Lashkar eToiba; Lashkar-i-Taiba) [WWW Document]. Counc. Foreign Relat. URL https://web.archive.org/web/2010060515191 8/http://www.cfr.org/publication/17882/ (accessed 11.04.18).

Balduzzi, M., Flores, R., Gu, L., Maggi, F., 2018. A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks (TrendLabs Research Paper). Trend Micro. BBC News, 2018a. Pakistan profile - Timeline [WWW Document]. BBC News. URL http://www.bbc.com/news/world-south-asia12966786 (accessed14.03.18).

BBC News, 2018b. India profile - Timeline [WWW Document]. BBC News. URL http://www.bbc.com/news/world-south-asia 12641776 (accessed 14.03.18). BBC News, 2001. India-Pakistan: Troubled relations [WWW Document]. BBC News. URL

ISBN : 978-81-943584-1-1

http://news.bbc.co.uk/hi/english/static/in_de_pth/south_asia/2002/india_pakistan/timeline/ default.stm (accessed 13.03.18).

BBC News, 1998. World: South Asia Indian army Website ambushed [WWW Document]. BBC News. URL http://news.bbc.co.uk/2/hi/south_asia/19484 4.stm (accessed 21.03.18).

Blaich, A., Flossman, M., 2018. Stealth Mango and Tangelo: Nation state mobile surveillanceware stealing data from military & government officials [WWW Document]. Lookout Blog. URL https://blog.lookout.com/stealth-mango (accessed 25.05.18).

Bussoletti, F., 2018. Between India-Pakistan is ongoing a cyberwar involving "patriot hackers" [WWW Document]. Difesa Sicurezza. URL https://www.difesaesicurezza.com/en/cyberen/between-india-pakistan-is-ongoingcyberwar-involving-patriot-hackers/ (accessed 21.03.18).

Center for Strategic and International Studies, 2018. Significant Cyber Incidents [WWW Document]. Cent. Strateg. Int. Stud. URL https://www.csis.org/programs/cybersecurityand-warfare/technology policyprogram/other-projects-cybersecurity (accessed 25.01.18).